Dihedral Universal Deformations

Shaunak V. Deo   Gabor Wiese

8th April 2020

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 side-results, we obtain cases of the unramified Fontaine–Mazur conjecture, and in many cases positively answer a question of Greenberg and Coleman on the splitting behaviour at p of p-adic Galois representations attached to newforms. 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 prove useful alternate characterisations to the dihedral property of a deformation ρ of $\overline{\rho}$ as above. 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 apply our results on the one hand to Boston's strengthening of the unramified Fontaine–Mazur conjecture. On the other hand, we positively answer many cases of a question of Greenberg and Coleman on the splitting behaviour at p of the p-adic Galois representation attached to a newform.

(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 an 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). Since $\overline{\rho}$ is assumed to be absolutely irreducible, the projective image of $\overline{\rho}$ is a dihedral group. If the projective image of $\overline{\rho}$ is a non-abelian dihedral group, then there is a unique index 2 subgroup $H \lhd G$ such that $\overline{\rho} \simeq \mathrm{Ind}_H^G(\overline{\chi})$. On the other hand, if the projective image is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then there are three such index 2 subgroups of G.

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:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \Gamma_\rho & \longrightarrow & \mathrm{im}(\rho) & \longrightarrow & \overline{\rho}(G) & \longrightarrow & 0 \\
 & & \| & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \Gamma_\rho & \longrightarrow & \mathrm{im}(\rho|_H) & \longrightarrow & \overline{\rho}(H) & \longrightarrow & 0 \\
 & & & & & \overset{s}{\longleftarrow} & & &
\end{array}
\tag{1.1}
$$

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, *i.e.* the largest continuous quotient of Γ_ρ that is an elementary abelian p-group (see §2.3).

Theorem 1.1. *The following statements are equivalent:*

(i) *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 $pR = 0$.*

It would also be justified to speak of *first-order deformations*; however, we stick to the above terminology.

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

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

where R^{univ} is the universal deformation ring of $\overline{\rho}$. The existence of both R^{univ} and ρ^{univ} follows from [Maz89, Proposition 1]. Moreover, it also implies that R^{univ} is a complete Noetherian local $W(\mathbb{F})$-algebra with residue field $\mathbb{F}$. 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). We also include an alternative proof of Theorem 1.4 using Generalised Matrix Algebras, which also works with coefficients in a finite extension of $\mathbb{Q}_p$ (see Theorem 2.19).

3

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. Denote the *constant determinant* counterpart of ρ_S^{univ} by $(\rho_S^{\mathrm{univ}})^0$. So $\det((\rho_S^{\mathrm{univ}})^0)$ 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 the 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 3.12 (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 3.13 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 $\overline{\chi}$.

1.3 Application to the Boston–Fontaine–Mazur Conjecture

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 [LMF, 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 is dihedral and 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 is dihedral and 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.

1.4 Application to a question of Greenberg and Coleman

A famous question due to R. Greenberg asks when the p-adic Galois representation attached to a p-ordinary cuspidal eigenform f of weight $k \geq 2$ is a sum of two characters when restricted to a decomposition group at p (see [GV04, Question 1]). An equivalent form of this question due to Coleman can also be found in [Col96] (see [CWE, Section 1] for more details). There has been a lot

of work on this question in the past; see [CWE, Section 1] for a brief summary of the work centred around this question. An answer to this question was found under certain hypotheses in [CWE] ([CWE, Theorem 1.3.1, Corollary 1.3.2]). We prove a similar theorem:

Theorem 1.8. *Assume Set-up 3.16 and suppose* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^{\sigma})) = 0$ *(cf. Theorem 1.5). Let f be a classical newform of tame level $\Gamma_1(M)$ such that*

1. $\overline{\rho}_f \simeq \overline{\rho}$,

2. $\rho_f|_{G_{\mathbb{Q}_p}}$ *is a sum of two characters,*

3. *if $\ell|M$ and $\overline{\rho}|_{G_{\mathbb{Q}_\ell}} = \eta \oplus \psi$, then $\eta\psi^{-1} \neq \omega_p^{(\ell)}, (\omega_p^{(\ell)})^{-1}$, where $\omega_p^{(\ell)}$ is the mod p cyclotomic character of $G_{\mathbb{Q}_\ell}$,*

4. *if $\ell|M$, $p|\ell - 1$ and $\overline{\rho}|_{G_{\mathbb{Q}_\ell}}$ is reducible, then one of the following holds:*

    (a) *ℓ is split in L,*

    (b) *ℓ is not split in L, $\det(\rho_f|_{I_\ell}) = \widehat{\det(\overline{\rho}|_{I_\ell})}$ and $\ell \nmid M/N$.*

Then f has CM by L.

