Dihedral Universal Deformations

Shaunak V. Deo and Gabor Wiese

14th May 2018

Abstract

This article deals with universal deformations of dihedral representations with a particular focus on the question when the universal deformation is dihedral. Results are obtained in three settings: (1) representation theory, (2) algebraic number theory, (3) modularity. As to (1), we prove that the universal deformation is dihedral if all infinitesimal deformations are dihedral. Concerning (2) in the setting of Galois representations of number fields, we give sufficient conditions to ensure that the universal deformation relatively unramified outside a finite set of primes is dihedral, and discuss in how far these conditions are necessary. As a side-result, we obtain cases of the unramified Fontaine-Mazur conjecture. As to (3), we prove a modularity theorem of the form '$R = \mathbb{T}$' for parallel weight one Hilbert modular forms for cases when the minimal universal deformation is dihedral.

MS Classification: 11F80 (primary), 11F41, 11R29, 11R37

1 Introduction

The basic object in this article is a continuous absolutely irreducible representation

$$\overline{\rho} : G \to \mathrm{GL}_2(\mathbb{F})$$

that is *dihedral* in the sense that it is induced from a character, where G is a profinite group and $\mathbb{F}$ is a finite field of characteristic p. We consider a deformation $\rho : G \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ for any complete local Noetherian algebra R over $W(\mathbb{F})$, the ring of Witt vectors of $\mathbb{F}$, with residue field $\mathbb{F}$. We prove results in the following three settings:

(1) Representation theory results:

We fully characterise in representation theory terms when a deformation ρ of $\overline{\rho}$ as above is *dihedral*. We also prove that being dihedral is an *infinitesimal property*, in the following sense: the universal deformation of $\overline{\rho}$ is dihedral if and only if all infinitesimal deformations are dihedral.

(2) Number theory results:

Here we let G be $G_K = \mathrm{Gal}(\overline{K}/K)$, the absolute Galois group of a number field K. We give sufficient conditions, using class field theory, to ensure that the universal deformation of $\overline{\rho}$ relatively unramified outside a finite set of primes remains dihedral. In those cases, we compute the structure of the corresponding universal deformation ring and discuss in a series of remarks in how far the sufficient conditions are necessary. We also apply our results to Boston's strengthening of the unramified Fontaine-Mazur conjecture.

(3) Modularity results (an '$R = \mathbb{T}$-theorem'):

Assume in addition that the number field K is totally real, that $\overline{\rho}$ is unramified above p, and that certain other conditions are satisfied. We prove that the minimal deformation ring of $\overline{\rho}$ coincides with the Hecke algebra acting on certain Hilbert modular forms in parallel weight one.

We now elaborate more on these results.

1.1 Representation theory results

Let $H \lhd G$ be the index 2 subgroup such that there is a character $\overline{\chi} : H \to \mathbb{F}^\times$ and $\overline{\rho}$ is the induction of $\overline{\chi}$ from H to G (these exist by the definition of dihedral representations 2.2). As initiated by Boston [Bos91] our analysis of deformations of $\overline{\rho}$ will be through actions on pro-p groups, as follows. Let R be a complete Noetherian local $W(\mathbb{F})$-algebra with residue field $\mathbb{F}$. Let $\rho : G \to \mathrm{GL}_2(R)$ be a lift of $\overline{\rho}$ and define the pro-p group Γ_ρ by the following diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & \Gamma_\rho \arrow[r] \arrow[d, equal] & \mathrm{im}(\rho) \arrow[r] & \overline{\rho}(G) \arrow[r] & 0 \\ 0 \arrow[r] & \Gamma_\rho \arrow[r] & \mathrm{im}(\rho|_H) \arrow[r] \arrow[u, hook] & \overline{\rho}(H) \arrow[r] \arrow[u, hook] \arrow[l, bend left, "s"] & 0 \end{tikzcd} \tag{1.1}$$

Let $\overline{G}^{\mathrm{ad}}$ be the image of the adjoint representation of $\overline{\rho}$ and $\overline{H}^{\mathrm{ad}}$ the image of its restriction to H. As indicated, the lower sequence in (1.1) always splits, and the upper sequence splits if $p > 2$. This gives us an action on Γ_ρ of $\overline{H}^{\mathrm{ad}}$ in all cases, and of $\overline{G}^{\mathrm{ad}}$ if $p > 2$ or Γ_ρ is abelian (see Lemma 2.9).

Our first main result is the following characterisation of dihedral deformations via the p-Frattini quotient $\Gamma_\rho/\Phi(\Gamma_\rho)$ of Γ_ρ.

Theorem 1.1. *The following statements are equivalent:*

(i) ρ is dihedral, i.e., there is a lift $\chi : H \to R^\times$ of $\overline{\chi}$ such that ρ is equivalent to $\mathrm{Ind}_H^G(\chi)_R$, the induction of χ from H to G.

(ii) The action of $\overline{H}^{\mathrm{ad}}$ on Γ_ρ is trivial (and hence $\rho(H) \cong \Gamma_\rho \times s(\mathrm{im}(\overline{\rho}|_H))$).

(iii) The action of $\overline{H}^{\mathrm{ad}}$ on $\Gamma_\rho/\Phi(\Gamma_\rho)$ is trivial.

Concerning the final item, we provide the full list of simple $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-modules and $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules that can occur in $\Gamma_\rho/\Phi(\Gamma_\rho)$ in Corollary 2.12. This theorem is applied to infinitesimal deformations that are defined as follows.

Definition 1.2. *Let $\rho : G \to \mathrm{GL}_2(R)$ be a deformation of $\overline{\rho}$ as above. Write $\rho_{\mathrm{inf}} := \pi \circ \rho$ for $\pi : \mathrm{GL}_2(R) \to \mathrm{GL}_2(R/(\mathfrak{m}_R^2, p))$, where $\mathfrak{m}_R$ is the maximal ideal of R. We say that ρ is* infinitesimal *if $\rho = \rho_{\mathrm{inf}}$, i.e. if $\mathfrak{m}_R^2 = 0$ and $pR = 0$.*

Note that this extends the definition of infinitesimal deformations as representations to the dual numbers that one often finds in the literature.

For the sequel we impose that the profinite group G satisfies Mazur's finiteness condition Φ_p (see [Maz89, §1.1]). In that case, there exists a universal deformation

$$\rho^{\mathrm{univ}} : G \to \mathrm{GL}_2(R^{\mathrm{univ}}).$$

Write $\rho_{\mathrm{inf}}^{\mathrm{univ}} := (\rho^{\mathrm{univ}})_{\mathrm{inf}}$, as well as $\Gamma^{\mathrm{univ}} := \Gamma_{\rho^{\mathrm{univ}}}$ and $\Gamma_{\mathrm{inf}}^{\mathrm{univ}} := \Gamma_{\rho_{\mathrm{inf}}^{\mathrm{univ}}}$. In this notation, we find the following description of the p-Frattini quotient associated with the universal deformation of $\overline{\rho}$.

Corollary 1.3. $\Gamma_{\mathrm{inf}}^{\mathrm{univ}} \cong \Gamma^{\mathrm{univ}}/\Phi(\Gamma^{\mathrm{univ}})$.

Our second main result states that the universal deformation of $\overline{\rho}$ is dihedral if and only if all infinitesimal deformations are.

Theorem 1.4. *(a) The following statements are equivalent:*

- *(i) ρ^{univ} is dihedral.*
- *(ii) Any deformation $\rho : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ of $\overline{\rho}$ is dihedral.*
- *(iii) Any infinitesimal deformation of $\overline{\rho}$ is dihedral.*
- *(iv) $\rho_{\mathrm{inf}}^{\mathrm{univ}}$ is dihedral.*

(b) If the conditions in (a) are satisfied, then R^{univ} is isomorphic to the universal deformation ring $R_{\overline{\chi}}^{\mathrm{univ}}$ of $\overline{\chi}$, as computed in Proposition 2.1.

The main step in the proof of the theorem is to realise any group extension of $\mathrm{im}(\overline{\rho})$ by an $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module that can occur in the p-Frattini quotient of some Γ_ρ as the image of an infinitesimal deformation of $\overline{\rho}$ (see Proposition 2.14).

1.2 Number theory results

Let K be a number field, let $G = G_K = \mathrm{Gal}(\overline{K}/K)$ be its absolute Galois group, and let $\overline{\rho} = \mathrm{Ind}_H^G(\overline{\chi})$ be as before. For a finite set S of places of K, denote by ρ_S^{univ} the universal deformation of $\overline{\rho}$ relatively unramified outside S and by $(\rho_S^{\mathrm{univ}})^0$ the one the determinant of which is the Teichmüller lift of $\det \circ \overline{\rho}$.

We need to introduce some further notation. Let S_∞ be the set of all archimedean places of K, let S_p be the set of all places above p and let S_0 be the set of finite places explicitly defined in terms of $\overline{\rho}$ in section 3. Denote by $\overline{\chi}^\sigma$ the conjugate character by any $\sigma \in G \setminus H$ and by $I(\overline{\chi}/\overline{\chi}^\sigma)$ the induction of $\overline{\chi}/\overline{\chi}^\sigma$ from H to G defined over its field of definition. Furthermore, let M^{ad} be fixed field under the image of the adjoint representation of $\overline{\rho}$, that is, $\mathrm{Gal}(M^{\mathrm{ad}}/K) = \overline{G}^{\mathrm{ad}}$. Denote by $A(M^{\mathrm{ad}})$ the class group of M^{ad}. We can now state our main result in this set-up, the representation-theoretic backbone of which is Theorem 1.1.

Theorem 1.5. *Let S be a finite set of places of K such that*

$$S_\infty \subseteq S, \quad S \cap S_p = \emptyset, \text{ and } S \cap S_0 = \emptyset.$$

Assume also that the following condition holds:

$$\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0.$$

If $p = 2$, assume in addition that M^{ad} is totally imaginary.

Then ρ_S^{univ} is a dihedral deformation of $\overline{\rho}$.

Note that in the basic case $S = S_\infty$ the set S_0 does not play any role, and the theorem essentially follows from Theorem 1.1. More generally, the set S_0 takes care of the maximal elementary abelian p-extension unramified outside S of M^{ad}, in the sense that the representation $I(\overline{\chi}/\overline{\chi}^\sigma)$ cannot occur in the corresponding Galois group viewed as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module. The definition of the set S_0 is thus rooted in global class field theory.

In Remark 3.11 (see also the Remarks 3.5, 3.6, 3.7, 3.8), we discuss in how far the hypotheses imposed in Theorem 1.5 are necessary for the conclusion to hold.

In Corollaries 3.12 and 3.14, the structure of the universal deformation ring and its variant with 'constant determinant' are computed (the latter only for $p > 2$) under the assumptions of Theorem 1.5. The main point is that all dihedral deformations of $\overline{\rho}$ are inductions of 1-dimensional deformations of the character $\overline{\chi}$.

Recall that Boston's strengthening of the unramified Fontaine-Mazur conjecture ([Bos99, Conjecture 2]) states the following (see [AC14] as well):

> *Let N be a number field, $\mathbb{F}$ be a finite field of characteristic p and $\rho : G_N \to \mathrm{GL}_n(\mathbb{F})$ be a continuous absolutely irreducible Galois representation. Let S be a finite set of primes of N not containing any prime of N lying above p. Then the universal deformation of ρ relatively unramified outside S (defined in the same way as in the remark after Lemma 3.9) has finite image.*

Corollary 1.6. *Let S be a finite set of primes of K. If the conditions given in Theorem 1.5 hold, then Boston's strengthening of the unramified Fontaine-Mazur conjecture is true for the tuple $(K, S, \overline{\rho})$.*

As an illustration of Corollary 1.6, we specialise it to a couple of examples which we describe now. Let $\mathbb{F}_{81}$ be the degree 4 extension of $\mathbb{F}_3$. The number field $L := \mathbb{Q}(\sqrt{-3}, \sqrt{-239}) = \mathbb{Q}(\sqrt{-3}, \sqrt{717})$ has class number 15 (see [LMF13, Global Number Field 4.0.514089.1]). Let M be its maximal unramified abelian 5-extension. Note that the class number of both $\mathbb{Q}(\sqrt{717})$ and $\mathbb{Q}(\sqrt{-3})$ is 1. Therefore, M is a Galois extension of both $\mathbb{Q}(\sqrt{717})$ and $\mathbb{Q}(\sqrt{-3})$ with $\mathrm{Gal}(M/\mathbb{Q}(\sqrt{-3})) \simeq \mathrm{Gal}(M/\mathbb{Q}(\sqrt{717})) \simeq D_5$. In these cases, Corollary 1.6 gives us the following results:

Corollary 1.7. *Let* $\chi : \mathrm{Gal}(M/\mathbb{Q}(\sqrt{-3}, \sqrt{-239}) \to \mathbb{F}_{81}^*$ *be a non-trivial continuous character.*

(a) Let $\overline{\rho}_1 : G_{\mathbb{Q}(\sqrt{717})} \to \mathrm{GL}_2(\mathbb{F}_{81})$ *be the representation* $\mathrm{Ind}_{\mathrm{Gal}(M/L)}^{\mathrm{Gal}(M/\mathbb{Q}(\sqrt{717}))}(\chi)$*. Let* S *be a finite set of primes of* $\mathbb{Q}(\sqrt{717})$ *such that* $S_\infty \subseteq S$*,* S *does not contain any prime above* 3*, and all the finite primes contained in* S *are split in* L *but not completely split in* M*. Then the universal deformation of* $\overline{\rho}_1$ *relatively unramified outside* S *has finite image.*

(b) Let $\overline{\rho}_2 : G_{\mathbb{Q}(\sqrt{-3})} \to \mathrm{GL}_2(\mathbb{F}_{81})$ *be the representation* $\mathrm{Ind}_{\mathrm{Gal}(M/L)}^{\mathrm{Gal}(M/\mathbb{Q}(\sqrt{-3}))}(\chi)$*. Let* S *be a finite set of primes of* $\mathbb{Q}(\sqrt{-3})$ *such that* $S_\infty \subseteq S$*,* S *does not contain any prime above* 3*, and all the finite primes contained in* S *are split in* L *but not completely split in* M*. Then the universal deformation of* $\overline{\rho}_2$ *relatively unramified outside* S *has finite image.*

Note that Boston's conjecture has been proved by Allen and Calegari for a certain class of representations of the absolute Galois groups of totally real fields (see [AC14, Corollary 3]). However, the two cases considered above do not satisfy the hypotheses of [AC14, Corollary 3] and, hence, they give us new evidence towards Boston's strengthening of the unramified Fontaine-Mazur conjecture.

In section 5, we report on some computer calculations that we carried out to obtain examples when the universal relatively unramified deformation of $\overline{\rho}$ is dihedral, and others when this is not the case. Those examples for which the universal relatively unramified deformation is dihedral also provide explicit examples in favour of Boston's strengthening of the unramified Fontaine-Mazur conjecture.

1.3 Modularity results

We apply our number theoretic results towards a comparison between a minimal universal deformation ring and a Hecke algebra in parallel weight one. The main point is that, when K is totally real, irreducible totally odd induced representations of finite order complex-valued characters are afforded by cuspidal Hilbert modular forms of parallel weight one that are induced from the corresponding Hecke character.

We keep the objects from the previous subsection and impose several additional hypotheses that are natural in view of the application to Hilbert modular forms and the previous results.

1. $p > 2$.
2. K is totally real.
3. the character $\overline{\chi}$ is such that $\overline{\rho}$ is totally odd.
4. $\overline{\rho}$ is unramified at all places above p.
5. If $\overline{\rho}$ is ramified at a prime ℓ of K and $\overline{\rho}|_{G_{K_\ell}}$ is not absolutely irreducible, then $\dim((\overline{\rho})^{I_\ell}) = 1$ where $(\overline{\rho})^{I_\ell}$ denotes the subspace of $\overline{\rho}$ fixed by the inertia group I_ℓ at ℓ.
6. $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$ (cf. Theorem 1.5).

Let $\mathbb{T}$ be the full Hecke algebra acting faithfully on the span of an explicit set of modular forms of parallel weight one the attached Galois representations of which lift $\overline{\rho}$ (see Definition 4.4 for a precise statement). By patching the Galois representations of these modular forms, a standard argument gives rise to a Galois representation $\rho_{\mathbb{T}} : G_K \to \mathrm{GL}_2(\mathbb{T})$ the determinant of which is the Teichmüller lift of $\det \circ \overline{\rho}$ and such that traces of Frobenius match Hecke operators in the usual way (see Proposition 4.5).

On the deformation theory side, we shall restrict to *minimal deformations* (see Definition 4.9), defined in the same way as in [CG18, Definition 3.1]. It turns out that $\rho_{\mathbb{T}}$ is such a minimal deformation of $\overline{\rho}$. Moreover, we find that there is an explicit choice for the set of places S such that $R^{\min} = (R_S^{\mathrm{univ}})^0$ (see Proposition 4.10), where $R^{\min}$ is the universal minimal deformation ring of $\overline{\rho}$ and $(R_S^{\mathrm{univ}})^0$ is the ring underlying $(\rho_S^{\mathrm{univ}})^0$. Applying this together with Theorem 1.5 leads to our main modularity result.

Theorem 1.8. *The map $\phi_{\mathbb{T}} : R^{\min} \to \mathbb{T}$ induced from the minimal deformation $\rho_{\mathbb{T}}$ of $\overline{\rho}$, constructed in Proposition 4.5, is an isomorphism.*

Finally, we discuss a relation between more general '$R^{\min} = \mathbb{T}$'-statements and the (non-)liftability of parallel weight one Hilbert modular forms in Remark 4.16.

1.4 Notation and conventions

We summarise some notation and conventions to be used throughout the paper. More notation is introduced during the text.

For a finite field $\mathbb{F}$, denote by $W(\mathbb{F})$ the ring of Witt vectors of $\mathbb{F}$. Let $\mathcal{C}$ be the category of local complete Noetherian $W(\mathbb{F})$-algebras R with residue field $\mathbb{F}$. The Teichmüller lift of an element $x \in \mathbb{F}$ to $W(\mathbb{F})$ (and to any $W(\mathbb{F})$-algebra) will be denoted by a hat: $\hat{x}$. All representations are assumed to be continuous without explicit mention of this. For a local ring R, denote by $\mathfrak{m}_R$ its maximal ideal.

Specific objects that are used without explicit mention in the statements of propositions and theorems are collected in 'set-up's'.

Set-up 1.9. *In the entire article, p will denote a fixed prime number and $\mathbb{F}$ a finite field of characteristic p.*

1.5 Acknowledgements

G. W. is partially supported by the IRP AMFOR at the University of Luxembourg.

2 Representation theory

In this section, we develop and prove the representation theory results outlined in section 1.1.

2.1 Explicit universal deformations of characters

Since dihedral representations are induced from characters, we first include a treatment of the universal deformation of a character. It can be derived from Mazur's fundamental paper [Maz89, §1.4], but due to its simplicity, we prefer to include a proof.

For $r \in \mathbb{N}$ and n-tuples of positive integers $(e_1, e_2, \ldots, e_n)$ we introduce the piece of notation

$$\mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)} := W(\mathbb{F})[[X_1, \ldots, X_{n+r}]]/((1+X_1)^{p^{e_r}} - 1, \ldots, (1+X_n)^{p^{e_n}} - 1).$$

Proposition 2.1. *Let H be a profinite group. We assume that the pro-p group $P = \prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z} \times \mathbb{Z}_p^r$ with $e_i \geq 1$ for all $1 \leq i \leq n$ is the maximal continuous abelian pro-p quotient of H. Let $g_1, \ldots, g_{n+r}$ be generators of P such that g_i topologically generates $\mathbb{Z}/p^{e_i}\mathbb{Z}$ for $1 \leq i \leq n$ and $\mathbb{Z}_p$ for $n+1 \leq i \leq n+r$.*

Let $\overline{\chi} : H \to \mathbb{F}^\times$ be a character and denote by $\widehat{\overline{\chi}} : H \to W(\mathbb{F})^\times$ its Teichmüller lift. Define the character $\psi^{\mathrm{univ}} : H \to \mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)}$ as the composition of the projection $H \twoheadrightarrow P$ and the group monomorphism $P \to \left(\mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)}\right)^\times$ sending g_i to $1 + X_i$ for $i = 1, \ldots, n+r$. Also define the universal character

$$\chi^{\mathrm{univ}} := \psi^{\mathrm{univ}} \cdot \widehat{\overline{\chi}}.$$

Then $\mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)}$ is the universal deformation ring of $\overline{\chi}$ in the category $\mathcal{C}$ and χ^{univ} is the universal deformation.

Proof. It is a simple check that χ^{univ} is well-defined and indeed a deformation of $\overline{\chi}$. Let now R be in $\mathcal{C}$ and $\chi : H \to R^\times$ a deformation of $\overline{\chi}$. We set $\psi := \chi \cdot \widehat{\overline{\chi}}^{-1}$. As the reduction of ψ is trivial, its image is a pro-p group and thus a quotient of P. We write this as $\psi : H \twoheadrightarrow P \overset{\pi}{\twoheadrightarrow} \mathrm{im}(\psi) \subseteq R^\times$.

We define the $W(\mathbb{F})$-algebra homomorphism

$$W(\mathbb{F})[[X_1, \ldots, X_{n+r}]] \to R, \quad X_1 \mapsto \pi(g_1) - 1, \ldots, X_{n+r} \mapsto \pi(g_{n+r}) - 1.$$

The elements $(1+X_1)^{p^{e_1}} - 1, \ldots, (1+X_n)^{p^{e_n}} - 1$ are clearly in its kernel so that we obtain a $W(\mathbb{F})$-algebra homomorphism

$$\phi : \mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)} \to R.$$

The commutativity of the diagram

$$\begin{tikzcd}
 & & \left(\mathcal{U}_{W(\mathbb{F}),(e_1,e_2,\ldots,e_n)}\right)^\times \arrow[dd, "\phi"] \\
H \arrow[r, two heads] \arrow[urr, bend left, "\psi^{\mathrm{univ}}"] \arrow[drr, bend right, "\psi"'] & P \arrow[ur] \arrow[dr] & \\
 & & R^\times
\end{tikzcd}$$

is clear. It implies $\chi = \phi \circ \chi^{\mathrm{univ}}$. The uniqueness of ϕ with this property is clear. All this together shows the universality of $(\mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)}, \chi^{\mathrm{univ}})$. $\square$

2.2 Dihedral representations

We start by clarifying what we mean by induced and dihedral representations in the special cases we need.

Definition 2.2. *Let G be a profinite group and R a topological ring. A representation $\rho : G \to \mathrm{GL}_2(R)$ is called* dihedral *if there is an open index-2 subgroup $H \lhd G$ and a character $\chi : H \to R^\times$ such that ρ is equivalent to $\mathrm{Ind}_H^G(\chi)_R$, where the free R-module of rank 2*

$$\mathrm{Ind}_H^G(\chi)_R = \{f : G \to R \text{ map} \mid \forall\, g \in G, \forall\, h \in H : f(hg) = \chi(h)f(g)\}$$

is the induced representation of χ from H to G *equipped with the left G-action via $(\tilde{g}.f)(g) = f(g\tilde{g})$ for $g, \tilde{g} \in G$.*

We stress that in the definition we ask the character χ to be defined over R. This choice may not be standard, but can always be achieved by extending R. It simplifies working matricially with induced representations.

For the sake of being explicit and making certain proofs more transparent, we quickly describe a matrix representation of $\rho = \mathrm{Ind}_H^G(\chi)_R$. Let us write $G = H \sqcup \sigma H$ and put $\chi^\sigma(h) = \chi(\sigma h \sigma^{-1})$ for $h \in H$. Then with respect to a natural choice of basis, for $h \in H$, we have

$$\rho(h) = \begin{pmatrix} \chi(h) & 0 \\ 0 & \chi^\sigma(h) \end{pmatrix} \text{ and } \rho(\sigma h) = \begin{pmatrix} 0 & \chi^\sigma(h) \\ \chi(h)\chi(\sigma^2) & 0 \end{pmatrix}. \tag{2.2}$$

The name *dihedral representation* is justified because an irreducible representation $\overline{\rho} : G \to \mathrm{GL}_2(\mathbb{F})$ with $\mathbb{F}$ a finite field is dihedral if and only if its projective image is a dihedral group (after possibly replacing $\mathbb{F}$ by a finite extension).

For a representation $\rho : G \to \mathrm{GL}_2(R)$ we define the adjoint representations $\mathrm{ad}(\rho)_R$ and $\mathrm{ad}^0(\rho)_R$ as the representations given by the conjugacy of ρ on $M_2(R)$ and $M_2^0(R)$, respectively, where $M_2(R)$ are the 2×2-matrices with coefficients in R and $M_2^0(R)$ is its subset consisting of the matrices having trace 0.

From now on, we assume the following set-up.

Set-up 2.3. *Let G be a profinite group, $H \lhd G$ an open subgroup of index 2 and $\sigma \in G \setminus H$.*

Definition 2.4. *(a) For an extension of topological rings $R \subseteq R'$, a character $\epsilon : G \to R^\times$ and a character $\chi : H \to R^\times$, we make the following definitions:*

- *$C(\epsilon)_{R'}$ is R' with G-action through ϵ; in particular, $C(1)_{R'}$ is the trivial module;*
- *$C(\chi)_{R'}$ is R' with H-action through χ;*
- *$N_{R'}$ is ${R'}^2$ with trivial H-action and σ acting by swapping the two standard basis vectors;*
- *$I(\chi)_{R'} = \mathrm{Ind}_H^G(\chi)_{R'}$, as described in Definition 2.2.*

(b) In the case of finite fields of characteristic $p > 0$, we sometimes drop minimal fields of definition from the notation. In particular, we write $C(1) := C(1)_{\mathbb{F}_p}$, $C(\epsilon) := C(\epsilon)_{\mathbb{F}_p}$ if ϵ is at most quadratic, $N := N_{\mathbb{F}_p}$ and $I(\chi) := I(\chi)_{F_0}$ if F_0 is the extension of $\mathbb{F}_p$ generated by the coefficients of all occurring characteristic polynomials.

Lemma 2.5. *Let R be a topological ring and let $\rho \cong \operatorname{Ind}_H^G(\chi)_R$ for some character $\chi : H \to R^\times$. Choose a basis of R^2 such that as in (2.2) under this basis, $\rho(h)$ is diagonal for all $h \in H$. Then, under the choice of this basis, the map*

$$\operatorname{ad}(\rho)_R \to N_R \oplus I(\chi/\chi^\sigma)_R, \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a \\ d \end{smallmatrix}\right) \oplus \left(\begin{smallmatrix} b \\ c \end{smallmatrix}\right)$$

is an isomorphism of $R[G]$-modules. Moreover, one has an isomorphism of $R[G]$-modules

$$\operatorname{ad}^0(\rho)_R \cong C(\epsilon)_R \oplus I(\chi/\chi^\sigma)_R,$$

where $\epsilon : G \twoheadrightarrow G/H \twoheadrightarrow \{\pm 1\} \subseteq R^\times$. Furthermore, if 2 is invertible in R, then N_R is isomorphic to $C(1)_R \oplus C(\epsilon)_R$ as $R[G]$-modules. Finally, the exact sequence of $R[G]$-modules

$$0 \to \operatorname{ad}^0(\rho)_R \to \operatorname{ad}(\rho)_R \xrightarrow{\operatorname{tr}} C(1)_R \to 0$$

is split if 2 is invertible in R with split $r \mapsto \begin{pmatrix} r/2 & 0 \\ 0 & r/2 \end{pmatrix}$.

Proof. These are elementary calculations. □

Set-up 2.6. *In addition to Set-up 2.3, let $\overline{\chi} : H \to \mathbb{F}^\times$ be a character such that $\overline{\chi} \neq \overline{\chi}^\sigma$, where $\overline{\chi}^\sigma(h) = \overline{\chi}(\sigma h \sigma^{-1})$ for $h \in H$ is the conjugate character. Let $\overline{\rho} : G \to \mathrm{GL}_2(\mathbb{F})$ be $\operatorname{Ind}_H^G(\overline{\chi})_{\mathbb{F}}$. By the assumption $\overline{\chi} \neq \overline{\chi}^\sigma$, the representation $\overline{\rho}$ is absolutely irreducible. We also use the following pieces of notation:*

$$\overline{G} = \overline{\rho}(G), \;\; \overline{H} = \overline{\rho}(H), \;\; \overline{G}^{\mathrm{ad}} = \operatorname{ad}(\overline{\rho})(G), \;\; \overline{H}^{\mathrm{ad}} = \operatorname{ad}(\overline{\rho})(H), \;\; C := \ker(\overline{G} \twoheadrightarrow \overline{G}^{\mathrm{ad}}).$$

Note that $\overline{G}^{\mathrm{ad}}$ is a quotient of $\overline{G}$ and $\overline{H}^{\mathrm{ad}}$ is a quotient of $\overline{H}$. Furthermore,

$$C = \ker(\overline{G} \twoheadrightarrow \overline{G}^{\mathrm{ad}}) = \ker(\overline{H} \twoheadrightarrow \overline{H}^{\mathrm{ad}}) \subseteq \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in \mathbb{F}^\times\}$$

and $\overline{G}^{\mathrm{ad}}$ is isomorphic to the image of $\operatorname{Ind}_H^G(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}$. If $\overline{\chi}/\overline{\chi}^\sigma = \overline{\chi}^\sigma/\overline{\chi}$, then $I(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}} = C(\overline{\chi}_1)_{\mathbb{F}} \oplus C(\overline{\chi}_2)_{\mathbb{F}}$ for some characters $\overline{\chi}_1, \overline{\chi}_2 : G \to \mathbb{F}^\times$. We will keep this notation for the rest of the section.

In the sequel, we will make frequent use of the Krull-Schmidt-Azumaya theorem ([CR81, (6.12)]) allowing us to express modules over group rings of finite groups uniquely as direct sums of indecomposables.

Lemma 2.7. *(a) The simple $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-modules occurring in $\operatorname{ad}(\overline{\rho})_{\mathbb{F}}$ are $C(1)$, $C(\overline{\chi}/\overline{\chi}^\sigma)$, $C(\overline{\chi}^\sigma/\overline{\chi})$. Every indecomposable $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module is simple.*

(b) *If $p > 2$, then the simple $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules occurring in $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$ are $C(1)$, $C(\epsilon)$ and $I(\overline{\chi}/\overline{\chi}^{\sigma})$ (or $C(\overline{\chi}_1)$ and $C(\overline{\chi}_2)$ for some characters $\overline{\chi}_1, \overline{\chi}_2 : \overline{G}^{\mathrm{ad}} \to \mathbb{F}^{\times}$ if $\overline{\chi}/\overline{\chi}^{\sigma} = \overline{\chi}^{\sigma}/\overline{\chi}$). Every indecomposable $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module is simple.*

(c) *For $p = 2$, the simple $\mathbb{F}_2[\overline{G}^{\mathrm{ad}}]$-modules occurring as Jordan-Hölder factors of $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$ are $C(1)$ and $I(\overline{\chi}/\overline{\chi}^{\sigma})$. The only indecomposable non-simple $\mathbb{F}_2[\overline{G}^{\mathrm{ad}}]$-module the composition factors of which are in $\{C(1), I(\overline{\chi}/\overline{\chi}^{\sigma})\}$ is N.*

Proof. (a,b) Since $p \nmid \#\overline{H}^{\mathrm{ad}}$ and $p \nmid \#\overline{G}^{\mathrm{ad}}$ if $p > 2$, by Maschke's theorem [CR81, Theorem 3.14] every indecomposable module is simple. Lemma 2.5 gives the list of occurring simple modules. Note that $I(\overline{\chi}/\overline{\chi}^{\sigma})$ is simple if and only if $(\overline{\chi}/\overline{\chi}^{\sigma})^2 \neq 1$. Note also that we use that $C(\epsilon)_{\mathbb{F}} \cong C(\epsilon) \otimes_{\mathbb{F}_p} \mathbb{F} \cong C(\epsilon)^{[\mathbb{F}:\mathbb{F}_p]}$ and $I(\overline{\chi}/\overline{\chi}^{\sigma})_{\mathbb{F}} \cong I(\overline{\chi}/\overline{\chi}^{\sigma})^{[\mathbb{F}:F_0]}$ (in the notation of Definition 2.4) as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules, and similarly for the other modules and over $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$.

(c) The list of simple modules from (b) is also valid for $p = 2$. Note that the Jordan-Hölder factors of N are all $C(1)$. By assumption we have $\overline{\chi}/\overline{\chi}^{\sigma} \neq \overline{\chi}^{\sigma}/\overline{\chi}$ (since $p = 2$). Let V be an indecomposable non-simple $\mathbb{F}_2[\overline{G}^{\mathrm{ad}}]$-module the composition factors of which occur as Jordan-Hölder factors of $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$. We first decompose V as $\mathbb{F}_2[\overline{H}^{\mathrm{ad}}]$-module into

$$V \cong C(1)^{r_1} \oplus C(\overline{\chi}/\overline{\chi}^{\sigma})^{r_2} \oplus C(\overline{\chi}^{\sigma}/\overline{\chi})^{r_3}.$$

This decomposition can be considered as a decomposition into simultaneous eigenspaces for the H-action. Note that G permutes the occurring simultaneous eigenspaces. More precisely, it stabilises $C(1)^{r_1}$ and $\sigma\big(C(\overline{\chi}/\overline{\chi}^{\sigma})\big) = C(\overline{\chi}^{\sigma}/\overline{\chi})$. So $r_2 = r_3$ follows and thus $V \cong C(1)^{r_1} \oplus I(\overline{\chi}/\overline{\chi}^{\sigma})^{r_2}$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules. By the indecomposable non-simple assumption $V \cong C(1)^{r_1}$, i.e. V is $\mathbb{F}_2^{r_1}$ with trivial H-action and an involutive action by σ. Due to the indecomposability, in the Jordan normal form of σ on V there can only be a single Jordan block. This block has to have size 1 or 2 as otherwise the order of σ would be larger than 2. As V is non-simple, the block size has to be 2 and V is thus isomorphic to N. □

Although we formulate the following corollary for all primes p, it is only non-trivial for $p = 2$.

Corollary 2.8. *Any indecomposable $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module the composition factors of which are among those of $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$ is a submodule of $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$.*

Proof. This follows immediately from Lemma 2.7. □

Let $R \in \mathcal{C}$, $\rho : G \to \mathrm{GL}_2(R)$ be a lift of $\overline{\rho}$ and Γ_ρ be defined by the diagram (1.1).

Lemma 2.9. *(a) The lower exact sequence in* (1.1) *splits, as indicated in the diagram.*

(b) *There is an R-basis of ρ such that for all $h \in H$ one has*

$$s \circ \overline{\rho}(h) = \begin{pmatrix} \widehat{\overline{\chi}}(h) & 0 \\ 0 & \widehat{\overline{\chi}}^{\sigma}(h) \end{pmatrix},$$

where the hat indicates the Teichmüller lift. In particular, $s \circ \overline{\rho}(h)$ is scalar if $\overline{\rho}(h)$ is scalar. Thus the conjugation action of $\overline{H}$ on Γ_ρ via s descends to $\overline{H}^{\mathrm{ad}}$.

(c) If $p > 2$, the upper sequence in (1.1) *splits, leading to a conjugation action of $\overline{G}$ on Γ_ρ, which descends to $\overline{G}^{\mathrm{ad}}$.*

(d) If Γ_ρ is abelian (for instance, if $\mathfrak{m}_R^2 = 0$), then via choices of preimages the group $\overline{G}$ acts on Γ_ρ via conjugation, and this action descends to $\overline{G}^{\mathrm{ad}}$.

Proof. The splitting of the exact sequences in (a) and (c) follows from the theorem of Schur-Zassenhaus [Asc93, (18.1)] since the group orders of $\overline{H}$ (resp. $\overline{G}$) are coprime to the order of Γ_ρ.

(b) By its explicit description, $\mathbb{F}^2$ has a basis consisting of simultaneous eigenvectors for $\overline{H}$; the eigenvalues are distinct for some matrices due to the assumption that $\overline{\rho}$ is irreducible. Let a, b be two such distinct eigenvalues, occurring for some $\overline{\rho}(h)$. The order n of $\overline{\rho}(h)$ is not divisible by p. Hence the polynomial $X^n - 1$ annihilates $\overline{\rho}(h)$ (and also $s \circ \overline{\rho}(h)$) and factors into n distinct coprime factors over $\mathbb{F}$. Then so it does over R i.e.

$$X^n - 1 = (X - \hat{a})(X - \hat{b})f(X)$$

for some $f \in R[X]$. Denote by $\overline{f} \in \mathbb{F}[X]$ the reduction of f modulo $\mathfrak{m}_R$. As $\det(\overline{f}(\overline{\rho}(h)))$ is invertible in $\mathbb{F}$, also $f(s \circ \overline{\rho}(h))$ is invertible. Consequently $(X - \hat{a})(X - \hat{b})$ annihilates $s \circ \overline{\rho}(h)$. As the two polynomials $(X - \hat{a})$ and $(X - \hat{b})$ are coprime, the representation space R^2 of ρ is the direct sum of the eigenspaces of $s \circ \overline{\rho}(h)$ for the eigenvalues $\hat{a}$ and $\hat{b}$. By Nakayama's lemma, each of these eigenspaces is a non-trivial quotient of R and each eigenspace is generated by one element over R as this is the case over $\mathbb{F}$. This leads to a surjection $R^2 \to R^2$ of Noetherian modules, which is hence an isomorphism, showing that the each eigenspace is free of rank 1 as R-module.

(c) The action descends to $\overline{G}^{\mathrm{ad}}$ because the kernel C of $\overline{G} \to \overline{G}^{\mathrm{ad}}$ acts through scalar matrices due to (b).

(d) is clear as by part (b), the action descends to $\overline{G}^{\mathrm{ad}}$. □

2.3 Characterisation of dihedral representations by Frattini quotients

For a pro-p group Γ we denote by $\Phi(\Gamma)$ its p-Frattini subgroup, that is, the closure of $\Gamma^p[\Gamma, \Gamma]$ in Γ. The quotient $\Gamma/\Phi(\Gamma)$ will be called the p-Frattini quotient. It can be characterised as the largest continuous quotient of Γ that is an elementary abelian p-group. Note that the p-Frattini subgroup is a characteristic subgroup and the actions on Γ_ρ from Lemma 2.9 induce actions on the p-Frattini quotient.

The key input for characterising dihedral deformations is the following fact from group theory.

Proposition 2.10. *Let Γ be a pro-p group and let $A \subseteq \mathrm{Aut}(\Gamma)$ be a finite subgroup of order coprime to p. Then the natural map $A \to \mathrm{Aut}(\Gamma/\Phi(\Gamma))$ is injective.*

Proof. The version for a finite p-group Γ is proved in [Asc93, (24.1)]. To see the statement for pro-p groups, consider an automorphism α of G that is trivial on $\Gamma/\Phi(\Gamma)$. By the result for finite p-groups, α is then also trivial on any finite quotient Γ' of Γ because $\Gamma'/\Phi(\Gamma')$ is a quotient of $\Gamma/\Phi(\Gamma)$. Consequently, α is trivial on Γ. □

We can now prove the characterisation of dihedral representations via Frattini quotients. We continue to use the notation introduced above.

Proof of Theorem 1.1. Before starting the proof of the equivalences, let us prove the implication mentioned in item (ii): if the action of $\overline{H}^{\mathrm{ad}}$ on Γ_ρ is trivial, then so is the action of $\overline{H}$; as this action is by conjugation via the split, $s(\overline{H})$ and Γ_ρ commute, leading to $\rho(H) = \Gamma_\rho \times s(\overline{H})$.

Next, we apply Proposition 2.10, yielding the equivalence of (ii) and (iii).

Let us assume (i). From the matricial description of ρ in (2.2) we see that $\rho(H)$ sits in the diagonal matrices and is hence abelian. Thus the conjugation action by $\overline{H}$ on Γ_ρ is trivial, showing (ii).

Let us now assume (ii). As already seen, we then have $\rho(H) = \Gamma_\rho \times s(\overline{H})$. We choose an R-basis v_1, v_2 as in Lemma 2.9 (b). For this basis of R^2, the matrices representing elements in Γ_ρ have to be diagonal as well, as any matrix commuting with a non-scalar diagonal matrix with unit entries is diagonal itself. This implies that Γ_ρ is an abelian pro-p group. We can thus see Γ_ρ as being given by two characters $\psi_1, \psi_2 : H \to R^\times$, i.e. $\rho(h) = \left(\begin{smallmatrix} \psi_1(h)\widehat{\overline{\chi}}(h) & 0 \\ 0 & \psi_2(h)\widehat{\overline{\chi}}^\sigma(h) \end{smallmatrix}\right)$ for $h \in H$. Moreover, conjugation by $\rho(\sigma)$ swaps the two simultaneous eigenvectors, proving $\psi_2 = \psi_1^\sigma$. The matricial description of induced representations in (2.2) immediately implies (i). $\square$

Lemma 2.11. *Let $R \in \mathcal{C}$ and $\rho : G \to \mathrm{GL}_2(R)$ a lift of $\overline{\rho}$. As before, define $\Gamma = \Gamma_\rho = \ker\big(\mathrm{im}(\rho) \twoheadrightarrow \mathrm{im}(\overline{\rho})\big)$. For $k \in \mathbb{Z}_{\geq 1}$, also define $\Gamma_k = \mathrm{im}\big(\Gamma \hookrightarrow \mathrm{im}(\rho) \twoheadrightarrow \mathrm{im}(\rho \mod \mathfrak{m}_R^k)\big)$.*

Then $\Gamma = \varprojlim_k \Gamma_k$ and we have $\overline{G}^{\mathrm{ad}}$-equivariantly:

$$\ker\big(\Gamma_k \twoheadrightarrow \Gamma_{k-1}\big) \subseteq 1 + M_2(\mathfrak{m}_R^{k-1}/\mathfrak{m}_R^k) \xrightarrow[\sim]{1+A \mapsto A} M_2(\mathbb{F})^{r_k},$$

where $r_k = \dim_{\mathbb{F}} \mathfrak{m}_R^{k-1}/\mathfrak{m}_R^k$. Moreover, if $\det(\rho)$ is the Teichmüller lift of $\det(\overline{\rho})$, then $\ker\big(\Gamma_k \twoheadrightarrow \Gamma_{k-1}\big)$ is contained in $M_2^0(\mathbb{F})^{r_k}$.