Note that Theorem 1.8 implies [CWE, Corollary 1.3.2] (see Remark 3.19 for more details). To prove Theorem 1.8, we identify a quotient $G_S^{p-\mathrm{ab}}$ of $G_{\mathbb{Q}}$ such that if f is an eigenform satisfying the conditions of Theorem 1.8, then ρ_f factors through $G_S^{p-\mathrm{ab}}$. Under the hypotheses of Theorem 1.8, we prove that the universal deformation of $\overline{\rho}$ for the group $G_S^{p-\mathrm{ab}}$ is dihedral by verifying the criteria proved in Theorem 1.4. The theorem follows directly from this.

1.5 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 characters.

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).

We shall restrict to *minimal deformations* (see Definition 4.6), defined in the same way as in [CG18, Definition 3.1]. We find that there is an explicit choice for the set of places S such that $(\rho_S^{\mathrm{univ}})^0$ is dihedral and $R^{\mathrm{min}} = (R_S^{\mathrm{univ}})^0$ (see Proposition 4.8), where R^{min} is the universal minimal deformation ring of $\overline{\rho}$ and $(R_S^{\mathrm{univ}})^0$ is the ring underlying $(\rho_S^{\mathrm{univ}})^0$.

Using that $(\rho_S^{\mathrm{univ}})^0$ is dihedral, from Proposition 4.2 we obtain a quotient $\mathbb{T}_{\mathrm{dih}}$ of the anemic $W(\mathbb{F})$-Hecke algebra acting on parallel weight one Hilbert modular forms over K, which comes equipped with a Galois representation $\rho_{\mathrm{dih}} : G_K \to \mathrm{GL}_2(\mathbb{T}_{\mathrm{dih}})$ and a ring homomorphism $\psi : \mathbb{T}_{\mathrm{dih}} \to (R_S^{\mathrm{univ}})^0$ such that $\psi \circ \rho_{\mathrm{dih}} = (\rho_S^{\mathrm{univ}})^0$. The determinant of ρ_{dih} is the Teichmüller lift of $\det \circ \overline{\rho}$. It turns out that ρ_{dih} is a minimal deformation of $\overline{\rho}$ and this leads to our main modularity result.

Theorem 1.9. *The map $R^{\mathrm{min}} \to \mathbb{T}_{\mathrm{dih}}$ induced from the minimal deformation property of ρ_{dih} is an isomorphism.*

1.6 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-ups'.

Set-up 1.10. *In the entire article, p will denote a fixed prime number and $\mathbb{F}$ a finite field of characteristic p.*

1.7 Acknowledgements

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 for the sake of completeness, we include a proof, which is quite simple and explicit.

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

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

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 $\psi : H \twoheadrightarrow P \xrightarrow{\pi} \mathrm{im}(\psi) \subseteq R^\times$.

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

8

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 $(\mathcal{U}_{W(\mathbb{F}),r,(e_1,e_2,\ldots,e_n)}, \chi^{\mathrm{univ}})$. $\qquad\square$

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 R-submodule 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;*

9

- $I(\chi)_{R'} = \mathrm{Ind}_H^G(\chi)_{R'}$, 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 $\rho \cong \mathrm{Ind}_H^G(\chi)_R$ 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*

$$\mathrm{ad}(\rho)_R \to N_R \oplus I(\chi/\chi^\sigma)_R, \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a \\ d \end{smallmatrix}\right) \oplus \left(\begin{smallmatrix} b \\ c/\chi(\sigma^2) \end{smallmatrix}\right)$$

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

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

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

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

is split if 2 is invertible in R with split $r \mapsto \left(\begin{smallmatrix} r/2 & 0 \\ 0 & r/2 \end{smallmatrix}\right)$.