Proof. The first statement is clear. The inclusion in the second statement is a consequence of the fact that the kernel of the projection $\pi_k : \mathrm{GL}_2(R/\mathfrak{m}_R^k) \twoheadrightarrow \mathrm{GL}_2(R/\mathfrak{m}_R^{k-1})$ is given by $1 + M_2(\mathfrak{m}_R^{k-1}/\mathfrak{m}_R^k)$. Furthermore, note that $\overline{G}$ acts on $\ker\big(\Gamma_k \twoheadrightarrow \Gamma_{k-1}\big)$ for any k by conjugation with a preimage in $\mathrm{im}(\rho)$ and that this action is independent of the choice of preimage because conjugation by $1 + M_2(\mathfrak{m}_R)$ on $\ker\big(\Gamma_k \twoheadrightarrow \Gamma_{k-1}\big)$ is trivial. Thus, by Lemma 2.9, the action descends indeed to an action of $\overline{G}^{\mathrm{ad}}$. The $\overline{G}^{\mathrm{ad}}$-equivariance and the final assertion follow from simple calculations $\square$

Corollary 2.12. *The indecomposable $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules occurring in $\Gamma_\rho/\Phi(\Gamma_\rho)$ are submodules of the adjoint representation $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$, that is, they are isomorphic to $C(1)$, $C(\epsilon)$, $I(\overline{\chi}/\overline{\chi}^\sigma)$ (or $C(\overline{\chi}_1)$, $C(\overline{\chi}_2)$ if $\overline{\chi}/\overline{\chi}^\sigma = \overline{\chi}^\sigma/\overline{\chi}$) or, if $p = 2$, the unique non-trivial extension N of $C(1)$ by itself.*

In particular, as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module, $\Gamma_\rho/\Phi(\Gamma_\rho)$ is isomorphic to $C(1)^r \oplus I(\overline{\chi}/\overline{\chi}^\sigma)^s$ (or to $C(1)^r \oplus C(\overline{\chi}/\overline{\chi}^\sigma)^s$ if $\overline{\chi}/\overline{\chi}^\sigma = \overline{\chi}^\sigma/\overline{\chi}$) for some $r, s \in \mathbb{N}$, and, thus, the $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-action on $\Gamma_\rho/\Phi(\Gamma_\rho)$ is trivial if and only if $s = 0$.

Proof. This follows from Lemmata 2.11, 2.7 and Corollary 2.8. $\square$

Note that the conclusion is in terms of $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-representations, not $\mathbb{F}[\overline{G}^{\mathrm{ad}}]$-representations because it is not clear (and usually wrong) that $\Gamma_\rho/\Phi(\Gamma_\rho)$ has the structure of $\mathbb{F}$-vector space.

2.4 The infinitesimal quotient of the universal representation

The previous computations are valid for all representations. In this subsection we specialise to the universal representation because for it we can replace the Frattini quotient by an infinitesimal deformation.

Lemma 2.13. *Let $\rho : G \to \mathrm{GL}_2(R)$ be an infinitesimal deformation of $\overline{\rho}$. Then $\mathfrak{m}_R$ is an $\mathbb{F}$-vector space of some finite dimension r and we have the inclusion of $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules $\Gamma_\rho \subseteq \mathrm{ad}(\overline{\rho})^r_{\mathbb{F}}$.*

Proof. The kernel Γ_ρ of reduction modulo $\mathfrak{m}_R$ clearly sits in $M_2(\mathfrak{m}_R)$, proving the result. □

We now prove a converse of Corollary 2.12. In the case $p = 2$, the lower exact sequence in (1.1) need not split. This is taken into account in the following proposition.

Proposition 2.14. *Let Z be an elementary abelian p-group and consider a group extension*

$$0 \to Z \to \mathcal{G} \to \overline{G} \to 0,$$

giving Z the structure of $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module. Assume that Z is an indecomposable $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module occurring in $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$ (see Lemma 2.7).

Then there is a lift $\rho_Z : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ of $\overline{\rho}$ such that $\mathrm{im}(\rho_Z) \cong \mathcal{G}$ and $Z \cong \Gamma_{\rho_Z}$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules.

The group extension is split in all cases except possibly if $p = 2$ and $Z = C(1) = \mathbb{F}_2$. In that case, there are two non-isomorphic extensions.

Proof. In order to compute the possible group extensions, we first observe that since the order of $\overline{H}$ is invertible in Z, by inflation-restriction [NSW08, Proposition 1.6.7] we obtain an isomorphism

$$\mathrm{H}^2(\overline{G}, Z) \cong \mathrm{H}^2(\overline{G}/\overline{H}, Z^{\overline{H}}).$$

For $p > 2$, the latter group is always zero because 2 is invertible in the $\mathbb{F}_p$-vector space $Z^{\overline{H}}$. Thus the group extension in question is always split.

For $p = 2$, we analyse the three possibilities for Z (see Lemma 2.7) individually. As $I(\overline{\chi}/\overline{\chi}^\sigma)^{\overline{H}} = 0$, we find $\mathrm{H}^2(\overline{G}, I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$ and the corresponding group extension is split. In order to compute the result for N, we make use of the fact that for a cyclic group H^2 is isomorphic to the 0-th Tate (or modified) cohomology group (see e.g. [NSW08, §1.2]), which can be described explicitly. More precisely,

$$\mathrm{H}^2(\overline{G}, N) \cong \mathrm{H}^2(\overline{G}/\overline{H}, N) \cong \hat{\mathrm{H}}^0(\overline{G}/\overline{H}, N) = N^{\overline{G}/\overline{H}}/(1+\sigma)N = N^{\overline{G}}/(1+\sigma)N \cong \mathbb{F}_2/\mathbb{F}_2 = 0,$$

so that also the corresponding group extension is split. With the same arguments, the case $Z = C(1) = \mathbb{F}_2$ leads to

$$\mathrm{H}^2(\overline{G}, \mathbb{F}_2) \cong \mathbb{F}_2/(1+\sigma)\mathbb{F}_2 = \mathbb{F}_2.$$

Consequently, there are two non-isomorphic group extensions of $\overline{G}$ by $\mathbb{F}_2$.

In all cases except when $p = 2$, $Z = \mathbb{F}_2$ and the sequence is non-split, we can proceed as follows. We have the exact sequence of groups

$$\begin{tikzcd} 0 \arrow[r] & M_2(\mathbb{F}) \arrow[r] & \mathrm{GL}_2(\mathbb{F}[X]/(X^2)) \arrow[r] & \mathrm{GL}_2(\mathbb{F}) \arrow[r] \arrow[l, bend left, "s"] & 0 \\ & Z \arrow[u, hook] & & \overline{G} \arrow[u, hook] & \end{tikzcd}$$

and the action of $\overline{G}^{\mathrm{ad}}$ on Z induced from this exact sequence is the action on Z as a submodule of $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$. We can thus simply obtain the split group extension of $\overline{G}$ by Z as the subgroup of $\mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ generated by Z and $s(\overline{G})$.

In order to treat the remaining case $p = 2$, $Z = \mathbb{F}_2$ and the sequence is non-split, we make use of the case $p = 2$, $Z = N$, where, as in Lemma 2.5, we view $N = 1 + X\{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in M_2(\mathbb{F}) \mid a, d \in \mathbb{F}_2\}$. We now define the group $\mathcal{G}' \subset \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ as the group generated by $s(\overline{H})$, the scalars $\mathbb{F}_2 = 1 + X\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \in M_2(\mathbb{F}) \mid a \in \mathbb{F}_2\} \subset N$ and the element $\left(\begin{smallmatrix} 0 & 1+X \\ \overline{\chi}(\sigma^2) & 0 \end{smallmatrix}\right)$. Let n be the order of $\overline{\chi}(\sigma^2)$ in $\mathbb{F}^\times$. Reducing the matrices in $\mathcal{G}'$ modulo X, we clearly obtain $\overline{G}$ and we have that the kernel of the reduction map is $\mathbb{F}_2$. Moreover, the element $\left(\begin{smallmatrix} 0 & 1+X \\ \overline{\chi}(\sigma^2) & 0 \end{smallmatrix}\right)$ is a lift of $\overline{\rho}(\sigma)$, but it has order $4n$, contrary to the split case which does not contain any element of order $4n$. This shows that $\mathcal{G}'$ is an explicit realisation of the non-split group extension, whence $\mathcal{G}' \cong \mathcal{G}$. □

Set-up 2.15. *In the context of Set-ups 2.3 and 2.6, assume now also that G satisfies Mazur's finiteness condition Φ_p (see [Maz89, §1.1]).*

Since $\overline{\rho}$ is irreducible, the deformation functor for the category $\mathcal{C}$ is representable (see [Maz89, §1.2])). One thus has a universal deformation

$$\rho^{\mathrm{univ}} : G \to \mathrm{GL}_2(R^{\mathrm{univ}}).$$

Write $\mathfrak{m}_{\mathrm{univ}}$ for $\mathfrak{m}_{R^{\mathrm{univ}}}$ and $\rho^{\mathrm{univ}}_{\mathrm{inf}} := (\rho^{\mathrm{univ}})_{\mathrm{inf}}$, as well as $\Gamma^{\mathrm{univ}} := \Gamma_{\rho^{\mathrm{univ}}}$ and $\Gamma^{\mathrm{univ}}_{\mathrm{inf}} := \Gamma_{\rho^{\mathrm{univ}}_{\mathrm{inf}}}$.

Proposition 2.16. *Let $\rho : G \to \mathrm{GL}_2(R)$ be a lift of $\overline{\rho}$. Then the morphism $R^{\mathrm{univ}} \to R$ existing by universality induces a surjection $\Gamma^{\mathrm{univ}}_{\mathrm{inf}} \twoheadrightarrow \Gamma_\rho/\Phi(\Gamma_\rho)$.*

Proof. From the exact sequence $0 \to \Gamma_\rho \to \mathrm{im}(\rho) \to \overline{G} \to 0$ we obtain the group extension

$$0 \to \Gamma_\rho/\Phi(\Gamma_\rho) \to \mathcal{G} \to \overline{G} \to 0. \tag{2.3}$$

Let $V = \Gamma_\rho/\Phi(\Gamma_\rho)$ and decompose it into a direct sum of indecomposable $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules. Corollary 2.12 allows us to apply Proposition 2.14 to each of the indecomposable summands, yielding that the group extension in (2.3) can be realised by an infinitesimal deformation $\rho_V : G \to \mathrm{GL}_2(T)$ for $T = \mathbb{F}[X_1, \ldots, X_r]/(X_iX_j \mid i,j)$ for some r, i.e. $\mathcal{G} = \mathrm{im}(\rho_V)$ and, in particular, $\Gamma_{\rho_V} \cong V$.

Let $\varphi : R^{\mathrm{univ}} \to T$ be the morphism existing by universality. As $\mathfrak{m}_T^2 = 0$ and $p\mathfrak{m}_T = 0$, it follows that φ factors over $(\mathfrak{m}_{\mathrm{univ}}^2, p)$ and thus induces a surjection $\mathrm{im}(\rho_{\mathrm{inf}}^{\mathrm{univ}}) \twoheadrightarrow \mathrm{im}(\rho_V)$. In particular, we obtain a surjection $\Gamma_{\mathrm{inf}}^{\mathrm{univ}} \twoheadrightarrow V$, as claimed. □

We can now give the remaining proofs in the representation theory part of the paper.

Proof of Corollary 1.3. Proposition 2.16 gives the surjection $\Gamma_{\mathrm{inf}}^{\mathrm{univ}} \twoheadrightarrow \Gamma^{\mathrm{univ}}/\Phi(\Gamma^{\mathrm{univ}})$, which has to be an isomorphism because $\Gamma_{\mathrm{inf}}^{\mathrm{univ}}$ is an elementary abelian p-quotient of Γ^{univ} while $\Gamma^{\mathrm{univ}}/\Phi(\Gamma^{\mathrm{univ}})$ is the largest such. □

Proof of Theorem 1.4. (a) The implications '(ai) $\Rightarrow$ (aii)' and '(aiii) $\Rightarrow$ (aiv)' are trivial and the implication '(aiv) $\Rightarrow$ (ai)' is immediate from Theorem 1.1 and Corollary 1.3. In order to see '(aii) $\Rightarrow$(aiii)', consider any infinitesimal deformation ρ of $\overline{\rho}$. Then, by Corollary 2.12, the associated Γ_ρ is an $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module the indecomposable submodules of which occur in $\mathrm{ad}(\overline{\rho})$. By Proposition 2.14, each such indecomposable submodule Z gives a representation of the type considered in (aii), and is thus dihedral. By Theorem 1.1 this means that Z is trivial as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module. Thus Γ_ρ is trivial as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module, whence ρ is dihedral by Theorem 1.1.

(b) Let $R_{\overline{\chi}}^{\mathrm{univ}}$ be the universal deformation ring of $\overline{\chi}$ as discussed in Proposition 2.1. As $\rho^{\mathrm{univ}} = \mathrm{Ind}_H^G(\chi)_{R^{\mathrm{univ}}}$ for some character χ is a deformation of $\overline{\rho}$, the character χ is a deformation of $\overline{\chi}$ (if, by restriction to H, we find that χ^σ deforms $\overline{\chi}$, then we simply replace χ by χ^σ), giving a morphism $\alpha : R_{\overline{\chi}}^{\mathrm{univ}} \to R^{\mathrm{univ}}$. On the other hand, given the deformation χ^{univ} of $\overline{\chi}$, we obtain a deformation $\mathrm{Ind}_H^G(\chi^{\mathrm{univ}})_{R_{\overline{\chi}}^{\mathrm{univ}}}$ of $\overline{\rho}$ and thus a morphism $\beta : R^{\mathrm{univ}} \to R_{\overline{\chi}}^{\mathrm{univ}}$. For the composite we have $\alpha \circ \beta \circ \rho^{\mathrm{univ}} = \rho^{\mathrm{univ}}$ and hence $\alpha \circ \beta$ is the identity. Similarly, $\beta \circ \alpha \circ \chi^{\mathrm{univ}} = \chi^{\mathrm{univ}}$, whence $\beta \circ \alpha$ is the identity, implying that both α and β are isomorphisms and $R^{\mathrm{univ}} \cong R_{\overline{\chi}}^{\mathrm{univ}}$, as claimed. □

Remark 2.17. *Let $R = \mathbb{F}[\epsilon]/(\epsilon^3)$ for a prime $p > 2$ and consider the p-group*

$$\Gamma = \{1 + \epsilon \left(\begin{smallmatrix} r & 0 \\ 0 & -r \end{smallmatrix}\right) + \epsilon^2 \left(\begin{smallmatrix} a & b \\ c & r^2 - a \end{smallmatrix}\right) \mid a,b,c,r \in \mathbb{F}_p\} \subset \mathrm{GL}_2(R).$$

It is stable under conjugation by matrices of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)$, i.e. by $\overline{G}$ viewed inside $\mathrm{GL}_2(R)$. Moreover, Γ is an elementary abelian p-group, so that $\Phi(\Gamma) = 0$ and Γ is its own Frattini quotient. Let $\mathcal{G} \subset \mathrm{GL}_2(R)$ be the subgroup generated by $\overline{G}$ and Γ. Then any lift $\rho : G \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ with image $\mathcal{G}$ (and then also $\Gamma = \Gamma_\rho$) provides an example where ρ_{inf} is dihedral but ρ is not (in view of Theorem 1.1).

3 Number theoretic dihedral universal deformations

In this section, we turn our attention to dihedral Galois representations of number fields and their deformations and develop and prove the results outlined in section 1.2. We keep the notation introduced previously. In addition, we use the following notation.

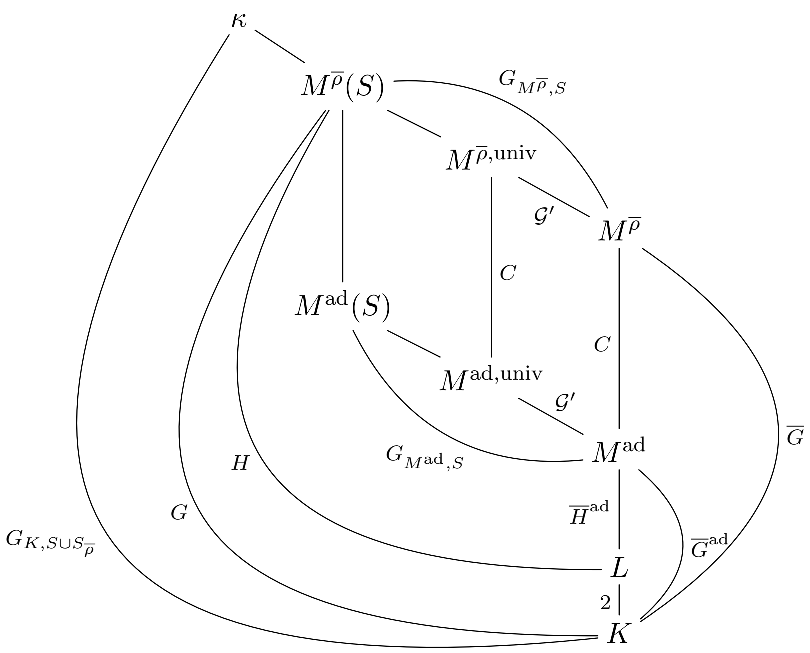
Notation 3.1. *For a number field N, denote by G_N the absolute Galois group of N and by $A(N)$ the class group of N. If $\mathfrak{p}$ is a prime of N, then denote by $N_{\mathfrak{p}}$ the completion of N at $\mathfrak{p}$. If ρ is a representation of a group G and H is a subgroup of G, then we denote by $\rho|_H$ the restriction of ρ to H. If L and K are two fields such that L is an algebraic Galois (but not necessarily finite) extension of K, then we denote the Galois group $\mathrm{Gal}(L/K)$ by $G_{L/K}$. Let μ_p be the group of p-th roots of unity inside an algebraic closure of the prime field.*

For an extension N/K of number fields and a set of places S of K, denote by $N(S)$ the maximal extension of N unramified outside the primes of N lying above S. Note that for a Galois extension N/K, the extension $N(S)/K$ is also Galois as any conjugate $\sigma(N(S))$ for σ fixing K is also unramified over N outside the primes of N lying above S. Furthermore, let $N(S)^{\mathrm{ab},p}$ be the maximal abelian extension of N inside $N(S)$ of exponent p.

Set-up 3.2. *Let K be a number field, L be a quadratic extension of K and $\overline{\chi} : G_L \to \mathbb{F}^\times$ be a character such that the representation $\overline{\rho} = \mathrm{Ind}_{G_L}^{G_K}(\overline{\chi}) : G_K \to \mathrm{GL}_2(\mathbb{F})$ is absolutely irreducible. So, $\overline{\rho}|_{G_L} = C(\overline{\chi})_{\mathbb{F}} \oplus C(\overline{\chi}^\sigma)_{\mathbb{F}}$ where $\overline{\chi}^\sigma(h) = \overline{\chi}(\sigma h \sigma^{-1})$ in the notation of Definition 2.4. Let $M^{\overline{\rho}}$ be the extension of K fixed by $\ker(\overline{\rho})$ and M^{ad} be the extension of K fixed by $\ker(\mathrm{ad}(\overline{\rho}))$. If $p = 2$, assume that M^{ad} is totally imaginary.*

Let $\overline{G}^{\mathrm{ad}} = \mathrm{Gal}(M^{\mathrm{ad}}/K)$ and $\overline{H}^{\mathrm{ad}} = \mathrm{Gal}(M^{\mathrm{ad}}/L)$. So, $\overline{H}^{\mathrm{ad}}$ is a cyclic subgroup of index 2 in $\overline{G}^{\mathrm{ad}}$. Also let $C := \ker(\overline{G} \twoheadrightarrow \overline{G}^{\mathrm{ad}})$. Let S_∞ be the set of all archimedean places of K (places of K lying above ∞). Let S_p be the set of primes of K lying above p. Furthermore, let $S_{\overline{\rho}}$ be the finite set of finite primes of K at which $M^{\overline{\rho}}$ is ramified over K. Let S be a finite set of primes of K such that $S_\infty \subseteq S$ and $S \cap S_p = \emptyset$. Let $\kappa = K(S \cup S_{\overline{\rho}})$.

We summarise some of the fields and Galois groups in the following diagram (some notation in the diagram is only introduced later).



Note that the extensions $M^{\overline{\rho}}(S)$ and $M^{\mathrm{ad}}(S)$ of K are Galois. Put $G = \mathrm{Gal}(M^{\overline{\rho}}(S)/K)$ and $H = \mathrm{Gal}(M^{\overline{\rho}}(S)/L)$. Note that these pieces of notation exactly correspond to those of section 2.

Let $G_{M^{\mathrm{ad}},S} = \mathrm{Gal}(M^{\mathrm{ad}}(S)/M^{\mathrm{ad}})$ and $G^{\mathrm{ab}}_{M^{\mathrm{ad}},S}$ be the continuous abelianisation of $G_{M^{\mathrm{ad}},S}$. As $\mathrm{Gal}(M^{\mathrm{ad}}(S)/M^{\mathrm{ad}})$ is normal in $\mathrm{Gal}(M^{\mathrm{ad}}(S)/K)$, the closure of the commutator subgroup of $\mathrm{Gal}(M^{\mathrm{ad}}(S)/M^{\mathrm{ad}})$ is also normal in $\mathrm{Gal}(M^{\mathrm{ad}}(S)/K)$. So, we get an action of $\overline{G}^{\mathrm{ad}} = \mathrm{Gal}(M^{\mathrm{ad}}/K)$ on $G^{\mathrm{ab}}_{M^{\mathrm{ad}},S}$ and hence, on the $\mathbb{F}_p$-vector space $\mathcal{G} := G^{\mathrm{ab}}_{M^{\mathrm{ad}},S}/(G^{\mathrm{ab}}_{M^{\mathrm{ad}},S})^p$ by conjugation.

Let S'' be the subset of S consisting of the finite primes q such that $\mu_p \subseteq M^{\mathrm{ad}}_{q'}$ for some (and then every) prime q' of M^{ad} dividing q (note: $S = S'' \cup S_\infty$ if $p = 2$). Denote by D_q a decomposition group of q inside $\overline{G}^{\mathrm{ad}}$. Let $\chi_p^{(q)}$ be the modulo p cyclotomic character viewed as a character of D_q for $q \in S''$ (note $\chi_2^{(q)}$ is the trivial character).

Proposition 3.3. *The elementary abelian p-group $\mathcal{G}$ admits $A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}})$ as a quotient and $\mathcal{M} = \ker\big(\mathcal{G} \twoheadrightarrow A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}})\big)$ is isomorphic to a quotient of $\prod_{q\in S''} \mathrm{Ind}_{D_q}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(q)})_{\mathbb{F}_p})$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules.*

Proof. See also [BM89, Section 1.2]. Let Y be the Galois group of $M^{\mathrm{ad}}(S)^{\mathrm{ab}}/M^{\mathrm{ad}}$, the maximal abelian extension of M^{ad} unramified outside the primes above S. Note $\mathcal{G} = Y/Y^p$. By global class field theory, we have the exact sequence of $\overline{G}^{\mathrm{ad}}$-modules:

$$\prod_{q'\in S'_{\mathrm{fin}}} \mathcal{O}_{q'}^\times \times \prod_{v\in S'_{\mathrm{real}}} \mathbb{Z}/2\mathbb{Z} \to Y \to A(M^{\mathrm{ad}}) \to 0, \tag{3.4}$$

where S'_{fin} is the set of finite primes of M^{ad} lying above S, $\mathcal{O}_{q'}$ is the ring of integers in $M^{\mathrm{ad}}_{q'}$ and S'_{real} is the set consisting of all real places of M^{ad}. Recall that, we have assumed M^{ad} to be totally complex if $p = 2$. Hence, taking the exact sequence (3.4) modulo p, we obtain the exact sequence of $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules:

$$\prod_{q'\in S'_{\mathrm{fin}}} \mathcal{O}_{q'}^\times/(\mathcal{O}_{q'}^\times)^p \to Y/Y^p \to A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}) \to 0. \tag{3.5}$$

As $\mathcal{O}_{q'}^\times$ is the direct product of the group of roots of unity in $M^{\mathrm{ad}}_{q'}$ and the group of 1-units (which is a pro-q group), it follows that $\mathcal{O}_{q'}^\times/(\mathcal{O}_{q'}^\times)^p$ is non-trivial if and only if $\mu_p \subseteq M^{\mathrm{ad}}_{q'}$. In that case $\mathcal{O}_{q'}^\times/(\mathcal{O}_{q'}^\times)^p$ is isomorphic to $C(\chi_p^{(q'/q)})_{\mathbb{F}_p}$ as $\mathbb{F}_p[D_{q'/q}]$-modules, where, for a moment, we keep track of the prime q' above q by denoting the decomposition group inside $\overline{G}^{\mathrm{ad}}$ corresponding to the prime q' by $D_{q'/q}$ and writing $\chi_p^{(q'/q)}$ for its modulo p cyclotomic character.

Thus $\mathcal{M}$ is an $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-quotient of $\prod_{q\in S''}\prod_{q'|q} C(\chi_p^{(q'/q)})_{\mathbb{F}_p}$. For a fixed $q \in S''$, $\overline{G}^{\mathrm{ad}}$ permutes the ideals $q' \mid q$ and one obtains that, as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules, $\prod_{q\in S''}\prod_{q'|q} C(\chi_p^{(q'/q)})_{\mathbb{F}_p}$ is isomorphic to $\prod_{q\in S''} \mathrm{Ind}_{D_q}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(q)})_{\mathbb{F}_p})$, which does not depend on the choice of q' above q (whence we simplified notation). $\square$

For further analysis, we first define the following sets of primes of K:

1. Let S_1 be the set of primes ℓ of K not lying above p such that ℓ is split in L, ℓ is unramified in M^{ad} and for any prime λ of M^{ad} lying above ℓ, $M^{\mathrm{ad}}_\lambda = K_\ell(\mu_p)$.

2. Let S_2 be the set of primes ℓ of K not lying above p such that ℓ is not split in L, for any prime λ of M^{ad} lying above ℓ, $\mu_p \subseteq M^{\mathrm{ad}}_\lambda$ and $[M^{\mathrm{ad}}_\lambda : K_\ell] = 2$ (so, the unique prime of L lying above ℓ splits completely in M^{ad}).

3. Let S_3 be the set of primes ℓ of K not lying above p such that $[K_\ell(\mu_p) : K_\ell] = 2$, ℓ is ramified in L and, for any prime λ of M^{ad} lying above ℓ, $\mathrm{Gal}(M^{\mathrm{ad}}_\lambda/K_\ell) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mu_p \subseteq M^{\mathrm{ad}}_\lambda$ (so, the unique prime of L above ℓ is unramified in M^{ad}).

Let $S_0 = S_1 \cup S_2 \cup S_3$.

As M^{ad} is Galois over K, if $\mu_p \subseteq M^{\mathrm{ad}}_{\lambda_0}$ for some prime λ_0 of M^{ad} lying above ℓ, then $\mu_p \subseteq M^{\mathrm{ad}}_\lambda$ for all primes λ of M^{ad} lying above ℓ. Moreover, $S_3 = \emptyset$ when $\overline{\chi}/\overline{\chi}^\sigma$ is of odd order. Observe that, when $\mu_p \subseteq K$ (thus, in particular, when $p = 2$), we have:

1. S_1 is the set of primes of K not lying above p which are completely split in M^{ad}.

2. $\ell \in S_2$ if and only if ℓ is not a prime above p, ℓ is either inert or ramified in L and the unique prime of L lying above ℓ is completely split in M^{ad}.

3. $S_3 = \emptyset$.

Proposition 3.4. *If $S \cap S_0 = \emptyset$ and $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$ in the notation of Definition 2.4, then $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathcal{G}, I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$.*

Proof. By Proposition 3.3, the notation of which we continue to use, restriction gives an injection

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathcal{G}, I(\overline{\chi}/\overline{\chi}^\sigma)) &\hookrightarrow \mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}\Big(\prod_{q\in S''} \mathrm{Ind}_{D_q}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(q)})_{\mathbb{F}_p}), I(\overline{\chi}/\overline{\chi}^\sigma)\Big)\\ &\cong \prod_{q\in S''} \mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathrm{Ind}_{D_q}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(q)})_{\mathbb{F}_p}), I(\overline{\chi}/\overline{\chi}^\sigma)). \quad (3.6)\end{aligned}$$

Frobenius reciprocity ([CR81, Thm. 10.8]) yields

$$\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathrm{Ind}_{D_q}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(q)})_{\mathbb{F}_p}), I(\overline{\chi}/\overline{\chi}^\sigma)) = \mathrm{Hom}_{\mathbb{F}_p[D_q]}(C(\chi_p^{(q)})_{\mathbb{F}_p}, I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}). \quad (3.7)$$

We see that $\mathrm{Hom}_{\mathbb{F}_p[D_q]}(C(\chi_p^{(q)})_{\mathbb{F}_p}, I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}) \neq 0$ if and only if $C(\chi_p^{(q)})_{\mathbb{F}_p}$ is an $\mathbb{F}_p[D_q]$-submodule of $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$. Now, we will do a case-by-case analysis of when this will happen. Let us point out that, in general, $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ is defined over some extension $\mathbb{F}/\mathbb{F}_p$. Note that $C(\chi_p^{(q)})_{\mathbb{F}_p}$ is an $\mathbb{F}_p[D_q]$-submodule of some module $C(\psi)_{\mathbb{F}}$ (for some $\mathbb{F}^\times$-valued character ψ of D_q) if and only if $\chi_p^{(q)} = \psi$. Note also that $\overline{G}^{\mathrm{ad}}$ acts faithfully on $\mathrm{ad}(\rho)_{\mathbb{F}} \cong N_{\mathbb{F}} \oplus I(\overline{\chi}/\overline{\chi}^\sigma)$ (see Lemma 2.5) and thus $\overline{H}^{\mathrm{ad}}$ acts faithfully on $C(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}$.

1. q **is split in** L**:** In this case, $D_q \subseteq \overline{H}^{\mathrm{ad}}$, whence $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q} = C(\overline{\chi}/\overline{\chi}^\sigma|_{D_q})_{\mathbb{F}} \oplus C(\overline{\chi}^\sigma/\overline{\chi}|_{D_q})_{\mathbb{F}}$. So, $C(\chi_p^{(q)})_{\mathbb{F}_p}$ is an $\mathbb{F}_p[D_q]$-submodule of $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ if and only if $\overline{\chi}/\overline{\chi}^\sigma|_{D_q} = \chi_p^{(q)}$ or $\overline{\chi}^\sigma/\overline{\chi}|_{D_q} = \chi_p^{(q)}$. This is the case if and only if the extension of $M_{q'}^{\mathrm{ad}}/K_q$, the Galois group of which equals D_q and acts faithfully on $C(\overline{\chi}^\sigma/\overline{\chi}|_{D_q})_{\mathbb{F}}$, equals the extension the Galois group of which acts faithfully on $C(\chi_p^{(q)})_{\mathbb{F}_p}$, i.e. $M_{q'}^{\mathrm{ad}} = K_q(\mu_p)$. Note that such primes q are exactly the ones lying in S_1.

2. q **is not split in** L**:** In this case, $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ is reducible if and only if D_q is either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\tilde{q}$ be the unique prime of L lying above q.

   Suppose first that $D_q = \mathbb{Z}/2\mathbb{Z}$. Then $D_q = \mathrm{Gal}(L_{\tilde{q}}/K_q)$. Consequently, $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ is $\mathbb{F}^2$ with D_q-action swapping the two standard basis vectors. So, if $p > 2$, then $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q} \cong C(1)_{\mathbb{F}} \oplus C(\epsilon)_{\mathbb{F}}$ for the quadratic character $\epsilon : D_q \cong \{\pm 1\} \subseteq \mathbb{F}^\times$. If $p = 2$, then $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ is the module $N_{\mathbb{F}}$ from Definition 2.4. Hence, for any p, we see that $C(\chi_p^{(q)})_{\mathbb{F}_p}$ is an $\mathbb{F}_p[D_q]$-submodule of $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ if and only if $\chi_p^{(q)}$ is the trivial character or equal to ϵ. This happens if and only if one of the following conditions hold:

   (a) $\mu_p \subseteq K_q$,

   (b) $L_{\tilde{q}} = K_q(\mu_p)$ (and then q is inert in L).

   Now, the primes q satisfying any one of the conditions above are exactly the ones lying in S_2.

   Suppose now that $D_q = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (note that this case cannot happen when $p = 2$). Then q is ramified in M^{ad} and is not split in L. Note that $\overline{\chi}/\overline{\chi}^\sigma$ is a non-trivial character of $\mathrm{Gal}(M_{q'}^{\mathrm{ad}}/L_{\tilde{q}}) = D_q \cap \mathrm{Gal}(M^{\mathrm{ad}}/L)$. So, in this case, $C(\chi_p^{(q)})_{\mathbb{F}_p}$ is an $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-submodule of $I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}$ if and only if $M_{q'}^{\mathrm{ad}} = L_{\tilde{q}}(\mu_p) \overset{2}{\supsetneq} L_{\tilde{q}} \overset{2}{\supsetneq} K_q$. This is equivalent to $[K_q(\mu_p) : K_q] = 2$, q is ramified in L and the unique prime of L lying above q is unramified in M^{ad}. So, primes satisfying these conditions are exactly the ones belonging to S_3.

Thus, the primes satisfying these conditions are contained in $S_1 \cup S_2 \cup S_3 = S_0$, whence by our assumption none of them lies in S. We thus obtain $\mathrm{Hom}_{\mathbb{F}_p[D_q]}(C(\chi_p^{(q)})_{\mathbb{F}_p}, I(\overline{\chi}/\overline{\chi}^\sigma)|_{D_q}) = 0$ for all $q \in S$. In view of (3.6) and (3.7), the assertion of the proposition follows. $\square$

Remark 3.5. *In the proof of Proposition 3.3, we are ignoring the contribution of the kernel of the first map of* (3.4)*, which is given by the global units $\mathcal{O}_{M^{\mathrm{ad}}}^\times$ of M^{ad}. So, it could happen that S contains some primes from S_0 and the conclusion of the proposition still continues to hold due to the contribution coming from $\mathcal{O}_{M^{\mathrm{ad}}}^\times$ negating the contribution coming from primes of M^{ad} lying above primes from S_0. However, we know the $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module structure of the finite dimensional $\mathbb{F}_p$-vector space $\mathcal{O}_{M^{\mathrm{ad}}}^\times/(\mathcal{O}_{M^{\mathrm{ad}}}^\times)^p$. So, we can find a number n_0 such that if S contains more than n_0 primes from S_0, then the statement of the proposition would not be true any more.*

Remark 3.6. *The assumption* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^{\sigma})) = 0$ *is necessary for Proposition 3.4 to hold because if the assumption is violated, then by* (3.4)*,* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathcal{G}, I(\overline{\chi}/\overline{\chi}^{\sigma}))$ *is non-zero.*

Remark 3.7. *If we include all primes* $\mathfrak{p}$ *of* K *lying above* p *in* S *and if* $\overline{\rho}$ *is not totally even (i.e.* M^{ad} *is not totally real), then the oddness of* $\overline{\rho}$ *would imply that the multiplicity of* $I(\overline{\chi}/\overline{\chi}^{\sigma})$ *occurring in* $\prod_{\mathfrak{p}'|p} \mathcal{O}_{\mathfrak{p}'}/(\mathcal{O}_{\mathfrak{p}'})^p$ *would be greater than the multiplicity of* $I(\overline{\chi}/\overline{\chi}^{\sigma})$ *occurring in* $\mathcal{O}_{M^{\mathrm{ad}}}^{\times}/(\mathcal{O}_{M^{\mathrm{ad}}}^{\times})^p$ *(here,* $\mathcal{O}_{\mathfrak{p}'}$ *is the ring of integers of the completion of* M^{ad} *at the prime* $\mathfrak{p}'$ *lying above* $\mathfrak{p}$*). Thus, we see that, in this case* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathcal{G}, I(\overline{\chi}/\overline{\chi}^{\sigma})) \neq 0$*. Therefore, it is necessary that* S *does not contain all the primes above* p *for Proposition 3.4 to hold when* $\overline{\rho}$ *is not totally even. From this logic, we also see that, if* $\overline{\rho}$ *is not totally even, then, in some cases, the presence of only some (and not all) of the primes of* K *lying above* p *in* S *is sufficient to conclude that Proposition 3.4 does not hold.*

Remark 3.8. *We have assumed that* M^{ad} *is totally complex when* $p = 2$*. If* M^{ad} *had a real place* v*, then its* $\overline{G}^{\mathrm{ad}}$*-orbit would consist entirely of real places. So, there would be a contribution from these places in the exact sequence* (3.4)*. Moreover, as* $\mathbb{F}_2[\overline{G}^{\mathrm{ad}}]$*-module, the contribution* $\prod_{g\in\overline{G}^{\mathrm{ad}}} \mathbb{Z}/2\mathbb{Z}$ *given by the Galois orbit of* v *in the first term of the exact sequence would be isomorphic to* $\mathbb{F}_2[\overline{G}^{\mathrm{ad}}]$*, i.e. the regular representation. Hence, there can be a non-zero* $\mathbb{F}_2[\overline{G}^{\mathrm{ad}}]$*-homomorphism from the first term in* (3.4) *to* $I(\overline{\chi}/\overline{\chi}^{\sigma})$*. Thus, the hypothesis seems essential for the proposition unless we know that contribution from global units negates the contribution coming from* S_{∞}*. So, in particular, if* M^{ad} *has sufficiently many real places, then the statement of Proposition 3.4 does not hold.*

We now turn towards deformation theory. Clearly, $\overline{\rho}$ is a representation of $G = \mathrm{Gal}(M^{\overline{\rho}}(S)/K)$. Denote by D_S the functor from $\mathcal{C}$ to the category of sets which sends R to the set of continuous deformations $\rho : G \to \mathrm{GL}_2(R)$ of $\overline{\rho}$. Let D_S^0 be the subfunctor of D_S which sends an object R of $\mathcal{C}$ to the set of continuous deformations $\rho : G \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ with determinant $\widehat{\det(\overline{\rho})}$.

Lemma 3.9. *The functors* D_S *and* D_S^0 *are representable by rings in* $\mathcal{C}$*.*

Proof. The group G is a quotient of $\mathrm{Gal}(\kappa/K)$ and, hence, satisfies the finiteness condition Φ_p of Mazur ([Maz89, 1.1]). Therefore, as seen just before Proposition 2.16, D_S is representable by a ring in $\mathcal{C}$. As a consequence, it follows that D_S^0 is also representable by a ring in $\mathcal{C}$ (see [Maz97, Section 24]). □

For an object R of $\mathcal{C}$, a deformation $\rho : \mathrm{Gal}(\kappa/K) \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ belongs to $D_S(R)$ if and only if the field fixed by $\ker(\rho)$ is an extension of $M^{\overline{\rho}}$ unramified outside the places of $M^{\overline{\rho}}$ lying above S. Hence, we make the following definition.

Definition 3.10. *We call the deformations belonging to* $D_S(R)$ *as deformations of* $\overline{\rho}$ relatively unramified outside S *and deformations belonging to* $D_S^0(R)$ *as deformations of* $\overline{\rho}$ relatively unramified outside S *with constant determinant.*

We are careful to speak of *relatively* unramified deformations of $\overline{\rho}$ instead of just unramified ones in order to avoid possible confusion with unramified representations: if S does not contain all of $S_{\overline{\rho}}$, then a deformation can be relatively unramified outside S even though as a representation it does ramify outside S.