Proof. These are elementary calculations. $\qquad\square$

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 $\mathrm{Ind}_H^G(\overline{\chi})_{\mathbb{F}}$. By the assumption $\overline{\chi} \neq \overline{\chi}^\sigma$, the representation $\overline{\rho}$ is absolutely irreducible. We also use the following pieces of notation:*

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

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 $\mathrm{Ind}_H^G(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}$. 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 $\mathrm{ad}(\overline{\rho})_{\mathbb{F}}$ 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 whose composition factors 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 $V \cong C(1)^{r_1} \oplus I(\overline{\chi}/\overline{\chi}^{\sigma})^r$ 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. $\square$

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. $\square$

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 $\overline{H}^{\mathrm{ad}}$.

11

(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 $\overline{G}^{\mathrm{ad}}$. $\qquad\square$

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 Γ 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. $\qquad\square$

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 splitting, $s(\overline{H})$ 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. $\rho(h) = \begin{pmatrix} \psi_1(h)\widehat{\chi}(h) & 0 \\ 0 & \psi_2(h)\widehat{\chi}^\sigma(h) \end{pmatrix}$ 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). $\qquad\square$

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 $\mathrm{im}(\rho \mod \mathfrak{m}_R^k)$ and that this action is independent of the choice of preimage because conjugation by $1 + M_2(\mathfrak{m}_R/\mathfrak{m}_R^k)$ 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. $\qquad\square$

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 a $\mathbb{F}_p[\overline{H}^{\mathrm{ad}}]$-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. $\qquad\square$

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 $\Gamma_\rho \subseteq \mathrm{ad}(\overline{\rho})_{\mathbb{F}}^r$.*

Proof. The kernel Γ_ρ of reduction modulo $\mathfrak{m}_R$ clearly sits in $1 + M_2(\mathfrak{m}_R)$, proving the result. $\qquad\square$

We now prove a converse of Corollary 2.12. In the case $p = 2$, the upper 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*

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

such that the induced action of $\overline{G}$ on Z factors through $\overline{G}^{\mathrm{ad}}$ making it a $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-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 $p \nmid |\overline{H}|$, 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 $p \nmid |\overline{G}/\overline{H}| = 2$. 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,

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

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 $\mathbb{F}_2$.

When the sequence splits, we can proceed as follows. We have the exact sequence of groups

$$0 \longrightarrow M_2(\mathbb{F}) \longrightarrow \mathrm{GL}_2(\mathbb{F}[X]/(X^2)) \underset{s}{\longrightarrow} \mathrm{GL}_2(\mathbb{F}) \longrightarrow 0$$

$$\begin{array}{ccc} & Z & & \overline{G} \end{array}$$

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 $s(\overline{G})$.

If the sequence is non-split, then the analysis above implies that $p = 2$ and $Z = \mathbb{F}_2$. In order to treat this case, 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 a non-split extension of $\overline{G}$ by $\mathbb{F}_2$. Recall that our calculation shows that there are only 2 isomorphism classes of extensions of $\overline{G}$ by $\mathbb{F}_2$. Since both $\mathcal{G}$ and $\mathcal{G}'$ are non-trivial extensions of $\overline{G}$ by $\mathbb{F}_2$, it follows that $\mathcal{G}' \cong \mathcal{G}$. $\qquad\square$

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

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

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 $T = \mathbb{F}[X_1, \ldots, X_r]/(X_i X_j \mid i, j)$ 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. $\qquad \square$

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. $\qquad \square$

Lemma 2.17. *Suppose any deformation of $\overline{\rho}$ to $\mathbb{F}[X]/(X^2)$ is dihedral. Then there exists a subgroup $H \lhd G$ of index 2 such that if $\rho : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ is a deformation of $\overline{\rho}$, then $\rho \simeq \mathrm{Ind}_H^G(\chi)$ for some character $\chi : H \to (\mathbb{F}[X]/(X^2))^\times$.*

Proof. Suppose the projective image of $\overline{\rho}$ is a non-abelian dihedral group. Then there is a unique index 2 subgroup $H \lhd G$ such that $\overline{\rho} \simeq \mathrm{Ind}_H^G(\overline{\chi})$ for some character $\overline{\chi} : H \to \mathbb{F}^\times$. Therefore, the lemma follows directly in this case.