We continue to essentially follow the notation introduced in section 2 with the exception that we keep track of the chosen set of primes S. Denote by R_S^{univ} the ring by which D_S is representable. Denote by $\rho_S^{\mathrm{univ}} : G \to \mathrm{GL}_2(R_S^{\mathrm{univ}})$ the universal deformation of $\overline{\rho}$ relatively unramified outside S. Let $(R_S^{\mathrm{univ}})^0$ be the ring which represents D_S^0 and $(\rho_S^{\mathrm{univ}})^0 : G \to \mathrm{GL}_2((R_S^{\mathrm{univ}})^0)$ the universal deformation of $\overline{\rho}$ relatively unramified outside S with constant determinant. So, we have a natural surjective homomorphism $R_S^{\mathrm{univ}} \to (R_S^{\mathrm{univ}})^0$. Let $\mathfrak{m}_{R_S^{\mathrm{univ}}}$ be the maximal ideal of R_S^{univ}.

Proof of Theorem 1.5. Write $\rho := \rho_S^{\mathrm{univ}}$ as abbreviation. We shall apply some of the main results from section 2. In particular, it will suffice to work with p-Frattini quotients and to apply the classifications of modules from section 2.

Let Γ_ρ be the group defined in (1.1) and let $\mathcal{G}' := \Gamma_\rho/\Phi(\Gamma_\rho)$ be its p-Frattini quotient. Let $M^{\overline{\rho},\mathrm{univ}}$ be the subfield of $M^{\overline{\rho}}(S)$ such that $\mathrm{Gal}(M^{\overline{\rho},\mathrm{univ}}/M^{\overline{\rho}}) = \mathcal{G}'$. We have $\mathrm{Gal}(M^{\overline{\rho},\mathrm{univ}}/M^{\mathrm{ad}}) \cong C \times \mathcal{G}'$ because C is cyclic and the action of C on $\mathcal{G}'$ by conjugation is trivial as it corresponds to conjugation by scalar matrices due to Lemma 2.9 and Corollary 1.3.

By Galois theory, there is a unique extension $M^{\mathrm{ad},\mathrm{univ}}$ of M^{ad} contained in $M^{\overline{\rho},\mathrm{univ}}$ such that $\mathrm{Gal}(M^{\mathrm{ad},\mathrm{univ}}/M^{\mathrm{ad}}) \cong \mathcal{G}'$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules. The field $M^{\mathrm{ad},\mathrm{univ}}$ is contained in $M^{\mathrm{ad}}(S)$ because if a prime of M^{ad} ramifies in $M^{\mathrm{ad},\mathrm{univ}}$, then there is a prime of $M^{\overline{\rho}}$ above it that ramifies in $M^{\overline{\rho},\mathrm{univ}}$ as the orders of C and $\mathcal{G}'$ are coprime. Note that $\mathcal{G}'$ is a quotient of $\mathcal{G}$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules. Since, by Proposition 3.4, $I(\overline{\chi}/\overline{\chi}^\sigma)$ does not occur in $\mathcal{G}$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module, it does not occur in $\mathcal{G}'$ either. So, by Corollary 2.12, $\overline{H}^{\mathrm{ad}}$ acts trivially on $\mathcal{G}'$. This allows us to conclude that $\rho = \rho_S^{\mathrm{univ}}$ is dihedral by Theorem 1.1. □

Remark 3.11. *If* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathcal{G}, I(\overline{\chi}/\overline{\chi}^\sigma)) \neq 0$, *then we can find an abelian extension* M_0 *of* $M^{\overline{\rho}}$ *unramified outside primes of* $M^{\overline{\rho}}$ *lying above* S *such that* M_0 *is Galois over* K *and such that the exact sequence* $0 \to \mathrm{Gal}(M_0/M^{\overline{\rho}}) \to \mathrm{Gal}(M_0/K) \to \mathrm{im}(\overline{\rho}) \to 0$ *gives* $\mathrm{Gal}(M_0/M^{\overline{\rho}})$ *the structure of* $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$*-module isomorphic to* $I(\overline{\chi}/\overline{\chi}^\sigma)$. *Therefore, from Proposition 2.14, we get a non-dihedral infinitesimal deformation of* $\overline{\rho}$ *relatively unramified outside* S. *So, in that case,* ρ_S^{univ} *is not dihedral. Thus, from Remark 3.6, we see that* ρ_S^{univ} *is not dihedral if* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma))$ *is non-zero. It follows, from Remark 3.5, that* ρ_S^{univ} *is not dihedral if the set* S *contains sufficiently many primes from the set* S_0. *Finally, Remark 3.7 implies that if* S *contains all the primes above* p *and* $\overline{\rho}$ *is not totally even, then* ρ_S^{univ} *is not dihedral.*

We will now see some consequences of Theorem 1.5, the hypotheses of which we assume to hold in the sequel.

Let $G^{\mathrm{ab},(p)}_{M^{\overline{\rho}}(S),L}$ be the maximal, continuous pro-p abelian quotient of $\mathrm{Gal}(M^{\overline{\rho}}(S)/L)$. As S does not contain any prime of K above p, it follows, from global class field theory, that $G^{\mathrm{ab},(p)}_{M^{\overline{\rho}}(S),L}$ is a finite, abelian p-group. Let L_S be the extension of L such that $\mathrm{Gal}(L_S/L) = G^{\mathrm{ab},(p)}_{M^{\overline{\rho}}(S),L}$. So, $M^{\overline{\rho}}L_S \subset M^{\overline{\rho}}(S)$. Note that L_S contains the maximal, abelian p-extension of L unramified outside primes of L lying above S. Moreover, note that $M^{\overline{\rho}}L_S$ is an abelian extension of L as both $M^{\overline{\rho}}$ and L_S are abelian extensions of L. As $p \nmid |\mathrm{Gal}(M^{\overline{\rho}}/L)|$ and $\mathrm{Gal}(L_S/L)$ is a finite abelian p-group, it follows that $\mathrm{Gal}(M^{\overline{\rho}}L_S/L) \simeq \mathrm{Gal}(M^{\overline{\rho}}/L) \times \mathrm{Gal}(L_S/L)$. Let $\mathfrak{q}$ be a prime of L. If $\mathfrak{q}$ ramifies in L_S, then any prime of $M^{\overline{\rho}}$ lying above $\mathfrak{q}$ ramifies in $M^{\overline{\rho}}.L_S$. As $M^{\overline{\rho}}L_S \subset M^{\overline{\rho}}(S)$, it follows that L_S is unramified outside primes of L lying above S. So, it follows that L_S is the maximal, abelian p-extension of L unramified outside primes of L lying above S.

Suppose $\mathrm{Gal}(L_S/L) = \prod_{i=1}^{n'} \mathbb{Z}/p^{e_i}\mathbb{Z}$.

Corollary 3.12. *Let S be a finite set of primes of K. Suppose the conditions given in Theorem 1.5 hold. Then $R^{\mathrm{univ}}_S \simeq W(\mathbb{F})[X_1, \cdots, X_{n'}]/((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_{n'})^{p^{e_{n'}}} - 1)$.*

Proof. This follows directly from Theorem 1.5, part (b) of Theorem 1.4 and Proposition 2.1. □

Proof of Corollary 1.6. If the conditions given in Theorem 1.5 hold, then Theorem 1.5 and part (b) of Theorem 1.4 together imply that $\rho^{\mathrm{univ}}_S = \mathrm{Ind}^{G_{M^{\overline{\rho}}(S)/K}}_{G_{M^{\overline{\rho}}(S)/L}} \chi^{\mathrm{univ}}$ where $\chi^{\mathrm{univ}} : \mathrm{Gal}(M^{\overline{\rho}}(S)/L) \to (R^{\mathrm{univ}}_S)^\times$ is the universal deformation of $\overline{\chi}$. It follows, from the description of χ^{univ} in Proposition 2.1 and the discussion before Corollary 3.12, that χ^{univ} has finite image. Therefore, from the discussion before Definition 2.4, we see that ρ^{univ}_S has finite image. □

Proof of Corollary 1.7. In order to prove this corollary, we will check that the set S satisfies the hypotheses of Theorem 1.5 in both the cases. Recall that we denoted by M the maximal unramified abelian 5-extension of L, which exists as the class number of L is 15. Now, the class number of M is 3 (see [LMF13, Number field 20.0.35908028125401873392383429449.1]).

Let us assume that we are in case (a) of the corollary. So, we have $K = \mathbb{Q}(\sqrt{717})$, $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-239})$, $M^{\mathrm{ad}} = M$ and $\overline{G}^{\mathrm{ad}} = \mathrm{Gal}(M/\mathbb{Q}(\sqrt{717})) \simeq D_5$. As the class number of M is 3, it follows that $\mathrm{Hom}_{\mathbb{F}_3[\overline{G}^{\mathrm{ad}}]}(A(M)/3A(M), I(\chi/\chi^\sigma)) = 0$. Now, $S_\infty \subseteq S$ and $S \cap S_p = \emptyset$. Let P be the set of all finite primes of $\mathbb{Q}(\sqrt{717})$. Now, as $\mu_3 \subset \mathbb{Q}(\sqrt{-3}, \sqrt{-239})$, we see that $S_1 = \{\ell \in P \mid \ell \text{ is totally split in } M\}$ and $S_2 = \{\ell \in P \mid \ell \text{ is inert in } L\}$. Since we are working with D_5, $S_3 = \emptyset$. Now, if ℓ is a finite prime contained in S, then ℓ is split in L, which means that $\ell \notin S_2$. But ℓ is not completely split in M, which means that $\ell \notin S_1$. So, $S \cap S_0 = \emptyset$. Hence, all the hypotheses of Theorem 1.5 are satisfied. Therefore, by Corollary 1.6, we get that the universal deformation of $\overline{\rho}_1$ relatively unramified outside S has finite image.

The proof in the other case follows in the exact same way. In that case $\mu_3 \subset \mathbb{Q}(\sqrt{-3}) = K$ and we have already given the description of S_0 in the case $\mu_p \subset K$. So, we can use that description to prove that $S \cap S_0 = \emptyset$. □

Remark 3.13. *In the introduction, we said that the examples of Corollary 1.7 do not satisfy the hypotheses of [AC14, Corollary 3]. Here, we would like to elaborate a bit more on that. Allen and Calegari prove, in [AC14, Corollary 3], that if F is a totally real field and $\rho : G_F \to \mathrm{GL}_2(\mathbb{F})$ is a totally* *odd representation satisfying certain hypotheses, then Boston's conjecture is true for ρ. As the base field is assumed to be totally real in [AC14, Corollary 3], the second part of Corollary 1.7 clearly does not satisfy its hypotheses. Moreover, one of the hypotheses of [AC14, Corollary 3] is that the image of $\rho|_{G_{F(\mu_p)}}$ is adequate. However, we see that the image of $\overline{\rho}_1|_{G_{\mathbb{Q}(\sqrt{717},\mu_3)}}$ is just $\overline{\rho}_1(G_{\mathbb{Q}(\sqrt{-3},\sqrt{-239})})$ which is an abelian group. Hence, it is not adequate, which means that the part one of Corollary 1.7 does not satisfy the hypotheses of [AC14, Corollary 3] either.*

Now suppose p is odd. We will now do a computation which will be used in the next section. Since L is Galois over K, $\mathrm{Gal}(M^{\overline{\rho}}(S)/L)$ is a normal subgroup of $\mathrm{Gal}(M^{\overline{\rho}}(S)/K)$ and hence, L_S is Galois over K. Now, we get an action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(L_S/L)$ by conjugation. As p is odd, we get a direct sum decomposition $\mathrm{Gal}(L_S/L) = \prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z} \oplus \prod_{i=n+1}^{n'} \mathbb{Z}/p^{e_i}\mathbb{Z}$ such that $\mathrm{Gal}(L/K)$ acts by inversion on $\prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and trivially on $\prod_{i=n+1}^{n'} \mathbb{Z}/p^{e_i}\mathbb{Z}$ (note that n could be 0 or n').

Corollary 3.14. *Let p be an odd prime and S be a finite set of primes of K. Suppose the conditions given in Theorem 1.5 hold. Then $(R_S^{\mathrm{univ}})^0 \simeq W(\mathbb{F})[X_1, \cdots, X_n]/((1+X_1)^{p^{e_1}}-1, \cdots, (1+X_n)^{p^{e_n}} - 1)$.*

Proof. It follows, from Theorem 1.5 and part (b) of Theorem 1.4 that $\rho_S^{\mathrm{univ}} = \mathrm{Ind}_{G_{M^{\overline{\rho}}(S)/L}}^{G_{M^{\overline{\rho}}(S)/K}} \chi^{\mathrm{univ}}$ where $\chi^{\mathrm{univ}} : \mathrm{Gal}(M^{\overline{\rho}}(S)/L) \to (R_S^{\mathrm{univ}})^\times$ is the universal deformation of $\overline{\chi}$. As p is odd, it follows, from part (c) of Lemma 2.9, that the exact sequence $0 \to \Gamma_S^{\mathrm{univ}} \to \mathrm{im}(\rho_S^{\mathrm{univ}}) \to \mathrm{im}(\overline{\rho}) \to 0$ splits. Note that χ^{univ} factors through $\mathrm{Gal}(M^{\overline{\rho}}L_S/L)$. So, from the description of χ^{univ} obtained in Proposition 2.1, we get that $\mathrm{im}(\det(\rho_S^{\mathrm{univ}}))$ is the subgroup of $(R_S^{\mathrm{univ}})^\times$ generated by $\widehat{\mathrm{im}(\det \overline{\rho})}$ and $(1+X_i)^2$ with $n+1 \leq i \leq n'$.

We know that $(R_S^{\mathrm{univ}})^0$ is the quotient R_S^{univ}/I, where I is the ideal generated by the elements $\det(\rho_S^{\mathrm{univ}}(g)) - \widehat{\det(\overline{\rho}(g))}$ for all $g \in \mathrm{Gal}(M^{\overline{\rho}}(S)/K)$ (see [Maz97, Section 24]). So, I is generated by the elements $X_i(X_i+2)$ with $n+1 \leq i \leq n'$. As $p > 2$ and $X_i \in \mathfrak{m}_{R_S^{\mathrm{univ}}}$ for all $1 \leq i \leq n'$, it follows that $I = (X_{n+1}, \cdots, X_{n'})$. Therefore, $(R_S^{\mathrm{univ}})^0 \simeq R_S^{\mathrm{univ}}/(X_{n+1}, \cdots, X_{n'}) \simeq W(\mathbb{F})[X_1, \cdots, X_n]/((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_n)^{p^{e_n}} - 1)$. $\square$

4 Modularity and an $R = \mathbb{T}$-theorem

This section is devoted to developing and proving the results outlined in section 1.3.

Notation 4.1. *In addition to the notation introduced in the previous sections, we introduce some more notation. For a prime ℓ of K, denote by G_{K_ℓ} by the absolute Galois group of K_ℓ and denote its inertia group by I_ℓ. We fix an embedding $G_{K_\ell} \to G_K$ for every prime ℓ of K. For a representation ρ of G_K, we denote by $\rho|_{G_{K_\ell}}$ the representation of G_{K_ℓ} obtained by composing ρ with the fixed embedding $G_{K_\ell} \to G_K$ and we denote by $\rho|_{I_\ell}$ the representation of I_ℓ obtained by restricting $\rho|_{G_{K_\ell}}$ to I_ℓ.*

Set-up 4.2. *We continue to assume Set-up 3.2. Thus, we have a number field K, a quadratic extension L of K, a finite extension $\mathbb{F}$ of $\mathbb{F}_p$ and a character $\overline{\chi} : G_L \to \mathbb{F}^\times$ such that the representation*

$\overline{\rho} = \mathrm{Ind}_{G_L}^{G_K}(\overline{\chi}) : G_K \to \mathrm{GL}_2(\mathbb{F})$ *is absolutely irreducible. The extensions of* K *fixed by* $\ker(\overline{\rho})$ *and* $\ker(\mathrm{ad}(\overline{\rho}))$ *are denoted by* $M^{\overline{\rho}}$ *and* M^{ad}*, respectively. We let* $\overline{G}^{\mathrm{ad}} = \mathrm{Gal}(M^{\mathrm{ad}}/K)$ *and* $\overline{H}^{\mathrm{ad}} = \mathrm{Gal}(M^{\mathrm{ad}}/L)$.

For this section, we specialise Set-up 3.2 as indicated in section 1.3:

1. p *is odd.*
2. K *is totally real.*
3. $\overline{\chi}$ *is such that* $\overline{\rho}$ *is totally odd.*
4. $\overline{\rho}$ *is unramified at all places of* K *above* p*, i.e.* $S_{\overline{\rho}} \cap S_p = \emptyset$*.*
5. *If a prime* ℓ *of* K *ramifies in* $M^{\overline{\rho}}$ *and* $\overline{\rho}|_{G_{K_\ell}}$ *is not absolutely irreducible, then* $\dim((\overline{\rho})^{I_\ell}) = 1$ *where* $(\overline{\rho})^{I_\ell}$ *denotes the subspace of* $\overline{\rho}$ *fixed by the inertia group* I_ℓ *at* ℓ*.*
6. $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0.$

For $K = \mathbb{Q}$*, conditions 4 and 5 are the ones given in [CG18, Section* 3.1*].*

We will first define the Hecke algebra $\mathbb{T}$. We begin by recalling the following classical lemma:

Lemma 4.3. *Let* K *be a totally real number field and* L *be a quadratic extension of* K*. Let* $\chi : G_L \to (\overline{\mathbb{Q}_p})^\times$ *be a finite order character of* G_L *such that it is unramified at places dividing* p *and such that the induced representation* $\rho = \mathrm{Ind}_{G_L}^{G_K}\chi$ *is a totally odd absolutely irreducible representation of* G_K*. Let* D *be the Artin conductor of* ρ*. Then there exists a Hilbert modular eigenform* f *over* K *of parallel weight one on* $\Gamma_1(D)$ *such that the Galois representation* ρ_f *attached to* f *is isomorphic to* ρ*.*

Proof. The existence of the Hilbert modular eigenform of parallel weight one over K follows from the proofs of [Oza17, Lemma 4.9 and Lemma 4.10], which uses automorphic induction, and [RT11, Theorem 1.4] (see [Gel97, Section $5.3(A)$ and Theorem 5.3.1] or [Rog97, Theorem 17] as well). The assertion for the level of f follows from [RT11, Theorem 1.4] and the local-global compatibility in the Langlands correspondence. When L/K is a CM field, the entire lemma also follows from [Hid79] (see [BGV13, Section 1]). □

Now, suppose the p-part of $A(L)$ equals $\prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z} \oplus W$ where $\mathrm{Gal}(L/K)$ acts trivially on W and by inversion on $\prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z}$ (as p is odd, we have seen in the previous section that we can get this splitting). Let L^ϵ be the abelian, unramified p-extension of L fixed by W. So, $\mathrm{Gal}(L^\epsilon/L) = \prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z}$ and $\mathrm{Gal}(L/K)$ acts by inversion on it. Note that $M^{\overline{\rho}}L^\epsilon$ is an abelian extension of L as $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/L) \simeq \mathrm{Gal}(M^{\overline{\rho}}/L) \times \mathrm{Gal}(L^\epsilon/L)$ and is also Galois over K.

Let $\chi : \mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/L) \to \overline{\mathbb{Q}_p}^\times$ be a character lifting the character $\overline{\chi}$ (as $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/L)$ is finite, χ takes values in the ring of integers of a finite extension of $\mathbb{Q}_p$, so it makes sense to say χ is a lift of $\overline{\chi}$). Thus, under the decomposition above, $\chi((g,0)) = \widehat{\overline{\chi}(g)}$. So, as χ is a lift of $\overline{\chi}$, the representation $\rho_\chi = \mathrm{Ind}_{G_L}^{G_K}\chi$ is a (relatively unramified) deformation of $\overline{\rho}$ (to the ring of integers of a suitable finite extension of $\mathbb{Q}_p$). Moreover, since $\mathrm{Gal}(L/K)$ acts by inversion on $\mathrm{Gal}(L^\epsilon/L)$, it follows that $\det \rho_\chi = \widehat{\det \overline{\rho}}$ and, hence, ρ is totally odd. As L^ϵ is unramified over L (and, thus, ρ_χ is a relatively unramified deformation), we see that the Artin conductor of $\rho_\chi =$ Artin conductor of $\overline{\rho} = D$, which is an ideal of K. So, a prime ℓ of K ramifies in $M^{\overline{\rho}}$ if and only if $\ell \mid D$.

For such a character χ, there exists a Hilbert modular eigenform f_χ of parallel weight 1 on $\Gamma_1(D)$ over K such that the Galois representation ρ_{f_χ} attached to f_χ is isomorphic to $\rho_\chi = \mathrm{Ind}_{G_L}^{G_K} \chi$ (this follows from Lemma 4.3). Note that even though ρ_χ is a p-adic representation, it is unramified at all places $\mathfrak{p}$ above p and the trace of $\rho_\chi(\mathrm{Frob}_\mathfrak{p})$ equals the eigenvalue of the Hecke operator $T_\mathfrak{p}$ acting on f_χ. Let $\mathcal{S}$ be the set of all such characters χ, that is, $\mathcal{S}$ is the set of all characters $\chi : \mathrm{Gal}(M^{\overline{\rho}} L^\epsilon / L) \to \overline{\mathbb{Q}_p}^\times$ such that $\chi((g, 0)) = \widehat{\overline{\chi(g)}}$.

Let $m = \max\{m_i : 1 \leq i \leq j\}$ and $\mathcal{K} = \mathrm{Frac}(W(\mathbb{F}))(\mu_{p^m})$, where $\mathrm{Frac}(W(\mathbb{F}))$ is the fraction field of $W(\mathbb{F})$ and μ_{p^m} is the group of p^m-th roots of unity. Let $\mathcal{O}$ be the ring of integers of $\mathcal{K}$. Let $S(\mathcal{O}, D)$ be the space of Hilbert modular forms of parallel weight 1 on $\Gamma_1(D)$ over K with Fourier coefficients in $\mathcal{O}$. So, $\{f_\chi : \chi \in \mathcal{S}\} \subset S(\mathcal{O}, D)$. We are now ready to define the Hecke algebra $\mathbb{T}$.

Definition 4.4. *Let $\mathcal{W}$ be the $\mathcal{O}$-submodule of $S(\mathcal{O}, D)$ generated by $\{f_\chi : \chi \in \mathcal{S}\}$. Let T be the $W(\mathbb{F})$-algebra generated by Hecke operators away from D. We define $\mathbb{T}$ to be largest quotient of T acting faithfully on $\mathcal{W}$. Thus, $\mathbb{T}$ is the $W(\mathbb{F})$-subalgebra of $\mathrm{End}_\mathcal{O}(\mathcal{W})$ generated by the Hecke operators away from D.*

Note that $\mathbb{T}$ is a local ring as all the f_χ's are congruent to each other. Moreover, as it is finite over $W(\mathbb{F})$, it is also complete and its residue field is $\mathbb{F}$ because the eigenvalues of the underlying characteristic p Hilbert modular eigenform (reduction of any of the f_χ's modulo the maximal ideal of $\mathcal{O}$) are in $\mathbb{F}$. We begin by constructing a deformation of $\overline{\rho}$ defined over $\mathbb{T}$.

Proposition 4.5. *There exists a representation $\rho_\mathbb{T} : G_K \to \mathrm{GL}_2(\mathbb{T})$ which is a dihedral deformation of $\overline{\rho}$ unramified outside $\{\ell \text{ is a prime of } K \mid \ell | D\} \cup \{S_\infty\}$ and satisfies $\mathrm{tr}(\rho_\mathbb{T}(\mathrm{Frob}_q)) = T_q$ for any prime $q \nmid D$, as well as $\det \circ \rho_\mathbb{T} = \widehat{\det \circ \overline{\rho}}$.*

Proof. Let K_χ be the finite extension of $\mathbb{Q}_p$ obtained by attaching the Hecke eigenvalues of f_χ to $\mathbb{Q}_p$. Let $\rho = \prod_{\chi \in \mathcal{S}} \rho_{f_\chi} : \mathrm{Gal}(M^{\overline{\rho}} L^\epsilon / K) \to \mathrm{GL}_2(\prod_{\chi \in \mathcal{S}} K_\chi)$ be the representation obtained by gluing all representations ρ_{f_χ}'s of $\mathrm{Gal}(M^{\overline{\rho}} L^\epsilon / L)$ obtained from the eigenforms f_χ's. Each f_χ gives us a homomorphism $\phi_\chi : \mathbb{T} \to K_\chi$ which sends each Hecke operator to its f_χ-eigenvalue. By definition of $\mathbb{T}$ the map $(\prod_{\chi \in \mathcal{S}} \phi_\chi) : \mathbb{T} \to \prod_{\chi \in \mathcal{S}} K_\chi$ is injective.

Now, $\mathrm{tr}(\rho)$ actually takes values in $(\prod_{\chi \in \mathcal{S}} \phi_\chi)(\mathbb{T})$. As $\overline{\rho}$ is absolutely irreducible, we get, from a theorem of Carayol [Car94, Th. 2], that there exists a representation $\rho_\mathbb{T} : \mathrm{Gal}(M^{\overline{\rho}} L^\epsilon / K) \to \mathrm{GL}_2(\mathbb{T})$ such that $\mathrm{tr}(\rho_\mathbb{T}) = \mathrm{tr}(\rho)$ and $\det(\rho_\mathbb{T}) = \det(\rho)$. So, for a prime $q \nmid D$, $\mathrm{tr}(\rho_\mathbb{T}(\mathrm{Frob}_q)) = T_q$ and $\det(\rho_\mathbb{T})$ is just the Teichmüller lift of $\det \overline{\rho}$ as the same is true for all f_χ's. Now, as $\mathrm{tr}\rho_\mathbb{T}(\mathrm{Frob}_q) \equiv \mathrm{tr}\overline{\rho}(\mathrm{Frob}_q) \pmod{\mathfrak{m}_\mathbb{T}}$ and $\overline{\rho}$ is absolutely irreducible, it follows that $\rho_\mathbb{T} \pmod{\mathfrak{m}_\mathbb{T}} \equiv \overline{\rho}$ over $\mathbb{F}$ and hence, $\rho_\mathbb{T}$ (or a conjugate of it), when seen as a representation of G_K, is a deformation of $\overline{\rho}$. From now on, we always consider $\rho_\mathbb{T}$ as a representation of G_K, unless mentioned otherwise.

Since D is the Artin conductor of $\overline{\rho}$, it follows that a prime q of K ramifies in $M^{\overline{\rho}}$ if and only if $q \in \{\ell \text{ is a prime of } K \mid \ell|D\} \cup \{S_\infty\}$. As $M^{\overline{\rho}}L^\epsilon$ is unramified over $M^{\overline{\rho}}$, it follows immediately from the construction that $\rho_{\mathbb{T}}$ is unramified outside $\{\ell \text{ is a prime of } K \mid \ell|D\} \cup \{S_\infty\}$. As $M^{\overline{\rho}}L^\epsilon$ is an abelian extension of L, it follows, from the construction of $\rho_{\mathbb{T}}$, that $\rho_{\mathbb{T}}(G_L)$ is an abelian group. Let $\Gamma_{\rho_{\mathbb{T}}}$ be the subgroup of $\mathrm{im}(\rho_{\mathbb{T}})$ introduced in (1.1). Since $\rho_{\mathbb{T}}(G_L)$ is abelian, the action of $\overline{H}^{\mathrm{ad}}$ on $\Gamma_{\rho_{\mathbb{T}}}$, given in Lemma 2.9 is trivial. Hence, by Theorem 1.1, $\rho_{\mathbb{T}}$ is dihedral. $\square$

Let $\sigma \in G_K \setminus G_L$. As $\rho_{\mathbb{T}}$ is dihedral, there exists a character $\chi_{\mathbb{T}} : G_L \to \mathbb{T}^\times$ deforming $\overline{\chi}$ such that after choosing a suitable basis, $\rho_{\mathbb{T}}|_{G_L} = \chi_{\mathbb{T}} \oplus \chi_{\mathbb{T}}^\sigma$, where $\chi_{\mathbb{T}}^\sigma(h) = \chi_{\mathbb{T}}(\sigma h \sigma^{-1})$ for all $h \in G_L$.

Lemma 4.6. *$\mathbb{T}$ is the $W(\mathbb{F})$-subalgebra of $\mathrm{End}_{\mathcal{O}}(\mathcal{W})$ generated by Hecke operators T_q with $q \nmid D$ and U_ℓ with $\ell \mid D$, that is, all U_ℓ for $\ell \mid D$ lie in $\mathbb{T}$.*

Proof. Let $\chi \in \mathcal{S}$. Now, if $\ell \mid D$ and $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible, then ℓ does not split in L and we know from [RT83] that the U_ℓ eigenvalue of f_χ is 0 (see [Jar97, Section 3 and Theorem 6.1] or [New15, Theorem 1.1]). If $\ell \mid D$ and $\overline{\rho}|_{G_{K_\ell}}$ is not absolutely irreducible, then, as $\overline{\rho}$ is dihedral, $\overline{\rho}|_{G_{K_\ell}} = \eta_\ell \oplus \zeta_\ell$ for some characters ζ_ℓ and η_ℓ. Moreover, the assumption 5 implies that one of the characters, say η_ℓ, is unramified and both the characters ζ_ℓ and η_ℓ take values in $\mathbb{F}^\times$. Let ℓ' be a prime of $M^{\overline{\rho}}$ lying above ℓ. So, $M^{\overline{\rho}}_{\ell'}$ is an abelian extension of K_ℓ. As $M^{\overline{\rho}}L^\epsilon$ is unramified over $M^{\overline{\rho}}$, the extension $M^{\overline{\rho}}L^\epsilon_{\ell''}$ of K_ℓ is also abelian for any prime ℓ'' of $M^{\overline{\rho}}L^\epsilon$ lying above ℓ. Thus, the decomposition group D_ℓ of ℓ in $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/K)$ is abelian.

Suppose first that ℓ is not split in L. Since $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/M^{\overline{\rho}})$ is an abelian and normal subgroup of $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/K)$, we get an action of $\mathrm{Gal}(M^{\overline{\rho}}/K)$ on it by conjugation. Now, $M^{\overline{\rho}}L^\epsilon$ is an abelian extension of L. As a consequence, we get that the action of $\mathrm{Gal}(M^{\overline{\rho}}/K)$ on $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/M^{\overline{\rho}})$ by conjugation factors through $\mathrm{Gal}(L/K)$. Note that $\mathrm{Gal}(L/K)$ acts by inversion on $\mathrm{Gal}(L^\epsilon/L)$ and hence, on $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/M^{\overline{\rho}})$. Thus, we see that D_ℓ does not contain any nontrivial element of $\mathrm{Gal}(M^{\overline{\rho}}L^\epsilon/M^{\overline{\rho}})$. So, it follows that $M^{\overline{\rho}}L^\epsilon_{\ell''} = M^{\overline{\rho}}_{\ell'}$ and hence, $|D_\ell| = |\overline{\rho}(G_{K_\ell})|$. Thus, $\rho_\chi|_{G_{K_\ell}}$ is just the sum of the Teichmüller lifts of ζ_ℓ and η_ℓ. Therefore, from [RT83], we get that the U_ℓ eigenvalue of f_χ is the Teichmüller lift of $\eta_\ell(\mathrm{Frob}_\ell)$ (see [Jar97, Section 3 and Theorem 6.1] and [New15, Theorem 1.1] as well). Thus, we see that for any $\ell|D$ which is not split in L, U_ℓ acts like a constant belonging to $W(\mathbb{F})$ on all f_χ's and hence, its image in $\mathrm{End}_{\mathcal{O}}(\mathcal{W})$ lies in $W(\mathbb{F})$.

Now, suppose ℓ is split in L. Then, we can identify G_{K_ℓ} with a subgroup of G_L. Thus, $\rho_{f_\chi}|_{G_{K_\ell}} = \eta_{\chi,\ell} \oplus \zeta_{\chi,\ell}$ where $\eta_{\chi,\ell}, \zeta_{\chi,\ell} : G_{K_\ell} \to \mathcal{O}^\times$ are characters deforming η_ℓ and ζ_ℓ, respectively. As η_ℓ is unramified at ℓ and $M^{\overline{\rho}}L^\epsilon$ is an unramified extension of $M^{\overline{\rho}}$, it follows, from the construction of ρ_{f_χ}, that $\eta_{\chi,\ell}$ is unramified at ℓ. Since ζ_ℓ is a ramified character of G_{K_ℓ}, $\zeta_{\chi,\ell}$ is also a ramified character of G_{K_ℓ}. Therefore, from [RT83], we get that the U_ℓ eigenvalue of f_χ is $\eta_{\chi,\ell}(\mathrm{Frob}_\ell)$ (see [Jar97, Section 3 and Theorem 6.1] and [New15, Theorem 1.1] as well).

As ℓ is split in L, we get, by the same logic as above, that $\rho_{\mathbb{T}}|_{G_{K_\ell}} = \eta_{\mathbb{T},\ell} \oplus \zeta_{\mathbb{T},\ell}$, where $\eta_{\mathbb{T},\ell}$, $\zeta_{\mathbb{T},\ell} : G_{K_\ell} \to \mathbb{T}^\times$ are characters deforming η_ℓ and ζ_ℓ, respectively. Now, the eigenform f_χ induces a homomorphism $\phi_\chi : \mathbb{T} \to \mathcal{O}$ of $W(\mathbb{F})$-algebras. Since ρ_{f_χ} is absolutely irreducible and $\mathrm{tr}(\rho_{f_\chi}(g)) = \mathrm{tr}(\phi_\chi \circ \rho_{\mathbb{T}}(g))$ for all $g \in G_K$, it follows, from the Brauer-Nesbitt theorem, that ρ_{f_χ} and $\phi_\chi \circ \rho_{\mathbb{T}}$

are isomorphic over $\mathcal{O}$. Therefore, by using the Brauer-Nesbitt theorem for G_{K_ℓ}, we conclude that $\{\phi_\chi \circ \eta_{\mathbb{T},\ell}, \phi_\chi \circ \zeta_{\mathbb{T},\ell}\} = \{\eta_{\chi,\ell}, \zeta_{\chi,\ell}\}$. Note that $\eta_{\mathbb{T},\ell}$ and $\eta_{\chi,\ell}$ both deform η_ℓ and $\eta_\ell \neq \zeta_\ell$. Therefore, we get $\phi_\chi \circ \eta_{\mathbb{T},\ell} = \eta_{\chi,\ell}$. Thus, we see that $(\phi_\chi \circ \eta_{\mathbb{T},\ell})(g) = 1$ for all $g \in I_\ell$ and all $\chi \in \mathcal{S}$. As $\cap_{\chi \in \mathcal{S}} \ker(\phi_\chi) = (0)$, we see that $\eta_{\mathbb{T},\ell}(g) = 1$ for all $g \in I_\ell$ and hence, $\eta_{\mathbb{T},\ell}$ is an unramified character of G_{K_ℓ}.

Now, the U_ℓ-eigenvalue of f_χ is $\eta_{\chi,\ell}(\mathrm{Frob}_\ell)$. Moreover, $\eta_{\chi,\ell}(\mathrm{Frob}_\ell)$ is also the image of the Hecke operator $\eta_{\mathbb{T},\ell}(\mathrm{Frob}_\ell) \in \mathbb{T}$ under the homomorphism ϕ_χ. Hence, the $\eta_{\mathbb{T},\ell}(\mathrm{Frob}_\ell)$-eigenvalue of f_χ is also $\eta_{\chi,\ell}(\mathrm{Frob}_\ell)$. Thus, the Hecke operator $U_\ell - \eta_{\mathbb{T},\ell}(\mathrm{Frob}_\ell)$ acts like 0 on f_χ for all $\chi \in \mathcal{S}$. Hence, its image in $\mathrm{End}_{\mathcal{O}}(\mathcal{W})$ is 0, which means that the image of U_ℓ in $\mathrm{End}_{\mathcal{O}}(\mathcal{W})$ lies in $\mathbb{T}$. Combining this with our conclusions for primes $\ell | D$ which are not split in L, we get the lemma. ☐

As a consequence, we get the following lemma:

Lemma 4.7. *$\mathbb{T}$ is a free $W(\mathbb{F})$-module of rank $\prod_{i=1}^{j} p^{m_j}$.*

Proof. As $\mathbb{T}$ is a finitely generated module over $W(\mathbb{F})$ which is torsion free, it is free. By Lemma 4.6 and the q-expansion principle, $\mathbb{T} \otimes_{W(\mathbb{F})} \mathcal{O}$ is the $\mathcal{O}$-linear dual of $\mathcal{W}$. Therefore, the $W(\mathbb{F})$-rank of $\mathbb{T}$ is the same as the $\mathcal{O}$-rank of $\mathcal{W}$. Now, $\{f_\chi : \chi \in \mathcal{S}\}$ is a set of $\mathcal{O}$-linearly independent elements of $\mathcal{W}$. Hence, the $\mathcal{O}$-rank of $\mathcal{W}$ is $|\{f_\chi : \chi \in \mathcal{S}\}| = |\mathcal{S}|$. But $|\mathcal{S}|$ is the number of different characters of $\mathrm{Gal}(L^\epsilon/L) = \prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z}$. This number is exactly $\prod_{i=1}^{j} p^{m_j}$. Hence, the lemma follows. ☐

Remark 4.8. *We proved Lemma 4.7 by proving first that $\mathbb{T}$ is the full Hecke algebra acting on $\mathcal{W}$ and then using the duality coming from the q-expansion principle. We could also prove Lemma 4.7 using a different method as follows: let $\mathbb{T}'$ be the full Hecke algebra (generated by all the Hecke operators over $W(\mathbb{F})$) acting faithfully on $\mathcal{W}$. From the proof of Lemma 4.7, it follows that $\mathbb{T}'$ is a free $W(\mathbb{F})$-module of rank $\prod_{i=1}^{j} p^{m_j}$. Now, $\mathbb{T}$ is a free $W(\mathbb{F})$-submodule of $\mathbb{T}'$ and hence, the rank of $\mathbb{T}$ over $W(\mathbb{F})$ is less than or equal to the rank of $\mathbb{T}'$ over $W(\mathbb{F})$. Let $\mathcal{O}_K$ be the ring of integers of K. For $f \in \mathcal{W}$ and an ideal I of $\mathcal{O}_K$, denote by $C(I, f)$ the Fourier coefficient of f corresponding to I. If the rank of $\mathbb{T}$ is less than the rank of $\mathbb{T}'$, then the perfect duality between $\mathbb{T}'$ and $\mathcal{W}$ would imply that there exists a non-zero $f \in \mathcal{W}$ such that $C(I, f) = 0$ for any ideal I of $\mathcal{O}_K$ which is co-prime to D. As $\mathcal{W}$ is generated by Hilbert modular newforms of level D, [SW93, Theorem 3.1] implies that such a non-zero f does not exists in $\mathcal{W}$ giving us a contradiction. Hence, we get that the rank of $\mathbb{T}$ equals the rank of $\mathbb{T}'$, which proves Lemma 4.7.*

A prime ℓ of K is called a *vexing prime* if $\overline{\rho}$ ramifies at ℓ, $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible, $\overline{\rho}|_{I_\ell}$ is *not* absolutely irreducible and $[K_\ell(\mu_p) : K_\ell] = 2$. We will now define minimal deformation problems, following [CG18].

Definition 4.9. *Let R be an object of $\mathcal{C}$. A deformation $\rho : G_K \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ is called minimal if it satisfies all the following properties:*

1. $\det \rho = \widehat{\det(\overline{\rho})}$.

2. *ρ is unramified at primes at which $\overline{\rho}$ is unramified.*

3. *If ℓ is a vexing prime, then $\rho(I_\ell) \simeq \overline{\rho}(I_\ell)$.*

4. *If ℓ is a prime such that $\overline{\rho}|_{G_{K_\ell}}$ is not absolutely irreducible, then ρ^{I_ℓ} is a rank 1 direct summand of ρ as an R-module.*

For $K = \mathbb{Q}$, this is just [CG18, Definition 3.1].

It follows, from the proof of [DDT97, Theorem 2.41], that the functor from $\mathcal{C}$ to the category of sets sending an object R of $\mathcal{C}$ to the set of continuous, minimal deformations of $\overline{\rho}$ to $\mathrm{GL}_2(R)$ is representable by a ring in $\mathcal{C}$ (see [CG18, Section 3.1] as well). We will denote this ring by $R^{\min}$ and we will denote the universal minimal deformation by $\rho^{\min}$.

Proposition 4.10. *Let S be the union of S_∞ and the set of primes ℓ of K such that $\ell \mid D$, $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible and ℓ is not a vexing prime. Then, $R^{\min} \simeq (R_S^{\mathrm{univ}})^0$.*

Proof. A minimal deformation is unramified at primes of K not dividing D. Let ℓ be a prime dividing D. By the definition of minimal deformations, if ℓ is a vexing prime, then $\rho^{\min}$ is a deformation of $\overline{\rho}$ which is relatively unramified at ℓ, i.e. if ℓ is a vexing prime, then $\rho^{\min}(I_\ell) \simeq \overline{\rho}(I_\ell)$. If $\overline{\rho}|_{G_{K_\ell}}$ is not absolutely irreducible, then we have assumed that the subspace $(\overline{\rho})^{I_\ell}$ has dimension 1. So, $\overline{\rho}|_{I_\ell} = 1 \oplus \delta$ for some non-trivial character δ. The minimality condition means that $(\rho^{\min})^{I_\ell}$ is a free $R^{\min}$-module of rank 1 which is a direct summand of $\rho^{\min}$ as an $R^{\min}$-module. As $\det \rho^{\min}$ is the Teichmüller lift of $\det \overline{\rho}$, we get that $\rho^{\min}|_{I_\ell} \simeq \begin{pmatrix} 1 & * \\ 0 & \widehat{\delta} \end{pmatrix}$. We have two cases:

1. δ **is tamely ramified:** In this case, $\rho^{\min}(I_\ell)$ factors through the tame inertia quotient of I_ℓ and is hence abelian. This means that the $*$ above is necessarily 0 as $\widehat{\delta}$ is non-trivial. Therefore, we get that $\rho^{\min}|_{I_\ell} \simeq 1 \oplus \widehat{\delta}$. Thus, $\rho^{\min}$ is a deformation of $\overline{\rho}$ which is relatively unramified at ℓ.