Now suppose the projective image of $\overline{\rho}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then there are exactly 3 index 2 subgroups H_1, H_2 and H_3 of G and characters $\overline{\chi}_i : H_i \to \mathbb{F}^\times$ such that $\overline{\rho} \simeq \mathrm{Ind}_{H_i}^G(\overline{\chi}_i)$ for every $1 \leq i \leq 3$. Note that in this case p is odd. Suppose $\rho : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ is a deformation of $\overline{\rho}$. Then we can twist ρ by a suitable character to get a deformation of $\overline{\rho}$ with constant determinant. Hence, it suffices to prove the lemma for deformations of $\overline{\rho}$ with constant determinant. Moreover, by part (b) of Lemma 2.7, we get that as an $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-module, $\mathrm{ad}^0(\overline{\rho})_\mathbb{F} \simeq \oplus_{i=1}^3 C(\epsilon_i)_\mathbb{F}$, where $\epsilon_i : G \twoheadrightarrow G/H_i \twoheadrightarrow \{\pm 1\} \subset \mathbb{F}^\times$ for $1 \leq i \leq 3$.

It follows from Theorem 1.1 that any non-trivial deformation $\rho : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ of $\overline{\rho}$ with constant determinant can only be induced from a single subgroup of G of index 2. Suppose not all such deformations are induced from the same subgroup. Then, without loss of generality for $i = 1, 2$, there are deformations $\rho_i : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ of $\overline{\rho}$ with constant determinant such that $\rho_i \simeq \mathrm{Ind}_{H_i}^G(\chi_i)$ for some character $\chi_i : H_i \to (\mathbb{F}[X]/(X^2))^\times$. Then for $i = 1, 2$, ρ_i corresponds to a non-zero element $x_i \in H^1(G, C(\epsilon_i)_\mathbb{F}) \subset H^1(G, \mathrm{ad}^0(\overline{\rho})_\mathbb{F})$. Let $\rho' : G \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ be the deformation of $\overline{\rho}$ corresponding to the element $x_1 + x_2$ of $H^1(G, \mathrm{ad}^0(\overline{\rho})_\mathbb{F})$. Note that $x_1 + x_2 \in H^1(G, C(\epsilon_1)_\mathbb{F} \oplus C(\epsilon_2)_\mathbb{F}) \setminus \cup_{i=1}^2 H^1(G, C(\epsilon_i)_\mathbb{F})$. Hence, the action of $\overline{H}_i^{\mathrm{ad}}$ on $\Gamma_{\rho'}$ is not trivial for every $1 \leq i \leq 3$. Therefore, Theorem 1.1 implies that ρ' is not dihedral. This finishes the proof of the lemma. $\qquad \square$

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 Lemma 2.17, there exists an index 2 subgroup $H \lhd G$ such that the representation given by each indecomposable submodule Z of Γ_ρ is induced from a character of H. By Theorem 1.1 this means that any such 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 $R^{\mathrm{univ}}_{\overline{\chi}}$ be the universal deformation ring of $\overline{\chi}$ as discussed in Proposition 2.1. Now we are assuming that $\rho^{\mathrm{univ}} = \mathrm{Ind}_H^G(\chi)_{R^{\mathrm{univ}}}$ for some character χ. Since ρ^{univ} 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 $\alpha : R^{\mathrm{univ}}_{\overline{\chi}} \to R^{\mathrm{univ}}$. On the other hand, given the deformation χ^{univ} of $\overline{\chi}$, we obtain a deformation $\mathrm{Ind}_H^G(\chi^{\mathrm{univ}})_{R^{\mathrm{univ}}_{\overline{\chi}}}$ of $\overline{\rho}$ and thus a morphism $\beta : R^{\mathrm{univ}} \to R^{\mathrm{univ}}_{\overline{\chi}}$. 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 $R^{\mathrm{univ}} \cong R^{\mathrm{univ}}_{\overline{\chi}}$, as claimed. $\qquad\square$

Remark 2.18. *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).

Appendix: An alternative proof

In this appendix, we prove a generalisation of Theorem 1.4 using a different argument.

To be precise, let G be a profinite group satisfying the finiteness condition Φ_p of Mazur (see [Maz89, Section 1.1]). Let p be a prime, E be a finite extension of $\mathbb{Q}_p$. Let $\overline{\rho} : G \to GL_2(E)$ be an absolutely irreducible dihedral representation. So there exists an open normal subgroup H of G of index 2 and a character $\overline{\chi} : H \to E^\times$ such that $\rho \simeq \mathrm{Ind}_H^G(\overline{\chi})$. Note that $\overline{\rho}|_H = \overline{\chi} \oplus \overline{\chi}^\sigma$.