2. δ **is wildly ramified:** Let W_ℓ be the wild inertia group at ℓ. As $\ell \nmid p$, W_ℓ does not admit any non-trivial pro-p quotient. So, $\rho^{\min}|_{W_\ell} \simeq 1 \oplus \widehat{\delta}|_{W_\ell}$. As W_ℓ is a normal subgroup of I_ℓ and $1 \neq \widehat{\delta}|_{W_\ell}$, we see that the submodules of $\rho^{\min}$ on which W_ℓ acts via 1 or $\widehat{\delta}$ are also I_ℓ-invariant. Therefore, we get that $\rho^{\min}|_{I_\ell} \simeq 1 \oplus \widehat{\delta}$. Hence, $\rho^{\min}$ is a deformation of $\overline{\rho}$ which is relatively unramified at ℓ.

Note that the primes considered above are exactly the primes of K which divide D but are not in S. Being a minimal deformation does not put any conditions on any other primes of K dividing D. Thus, $\rho^{\min}$ is relatively unramified outside S and has constant determinant. On the other hand, any deformation of $\overline{\rho}$ which is relatively unramified outside S with constant determinant is also minimal by definition. Hence, we get morphisms $\alpha : R^{\min} \to (R_S^{\mathrm{univ}})^0$ and $\beta : (R_S^{\mathrm{univ}})^0 \to R^{\min}$. It follows, from looking at the corresponding deformations, that both morphisms $\alpha \circ \beta$ and $\beta \circ \alpha$ are the identity and hence, $R^{\min} \simeq (R_S^{\mathrm{univ}})^0$. $\square$

Remark 4.11. *The proof of Proposition 4.10 above is independent of the hypothesis*

$$\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^{\sigma})) = 0.$$

Hence, the proposition still holds without this hypothesis.

As a consequence, we get the following corollary: Recall that, we have assumed that the p-part of $A(L)$ equals $\prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z} \oplus W$ where $\mathrm{Gal}(L/K)$ acts trivially on W and by inversion on $\prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z}$.

Corollary 4.12. $R^{\min} \simeq W(\mathbb{F})[X_1, \cdots, X_j]/((1+X_1)^{p^{m_1}} - 1, \cdots, (1+X_j)^{p^{m_j}} - 1)$.

Proof. As in Proposition 4.10, let S be the union of S_∞ and the set of primes ℓ of K such that $\ell \mid D$, $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible and ℓ is not a vexing prime. Note that in the notation of the previous section, $S \cap S_0 = \emptyset$. Indeed, let $\ell \in S \cap S_0$ be a finite place. Firstly, $\ell \in S$ implies that $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible and ℓ is not a vexing prime. As $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible and $\overline{\rho}$ ramifies at ℓ, the assumption that ℓ is not a vexing prime means that either $[K_\ell(\mu_p) : K_\ell] \neq 2$ or $\overline{\rho}|_{I_\ell}$ is absolutely irreducible. Now, if $q \in S_1 \cup S_2$, then it follows, from the definitions of S_1 and S_2, that the projective image of $\overline{\rho}|_{G_{K_q}}$ is cyclic. Therefore, the image of $\overline{\rho}|_{G_{K_q}}$ is abelian and, hence, $\overline{\rho}|_{G_{K_q}}$ is not absolutely irreducible. So, $\ell \notin S_1 \cup S_2$ which means that $\ell \in S_3$. From the definition of S_3, we get that $[K_\ell(\mu_p) : K_\ell] = 2$ and $|\mathrm{ad}\overline{\rho}(I_\ell)| = 2$. Thus, the projective image of $\overline{\rho}|_{I_\ell}$ is a cyclic group (of order 2). Hence, the image of $\overline{\rho}|_{I_\ell}$ is abelian. So, it follows that $\overline{\rho}|_{I_\ell}$ is not absolutely irreducible. This contradicts our assumption that ℓ is not a vexing prime. Hence, we get that $S \cap S_0 = \emptyset$.

So, by Corollary 3.14, we see that $(R_S^{\mathrm{univ}})^0 \simeq W(\mathbb{F})[[X_1, \cdots, X_n]]/((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_n)^{p^{e_n}} - 1)$ where $\mathrm{Gal}(L_S/L) = \prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z} \oplus V$. Recall that, L_S is the maximal abelian p-extension of L unramified outside primes of L lying above S and $\mathrm{Gal}(L/K)$ acts trivially on V and by inversion on $\prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}$.

Let $\ell \in S$ and let L' be a sub-extension of L_S such that the Galois group $\mathrm{Gal}(L/K)$ acts by inversion on $\mathrm{Gal}(L'/L)$. As $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible, ℓ is not split in L. Let ℓ' be the unique prime of L lying above ℓ. By local class field theory, if the elementary abelian p-extension L'/L is ramified at ℓ', then $\mu_p \subset L_{\ell'}$. As p is odd, ℓ is not a prime lying above p, and $[L_{\ell'} : K_\ell] = 2$, it follows that either $\mu_p \not\subset K_\ell$ or all the p-power roots of unity lying in $L_{\ell'}$ are in K_ℓ. As $\mathrm{Gal}(L/K)$ acts on $\mathrm{Gal}(L'/L)$ by inversion, the latter case does not occur. Therefore, ℓ is inert in L and $[K_\ell(\mu_p) : K_\ell] = 2$. This means that $\overline{\rho}|_{I_\ell}$ is not absolutely irreducible. But as ℓ is not a vexing prime and $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible, these two conditions do not hold.

So, it follows that L' is unramified at all $\ell \in S$. It is also unramified at all archimedean places of L as it is a p-extension of L and p is odd. Hence, it is an extension of L unramified everywhere. Therefore, we see that the maximal sub-extension of L_S fixed by V is an abelian, unramified p-extension of L on which $\mathrm{Gal}(L/K)$ acts by inversion and since $L^\epsilon \subset L_S$, the sub-extension is L^ϵ. Therefore, $\prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z} = \prod_{i=1}^{j} \mathbb{Z}/p^{m_i}\mathbb{Z}$ and the corollary follows. □

Before proceeding further, let us record an observation, which follows from the work done so far:

Proposition 4.13. *Let $\overline{\rho}$ be a dihedral representation satisfying all the hypotheses of Set-up 4.2 with the possible exception of Assumption 6. Then the following statements hold:*

(a) Every infinitesimal deformation of $\overline{\rho}$ relatively unramified outside S with constant determinant is relatively unramified outside S_∞.

(b) The tangent spaces of $R^{\min}/(p)$ and $(R^{\mathrm{univ}}_{S_\infty})^0/(p)$ have the same dimension as $\mathbb{F}$-vector spaces.

Proof. (a) As before, let S be the union of S_∞ and the set of primes ℓ of K such that $\ell \mid D$, $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible and ℓ is not a vexing prime. Let $\rho : G_K \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ be an infinitesimal deformation of $\overline{\rho}$ relatively unramified outside S with constant determinant. Let Γ_ρ be the group introduced in (1.1). Therefore, if $\mathcal{M}$ is the extension of K fixed by $\ker(\rho)$, then $\mathcal{M} \subset M^{\overline{\rho}}(S)$ and $\mathrm{Gal}(\mathcal{M}/M^{\overline{\rho}}) = \Gamma_\rho$. Now, Γ_ρ is an elementary abelian p-group. From Lemma 2.9, we get an action of $\overline{G}$ on Γ_ρ via conjugation and the action factors through $\overline{G}^{\mathrm{ad}}$. As p is odd, we see, from Lemma 2.11 and Corollary 2.12, that as a $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module, Γ_ρ is a direct sum of simple $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules occurring in $\mathrm{ad}^0(\overline{\rho})_{\mathbb{F}}$.

Recall that, $\mathrm{Gal}(M^{\overline{\rho}}/M^{\mathrm{ad}}) \simeq C := \ker(\overline{G} \twoheadrightarrow \overline{G}^{\mathrm{ad}})$. By Lemma 2.9, we see that the action of $\mathrm{Gal}(M^{\overline{\rho}}/M^{\mathrm{ad}})$ on $\mathrm{Gal}(\mathcal{M}/M^{\overline{\rho}})$ by conjugation corresponds to conjugation by scalar matrices and hence, this action is trivial. As $\mathrm{Gal}(M^{\overline{\rho}}/M^{\mathrm{ad}})$ is cyclic, we see that $\mathrm{Gal}(\mathcal{M}/M^{\mathrm{ad}}) \simeq C \times \Gamma_\rho$. Hence, there is a unique extension $\mathcal{M}^{\mathrm{ad}}$ of M^{ad} contained in $\mathcal{M}$ such that $\mathrm{Gal}(\mathcal{M}^{\mathrm{ad}}/M^{\mathrm{ad}}) \simeq \Gamma_\rho$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules. As $p \nmid |\mathrm{Gal}(M^{\overline{\rho}}/M^{\mathrm{ad}})|$ and $\mathcal{M}^{\mathrm{ad}}.M^{\overline{\rho}} = \mathcal{M} \subset M^{\overline{\rho}}(S)$, it follows that $\mathcal{M}^{\mathrm{ad}} \subset M^{\mathrm{ad}}(S)$.

Keeping the notation of the previous section, let ℓ be a prime of K lying in S, $\tilde{\ell}$ be a prime of M^{ad} lying above ℓ and D_ℓ be a decomposition group of ℓ inside $\mathrm{Gal}(M^{\mathrm{ad}}/K)$. Suppose $\mu_p \subset M^{\mathrm{ad}}_{\tilde{\ell}}$ and let $\chi_p^{(\ell)}$ be the modulo p cyclotomic character viewed as a character of D_ℓ. As $\ell \in S$, $\overline{\rho}|_{G_{K_\ell}}$ is absolutely irreducible and hence, ℓ is not split in L. Let ℓ' be the unique prime of L lying above ℓ. If $\chi_p^{(\ell)} = \epsilon|_{D_\ell}$, then this means that $\mu_p \subset L_{\ell'}$ and $\mu_p \not\subset K_\ell$. Thus, we see that ℓ is unramified in L. But this means that $\overline{\rho}|_{I_\ell}$ is reducible. As $\mu_p \subset L_{\ell'}$, we also have $[K_\ell(\mu_p) : K_\ell] = 2$. This implies that ℓ is a vexing prime which contradicts the assumption that $\ell \in S$. Therefore, we get that $\chi_p^{(\ell)} \neq \epsilon|_{D_\ell}$.

As a consequence, we get that $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathrm{Ind}_{D_\ell}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(\ell)})_{\mathbb{F}_p}), C(\epsilon)) = 0$. From the proof of Corollary 4.12, we know that $S \cap S_0 = \emptyset$. Hence, from the proof of Proposition 3.4, we get

$$\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathrm{Ind}_{D_\ell}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(\ell)})_{\mathbb{F}_p}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0.$$

Thus, we see that for $\ell \in S$, either $\mu_p \not\subset M^{\mathrm{ad}}_{\tilde{\ell}}$ or $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathrm{Ind}_{D_\ell}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(\ell)})_{\mathbb{F}_p}), \mathrm{ad}^0(\overline{\rho})_{\mathbb{F}}) = 0$. So, Proposition 3.3 implies

$$\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(G^{\mathrm{ab}}_{M^{\mathrm{ad}},S}, \mathrm{ad}^0(\overline{\rho})) = \mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), \mathrm{ad}^0(\overline{\rho})).$$

Therefore, from global class field theory, we see that $\mathcal{M}^{\mathrm{ad}}$ is an everywhere unramified extension of M^{ad} and hence, $\mathcal{M}^{\mathrm{ad}} \subset M^{\mathrm{ad}}(S_\infty)$. Therefore, $\mathcal{M}^{\mathrm{ad}}.M^{\overline{\rho}} = \mathcal{M} \subset M^{\overline{\rho}}(S_\infty)$. Thus, we see that every infinitesimal deformation of $\overline{\rho}$ relatively unramified outside S with constant determinant is relatively unramified outside S_∞.

(b) It follows, from Remark 4.11, that for the $\overline{\rho}$ considered in the proposition, we have $R^{\min} \simeq (R_S^{\text{univ}})^0$. As it is trivial that every infinitesimal deformation of $\overline{\rho}$ relatively unramified outside S_∞ with constant determinant is relatively unramified outside S, using (a), it follows from [Maz89] that the tangent spaces of $(R_S^{\text{univ}})^0/(p)$ and $(R_{S_\infty}^{\text{univ}})^0/(p)$ have the same dimension as vector spaces over $\mathbb{F}$. $\square$

We will now prove that the representation $\rho_{\mathbb{T}}$ constructed above is a minimal deformation of $\overline{\rho}$ over $\mathbb{T}$.

Lemma 4.14. *The representation $\rho_{\mathbb{T}} : G_K \to \mathrm{GL}_2(\mathbb{T})$, constructed in Proposition 4.5, is a minimal deformation of $\overline{\rho}$.*

Proof. We have already seen in Proposition 4.5 that $\rho_{\mathbb{T}}$ is a deformation of $\overline{\rho}$. Note that $\rho_{\mathbb{T}}$ factors through $\mathrm{Gal}(M^{\overline{\rho}}L^{\epsilon}/K)$. As $M^{\overline{\rho}}L^{\epsilon}$ is unramified over $M^{\overline{\rho}}$, we see that $\rho_{\mathbb{T}}$, when seen as a representation of G_K, is a relatively unramified deformation of $\overline{\rho}$ with constant determinant and hence, a minimal deformation of $\overline{\rho}$ (in the sense of Definition 4.9). $\square$

Proof of Theorem 1.8. Recall that, we have denoted by $\rho^{\min}$ the universal minimal deformation of $\overline{\rho}$ taking values in $\mathrm{GL}_2(R^{\min})$. Now, $\phi_{\mathbb{T}} : R^{\min} \to \mathbb{T}$ is the map induced by the minimal deformation $\rho_{\mathbb{T}}$. For all primes $q \nmid D$, $T_q = \mathrm{tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_q))$. Therefore, $T_q = \phi_{\mathbb{T}}(\mathrm{tr}(\rho^{\min}(\mathrm{Frob}_q)))$ for all primes $q \nmid D$. As $\mathbb{T}$ is generated by T_q's, with $q \nmid D$, over $W(\mathbb{F})$ and T_q is in the image of $\phi_{\mathbb{T}}$ for all $q \nmid D$, it follows that $\phi_{\mathbb{T}}$ is surjective.

From Corollary 4.12, we see that $R^{\min}$ is a free $W(\mathbb{F})$-module of rank $\prod_{i=1}^{j} p^{m_j}$. Now, $\phi_{\mathbb{T}}$ is a surjective map from $R^{\min}$ to $\mathbb{T}$ which is also a free module of the same rank. Hence, $\phi_{\mathbb{T}}$ is an isomorphism. So, we have $R^{\min} \simeq \mathbb{T}$. $\square$

Remark 4.15. *Reducing both $R^{\min}$ and $\mathbb{T}$ modulo the maximal ideal of $W(\mathbb{F})$, we get an $R = \mathbb{T}$ theorem in characteristic p. Note that then $\mathbb{T}$ is the Hecke algebra acting on a* subspace *of the generalised eigenspace of characteristic p parallel weight 1 Hilbert modular forms of level D corresponding to $\overline{\rho}$. The whole generalised eigenspace might be bigger due to the existence of non-liftable forms. However, if we know the existence of a surjective map $R^{\min}/(p) \to \bar{\mathbb{T}}$, where $\bar{\mathbb{T}}$ is the full Hecke algebra acting faithfully on the generalised eigenspace of characteristic p parallel weight 1 Hilbert modular forms of level D corresponding to $\overline{\rho}$, then we can conclude that $\mathbb{T}/(p) = \bar{\mathbb{T}}$ under the Set-up 4.2. Hence, in this case, there are no non-liftable forms in the generalised eigenspace of characteristic p parallel weight 1 Hilbert modular forms of level D corresponding to $\overline{\rho}$.*

Remark 4.16. *If $\mathrm{Hom}_{\overline{G}^{\mathrm{ad}}}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^{\sigma})) \neq 0$, then, as seen in Remark 3.11, there exists a non-dihedral infinitesimal deformation which is relatively unramified everywhere. Hence, we get a non-dihedral infinitesimal minimal deformation which means that, in this case, the universal minimal deformation is not dihedral. So, the methods of this article will not be useful to prove an $R^{\min} = \mathbb{T}$ theorem. However, if one can prove an '$R^{\min} = \mathbb{T}$'-statement (in the spirit of Calegari-Geraghty ([CG18])) in such cases, then one gets non-liftable forms in the generalised eigenspace of* *(the system of eigenvalues corresponding to) $\overline{\rho}$ in characteristic p. On the other hand, if one has examples of non-liftable forms in the generalised eigenspace of (the system of eigenvalues corresponding to) $\overline{\rho}$ in characteristic p, then the existence of a surjective map $R^{\min} \to \mathbb{T}$ theorem, together with the previous remark, will imply that the universal minimal deformation is not dihedral and hence, $\mathrm{Hom}_{\overline{G}^{\mathrm{ad}}}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^{\sigma})) \neq 0$. So using such $R = \mathbb{T}$ theorems in the dihedral case, one can use the information about the class group $A(M^{\mathrm{ad}})$ to get information about non-liftability and vice versa. Note that $R^{\min} = \mathbb{T}$ has been proved for $K = \mathbb{Q}$ by Calegari-Geraghty ([CG18]), so we know that this correspondence is true for $K = \mathbb{Q}$.*

Note that we can remove assumption 5 from Set-up 4.2 and look at deformations unramified outside $S(\supseteq S_\infty)$ with constant determinant for a finite set S of primes of K with $S \cap (S_0 \cup S_p) = \emptyset$ instead of minimal deformations. In this case, our methods will not give an $R = \mathbb{T}$ theorem, but we can still conclude the following:

Proposition 4.17. *Let $\overline{\rho}$ be a dihedral representation satisfying all the assumptions of Set-up 4.2 except possibly assumption 5. Let $\mathcal{R}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ such that the residue field of $\mathcal{R}$ contains $\mathbb{F}$. Let $S(\supset S_\infty)$ be a finite set of primes of K with $S \cap (S_0 \cup S_p) = \emptyset$. If $\rho : G_K \to \mathrm{GL}_2(\mathcal{R})$ is a deformation of $\overline{\rho}$ with constant determinant which is unramified outside S, then there exists a classical Hilbert modular eigenform f of parallel weight one over K such that ρ is isomorphic to the Galois representation attached to f.*

Proof. From Theorem 1.5, it follows that ρ is a dihedral representation. From Lemma 4.3, we conclude the existence of the parallel weight one eigenform f over K having the required property. □

See [Calar, Theorem 1.1] for a similar but much stronger result for $K = \mathbb{Q}$.

Remark 4.18. *To conclude that ρ is dihedral we do not need the hypotheses 2 (K is totally real) and 3 ($\overline{\rho}$ is totally odd). Hence, if we further remove the assumptions that K is totally real and $\overline{\rho}$ is totally odd from the Proposition above, then we can still conclude, by automorphic induction ([Gel97], [Rog97]), that ρ comes from an automorphic representation for $\mathrm{GL}_2(K)$.*

5 Examples

In this section, we present several examples of irreducible dihedral representations $\overline{\rho} : G \to \mathrm{GL}_2(\mathbb{F})$ as in the rest of the article and determine whether their universal deformation relatively unramified outside a finite set S is dihedral or not. Most of the time we take $S = S_\infty$, i.e. we consider deformations that are relatively unramified at all finite places.

For $p = 2$, there is, in a sense, a generic source of examples where a dihedral representation deforms infinitesimally into a non-dihedral one. Denote by S_n the symmetric group on n letters. We start with an S_4-extension M/K of number fields. We know that the double-transpositions generate the normal subgroup $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of S_4 the quotient of which is isomorphic to $S_3 \cong D_3 \cong$

$\mathrm{SL}_2(\mathbb{F}_2)$. Moreover, the surjection $S_4 \twoheadrightarrow S_3$ is split by the natural map $S_3 \hookrightarrow S_4$ and the conjugation action by S_3 on V_4 is non-trivial and thus, after identifying $S_3 \cong \mathrm{SL}_2(\mathbb{F}_2)$, we have that V_4 becomes $I = \mathrm{Ind}_H^G(\overline{\chi}) = I(\overline{\chi}/\overline{\chi}^\sigma)$. We thus find the following commutative diagram with split exact rows:

$$\begin{tikzcd}
 & & \mathrm{Gal}(M/K) \arrow[d, "\sim"] \arrow[dd, bend right, "\rho"'] \arrow[dr, two heads] \arrow[ddr, "\overline{\rho}"] & & \\
0 \arrow[r] & V_4 \arrow[r] \arrow[d, hook, "\mathrm{id}\oplus 0"] & S_4 \arrow[r, two heads] \arrow[d, hook] & S_3 \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & I \oplus C(1) \arrow[r] & \mathrm{SL}_2(\mathbb{F}_2[\epsilon]/(\epsilon^2)) \arrow[r] & \mathrm{SL}_2(\mathbb{F}_2) \arrow[r] & 0
\end{tikzcd}$$

We thus see that ρ is an infinitesimal deformation of the representation $\overline{\rho}$. In order to satisfy Definition 2.2, we must extend the scalars of both $\overline{\rho}$ and ρ from $\mathbb{F}_2$ to $\mathbb{F}_4$. Then $\overline{\rho}$ is a dihedral representation admitting the non-dihedral deformation ρ. This situation occurs, for instance, for $K = \mathbb{Q}$ and the S_3-extension of $\mathbb{Q}$ given by the Hilbert class field of $Q(\sqrt{229})$. This is a totally real field and its ray class field ramifying only at infinity provides the desired S_4-extension of $\mathbb{Q}$.

For the other examples, we take $S = S_\infty$ (i.e. we only consider relatively unramified deformations), $p > 2$ and $\overline{\rho}$ that are unramified above p. In that case, the only condition in Theorem 1.5 is that the induced representation $I(\overline{\chi}/\overline{\chi}^\sigma)$ does not occur in the p-part of the class group of M^{ad}.

Let K be a number field and L a quadratic extension of K. For simplicity, we shall only consider cases when a chosen odd prime $q \neq p$ exactly divides the class number of L. Let M/L be the corresponding cyclic extension with Galois group $\mathbb{Z}/q\mathbb{Z}$ inside the Hilbert class field of L. Note that M/K is Galois. We shall further assume that the Galois group of M/K is not $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, whence it automatically is isomorphic to the dihedral group D_q. We fix a character $\overline{\chi} : G_L \to \mathbb{F}_{p^r}^\times$ of kernel G_M with r the multiplicative order of q modulo p. Note that $\overline{\chi}^\sigma = \overline{\chi}^{-1}$ for any $\sigma \in G_K \setminus G_L$.

Next consider the maximal elementary abelian p-extension M_1/M (resp. L_1/L) inside the Hilbert class field of M (resp. of L). We shall consider the group $\mathcal{G} := \mathrm{Gal}(M_1/M)$ as $\mathbb{F}_p[\mathrm{Gal}(M/K)]$-module. Then two mutually exclusive cases can arise.

(1) $[L_1 : L] = [M_1 : M]$.

This happens if and only if $M_1 = L_1 M$. This condition is furthermore equivalent to the only simple $\mathbb{F}_p[\mathrm{Gal}(M/K)]$-modules occuring in $\mathcal{G}$ being 1-dimensional (as $\mathbb{F}_p$-vector space) and, thus, either $C(1)$ or $C(\epsilon)$ with $\epsilon : G_K \twoheadrightarrow \mathrm{Gal}(L/K) \cong \{\pm 1\}$.

In this case, $\mathcal{G}$ is trivial as $\mathbb{F}_p[\mathrm{Gal}(M/L)]$-module. Let $\overline{\rho} := \mathrm{Ind}_{G_L}^{G_K}(\overline{\chi}^b)$ for any $b \in \mathbb{F}_q^\times$. In the notation used previously in the article, $\overline{H}^{\mathrm{ad}} = \mathrm{Gal}(M/L)$ and we have that $\mathcal{G}$ is trivial as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module. For any infinitesimal deformation $\rho : G_K \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ that is everywhere relatively unramified, the corresponding Γ_ρ is a quotient of $\mathcal{G}$, and thus trivial as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module. Consequently, by Theorem 1.1, ρ is dihedral, so that by Theorem 1.4, the universal relatively unramified deformation ρ^{univ} of $\overline{\rho}$ is dihedral.

(2) $[L_1 : L] < [M_1 : M]$.

This is the case if and only if $\mathcal{G}$ contains an irreducible $\mathbb{F}_p[\mathrm{Gal}(M/K)]$-module of $\mathbb{F}_p$-dimension at least 2.

In this case, by the representation theory of the dihedral group D_q, this representation is then $I := \mathrm{Ind}_{G_L}^{G_K}(\overline{\chi}^a)$ (defined over its minimal field of definition, but viewed as $\mathbb{F}_p[\mathrm{Gal}(M/K)]$-module) for some $a \in \mathbb{F}_q^\times$. Let now $b \in \mathbb{F}_q^\times$ be such that $2b = a$. Now consider $\overline{\rho} := \mathrm{Ind}_{G_L}^{G_K}(\overline{\chi}^b)$. In the notation used previously in the article, $\overline{G}^{\mathrm{ad}} = \mathrm{Gal}(M/K)$. Then $I = I((\overline{\chi}^b)/(\overline{\chi}^b)^\sigma)$, which occurs in $\mathrm{ad}(\overline{\rho})$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module according to Lemma 2.7. By Proposition 2.14, there is thus a deformation ρ_I of $\overline{\rho}$, which is non-dihedral according to Theorem 1.1. Consequently, the universal everywhere relatively unramified deformation ρ^{univ} of $\overline{\rho}$ is non-dihedral.

Note that we are sure to be in case (1) if p does not divide the quotient of the class number of M by the class number of L. Conversely, suppose that the p-part of the Hilbert class field of L equals L_1 (i.e. the p-part of the class group is an elementary abelian p-group) and assume $[L_1 : L] = [M_1 : M]$. Let M_2 be the p-part of the Hilbert class field of M. Then the p-Frattini quotient of $\mathrm{Gal}(M_2/M)$ is its maximal elementary abelian quotient $\mathrm{Gal}(M_1/M)$. The group $\mathrm{Gal}(M/L)$ is of order prime-to p and acts trivially on $\mathrm{Gal}(M_1/M)$, and, thus, by Proposition 2.10, it also acts trivially on $\mathrm{Gal}(M_2/M)$. There is thus an extension L_2/L such that $M_2 = L_2M$ with L_2 inside the Hilbert class field of L. By assumption, $L_2 = L_1$ and consequently $M_2 = M_1$. This means that p does not divide the quotient of the class number of M by the class number of L.

We summarise the discussion so far: Starting with a number field K, we take a quadratic extension L/K such that an odd prime $q \neq p$ exactly divides the class number of L and we let M be the corresponding cyclic $\mathbb{Z}/q\mathbb{Z}$-extension of L inside the Hilbert class field of L, assuming that $\mathrm{Gal}(M/K)$ is dihedral and that the p-part of the class group of L is of exponent p. Then we are in case (1) if and only if p does not divide the quotient of the class number of M by the class number of L; otherwise we are in case (2).

This observation allowed us to derive concrete examples of dihedral $\overline{\rho}$ the everywhere relatively unramified universal deformation of which remains dihedral (case (1)) and others for which this is not the case (case (2)), by computing class numbers of abelian extensions. All computations were performed using Magma [BCP97] under the assumption of the Generalised Riemann Hypothesis (GRH).

The first set of examples is for the base field $K = \mathbb{Q}$ and aims at providing examples for both cases. We want these examples to be non-trivial, in the sense that there does exist a non-trivial dihedral infinitesimal deformation. We did some small systematic calculation among imaginary quadratic fields L of class numbers $15, 21, 33, 35$. The four numbers are products of two distinct primes and we took p and q to be either choice. The results are summarised in the following table.

p	q	fields L	results
5	3	all imaginary quadratic fields of class number 15	case (2): discriminants: $-4219, -19867$ case (1): all others

3	5	all imaginary quadratic fields of class number 15 of abs. value of discriminants ≤ 19387	case (1): all fields
7	3	all imaginary quadratic fields of class number 21 of abs. value of discriminants ≤ 14419	case (2): discriminant: -8059 case (1): all others
3	7	all imaginary quadratic fields of class number 21 of abs. value of discriminants ≤ 5867	case (1): all fields
11	3	all imaginary quadratic fields of class number 33 of abs. value of discriminants ≤ 28163	case (1): all fields
3	11	all imaginary quadratic fields of class number 33 of abs. value of discriminants ≤ 1583	case (1): all fields
7	5	all imaginary quadratic fields of class number 35 of abs. value of discriminants ≤ 16451	case (1): all fields
5	7	all imaginary quadratic fields of class number 35 of abs. value of discriminants ≤ 4931	case (1): all fields

We also looked at examples for quadratic base fields K. In the first set of examples of this kind, let $K = \mathbb{Q}(\sqrt{d})$ for $d = 2, 5, 13, 17$. We ran through some CM extensions L of K that admit a class number that is divisible by two odd primes p, q to the first power, with q being 3 or 5. In total we computed 103 fields with these properties. All of them fell into case (1). Note that this also gives examples when our $R^{\min} = \mathbb{T}$-result (Theorem 1.8) holds because in these cases $\overline{\rho}$ is unramified above p, totally odd and the condition on the inertia invariants is satisfied because the orders of the inertia groups are 1 or 2.

In order not to only treat real quadratic fields, we also searched for and found a case-(1) example for the imaginary quadratic field $K = \mathbb{Q}(i)$ with $i = \sqrt{-1}$ for $q = 3$ and $p = 5$. It is obtained for the quadratic extension $L = K(\sqrt{-79i + 84})$ of K, which has class number 30. The field M is the unique unramified degree 3 extension of L, and its class number is 10.

Since in the range where we looked, case (2) seems to be rather rare in the above set-up, we looked explicitly for case (2)-examples for the base field $K = \mathbb{Q}$. We ran through imaginary quadratic fields of negative prime discriminant (for each line, up to the largest value appearing in the line). The results are summarised in the following table.

q	p	negative prime discriminants with case (2)
3	5	673, 1193, 1993, 1999, 2819, 4219, 4637, 5087, 5437, 5791, 5897, 7907, 8803, 9013, 9103, 9349, 9551, 9857, 10391, 10453, 10937, 11491, 13873
3	7	2749, 4513, 5717, 6581, 8059, 9613, 9733, 11971
3	11	3061
3	13	9397
5	11	709, 1489
5	19	3389, 3701
7	13	997

We also looked for a case-(2) example over a real quadratic field. We found one for $K = \mathbb{Q}(\sqrt{13})$, $q = 3$, $p = 5$. Let $\omega = \frac{1+\sqrt{13}}{2}$ and $\alpha = 15\omega - 73$ and set $L = K(\sqrt{\alpha})$. The norm of α is the prime 3559. The class number of L equals $24 = 2^3 \cdot 3$ and we let M be the unique unramified cyclic extension of L of degree 3. The class number of M equals $200 = 2^3 \cdot 5^2$, so that the quotient of the two class numbers is 5^2 and we are indeed in case (2) by the above criterion.

6 Appendix

In this section, we give a different proof of Theorem 1.5.

Second proof of Theorem 1.5. It follows, from part (b) of Lemma 2.9, that there exists an element $g_0 \in \mathrm{Gal}(M^{\overline{\rho}}(S)/L)$ such that $\rho_S^{\mathrm{univ}}(g_0) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a \neq b$. Note that $M_2(R_S^{\mathrm{univ}})$ is a Generalized Matrix Algebra (GMA) (see [BC09, Chapter 1] for definition of GMA). Therefore, by [Bel, Lemma 2.4.5], we get that $A = R_S^{\mathrm{univ}}[\rho_S^{\mathrm{univ}}(\mathrm{Gal}(M^{\overline{\rho}}(S)/L))]$ is a sub-R_S^{univ}-GMA of $M_2(R_S^{\mathrm{univ}})$.

Recall that A being a sub-R_S^{univ}-GMA of $M_2(R_S^{\mathrm{univ}})$ means that $A = \begin{pmatrix} R_S^{\mathrm{univ}} & B \\ C & R_S^{\mathrm{univ}} \end{pmatrix}$, where B and C are ideals of R_S^{univ} (see [Bel, Section 2.2]). As R_S^{univ} is Noetherian, B and C are finitely generated R_S^{univ}-modules. Moreover, since the image of A modulo $m_{R_S^{\mathrm{univ}}}$ is diagonal, it follows that $B \subset m_{R_S^{\mathrm{univ}}}$ and $C \subset m_{R_S^{\mathrm{univ}}}$.

Let $\phi \in \mathrm{Hom}_{R_S^{\mathrm{univ}}}(B/m_{R_S^{\mathrm{univ}}}B, \mathbb{F})$. Since $B, C \subset m_{R_S^{\mathrm{univ}}}$, ϕ induces a homomorphism $\phi^* : A \to M_2(\mathbb{F})$ which sends $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} a \pmod{m_S} & \phi(b) \\ 0 & d \pmod{m_S} \end{pmatrix}$. Note that $\phi^* \circ \rho_S^{\mathrm{univ}} : \mathrm{Gal}(M^{\overline{\rho}}(S)/L) \to M_2(\mathbb{F})$ gives us an element of $\mathrm{Ext}^1_{\mathrm{Gal}(M^{\overline{\rho}}(S)/L)}(\overline{\chi}^{\sigma}, \overline{\chi})$. By [BC09, Theorem 1.5.5] and its proof, the map $\mathrm{Hom}_{R_S^{\mathrm{univ}}}(B/m_{R_S^{\mathrm{univ}}}B, \mathbb{F}) \to \mathrm{Ext}^1_{\mathrm{Gal}(M^{\overline{\rho}}(S)/L)}(\overline{\chi}^{\sigma}, \overline{\chi})$ sending ϕ to $\phi^* \circ \rho_S^{\mathrm{univ}}$ is injective.

Suppose ζ is a non-trivial element of $\mathrm{Ext}^1_{\mathrm{Gal}(M^{\overline{\rho}}(S)/L)}(\overline{\chi}^{\sigma}, \overline{\chi})$ and let ρ_ζ be the corresponding representation of $\mathrm{Gal}(M^{\overline{\rho}}(S)/L)$. So, we get that the extension M_ζ of M^{ad} fixed by $\ker(ad(\rho_\zeta))$ (i.e. the subgroup of $\mathrm{Gal}(M^{\overline{\rho}}(S)/L)$ getting mapped to scalars under ρ_ζ) is an abelian, p-torsion

Galois extension of M^{ad} which is unramified outside primes lying above $S \cup S_\infty$. Moreover, as M_ζ is Galois over L, we get an action of $\overline{H}^{\mathrm{ad}}$ on $\mathrm{Gal}(M_\zeta/M^{\mathrm{ad}})$ by conjugation. By explicitly calculating this action (by choosing lifts of $\overline{H}^{\mathrm{ad}}$ in the projective image of ρ_ζ), it follows that, as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module, $\mathrm{Gal}(M_\zeta/M^{\mathrm{ad}})$ is a direct sum of some copies of $C(\overline{\chi}/\overline{\chi}^\sigma)$.

Note that $\mathrm{Gal}(M_\zeta/M^{\mathrm{ad}})$ is a quotient of $\mathcal{G}$ as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module. However, if the conditions given in Theorem 1.5 hold, then Proposition 3.4 implies that $C(\overline{\chi}/\overline{\chi}^\sigma)$ does not occur as a quotient of $\mathcal{G}$ as $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-module. So, we get contradiction. Therefore, it follows that if the conditions given in Theorem 1.5 hold, then $\mathrm{Ext}^1_{\mathrm{Gal}(M^{\overline{\rho}}(S)/L)}(\overline{\chi}^\sigma, \overline{\chi}) = 0$. Hence, it implies that $B = 0$. By the same logic, we can conclude $C = 0$.

Thus, we get that A is abelian and hence, $\rho_S^{\mathrm{univ}}(\mathrm{Gal}(M^{\overline{\rho}}(S)/L))$ is abelian. Recall that, there exists an element $g_0 \in \mathrm{Gal}(M^{\overline{\rho}}(S)/L)$ such that $\rho_S^{\mathrm{univ}}(g) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a \neq b$. Due to the fact that $\rho_S^{\mathrm{univ}}(\mathrm{Gal}(M^{\overline{\rho}}(S)/L))$ is abelian, it follows that $\rho_S^{\mathrm{univ}}(\mathrm{Gal}(M^{\overline{\rho}}(S)/L)) = \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$ for some characters χ_1, χ_2 taking values in $(R_S^{\mathrm{univ}})^\times$ and deforming $\overline{\chi}$ and $\overline{\chi}^\sigma$. Therefore, it follows, from the proof of Theorem 1.1, that ρ_S^{univ} is dihedral. □

References

[AC14] Patrick B. Allen and Frank Calegari. Finiteness of unramified deformation rings. *Algebra Number Theory*, 8(9):2263–2272, 2014.

[Asc93] Michael Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993. Corrected reprint of the 1986 original.

[BC09] Joël Bellaïche and Gaëtan Chenevier. Families of Galois representations and Selmer groups. *Astérisque*, (324):xii+314, 2009.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bel] Joël Bellaïche. Image of pseudorepresentations and coefficients of modular forms modulo p. *Preprint*.

[BGV13] Baskar Balasubramanyam, Eknath Ghate, and Vinayak Vatsal. On local Galois representations associated to ordinary Hilbert modular forms. *Manuscripta Math.*, 142(3-4):513–524, 2013.

[BM89] N. Boston and B. Mazur. Explicit universal deformations of Galois representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 1–21. Academic Press, Boston, MA, 1989.

[Bos91] Nigel Boston. Explicit deformation of Galois representations. *Invent. Math.*, 103(1):181–196, 1991.

[Bos99] Nigel Boston. Some cases of the Fontaine-Mazur conjecture. II. *J. Number Theory*, 75(2):161–169, 1999.

[Calar] Frank Calegari. Non-minimal modularity lifting in weight one. *J. Reine Angew. Math.*, To appear.

[Car94] Henri Carayol. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemp. Math.*, pages 213–237. Amer. Math. Soc., Providence, RI, 1994.

[CG18] Frank Calegari and David Geraghty. Modularity lifting beyond the Taylor-Wiles method. *Invent. Math.*, 211(1):297–433, 2018.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[Gel97] Stephen Gelbart. Three lectures on the modularity of $\overline{\rho}_{E,3}$ and the Langlands reciprocity conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 155–207. Springer, New York, 1997.

[Hid79] Haruzo Hida. On abelian varieties with complex multiplication as factors of the abelian variety attached to Hilbert modular forms. *Japan. J. Math. (N.S.)*, 5(1):157–208, 1979.

[Jar97] Frazer Jarvis. On Galois representations associated to Hilbert modular forms. *J. Reine Angew. Math.*, 491:199–216, 1997.

[LMF13] The LMFDB Collaboration. The l-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 16 September 2013].

[Maz89] B. Mazur. Deforming Galois representations. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 385–437. Springer, New York, 1989.

[Maz97] B. Mazur. An introduction to the deformation theory of galois representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 243–311. Springer, New York, 1997.

[New15] James Newton. Towards local-global compatibility for Hilbert modular forms of low weight. *Algebra Number Theory*, 9(4):957–980, 2015.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Oza17] Tomomi Ozawa. Classical weight one forms in Hida families: Hilbert modular case. *Manuscripta Math.*, 153(3-4):501–521, 2017.

[Rog97] Jonathan D. Rogawski. Functoriality and the Artin conjecture. In *Representation theory and automorphic forms (Edinburgh, 1996)*, volume 61 of *Proc. Sympos. Pure Math.*, pages 331–353. Amer. Math. Soc., Providence, RI, 1997.

[RT83] J. D. Rogawski and J. B. Tunnell. On Artin L-functions associated to Hilbert modular forms of weight one. *Invent. Math.*, 74(1):1–42, 1983.

[RT11] A. Raghuram and Naomi Tanabe. Notes on the arithmetic of Hilbert modular forms. *J. Ramanujan Math. Soc.*, 26(3):261–319, 2011.

[SW93] Thomas R. Shemanske and Lynne H. Walling. Twists of Hilbert modular forms. *Trans. Amer. Math. Soc.*, 338(1):375–403, 1993.

Shaunak V. Deo, Gabor Wiese
University of Luxembourg
Mathematics Research Unit
Maison du nombre
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Grand-Duchy of Luxembourg
deoshaunak@gmail.com, gabor.wiese@uni.lu