Let $\mathcal{D}$ be the category of local Artinian algebras with residue field E. Then, it follows, from [Kis03, Lemma 9.3], that the functor from $\mathcal{D}$ to the category of sets sending an object R of $\mathcal{D}$ to the set of deformations of $\overline{\rho}$ to $GL_2(R)$ is pro-representable by a local complete Noetherian ring with residue field E. Let R^{univ} be the universal deformation ring of $\overline{\rho}$, $\mathfrak{m}^{\mathrm{univ}}$ be the maximal ideal of R^{univ} and $\rho^{\mathrm{univ}} : G \to GL_2(R^{\mathrm{univ}})$ be the universal deformation of $\overline{\rho}$.

Theorem 2.19. *Suppose p is a prime, E is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p$ and G is a profinite group satisfying Mazur's finiteness condition Φ_p. Let $\overline{\rho} : G \to GL_2(E)$ be an absolutely irreducible dihedral representation. Then ρ^{univ} is dihedral if and only if any infinitesimal deformation $\tilde{\rho} : G \to \mathrm{GL}_2(E[\epsilon]/(\epsilon^2))$ of $\overline{\rho}$ is dihedral.*

Proof. The forward direction is trivial. So, we only need to prove the backward direction. Let $H \lhd G$ be an index 2 subgroup such that $\overline{\rho} \simeq \operatorname{Ind}_H^G \overline{\chi}$ for some character $\overline{\chi} : H \to E^\times$. Now the proof of Lemma 2.17 implies that to prove the theorem, it suffices to prove that if ρ^{univ} is not dihedral, then for every such H, there exists an infinitesimal deformation of $\overline{\rho}$ which is not induced from a character of H. Note that a non-zero element of $H^1(G, \operatorname{Ind}_H^G(\overline{\chi}/\overline{\chi}^\sigma))$ gives us an infinitesimal deformation of $\overline{\rho}$ which is not induced from a character of H. Thus it suffices to prove that if ρ^{univ} is not dihedral, then $H^1(G, \operatorname{Ind}_H^G(\overline{\chi}/\overline{\chi}^\sigma)) \neq 0$. By Shapiro's lemma, we have $H^1(G, \operatorname{Ind}_H^G(\overline{\chi}/\overline{\chi}^\sigma)) \simeq H^1(H, \overline{\chi}/\overline{\chi}^\sigma)$. So, it suffices to prove $H^1(H, \overline{\chi}/\overline{\chi}^\sigma) \neq 0$.

We will now assume ρ^{univ} is not dihedral and construct a non-zero element of $H^1(H, \overline{\chi}/\overline{\chi}^\sigma)$. It follows, from part (b) of Lemma 2.9, that there exists an element $g_0 \in H$ such that $\rho^{\mathrm{univ}}(g_0) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a \neq b$. Note that $M_2(R^{\mathrm{univ}})$ is a Generalized Matrix Algebra (GMA) (see [BC09, Chapter 1] for the definition). Therefore, by [Bel19, Lemma 2.4.5], we get that $A = R^{\mathrm{univ}}[\rho^{\mathrm{univ}}(H)]$ is a sub-R^{univ}-GMA of $M_2(R^{\mathrm{univ}})$.

Recall that A being a sub-R^{univ}-GMA of $M_2(R^{\mathrm{univ}})$ means that $A = \begin{pmatrix} R^{\mathrm{univ}} & B \\ C & R^{\mathrm{univ}} \end{pmatrix}$, where B and C are ideals of R^{univ} (see [Bel19, Section 2.2]). As R^{univ} is Noetherian, B and C are finitely generated R^{univ}-modules. Moreover, since the image of A modulo $\mathfrak{m}^{\mathrm{univ}}$ is diagonal, it follows that $B \subset \mathfrak{m}^{\mathrm{univ}}$ and $C \subset \mathfrak{m}^{\mathrm{univ}}$.

As we have assumed that ρ^{univ} is not dihedral and H is normal in G, it follows that both $B \neq 0$ and $C \neq 0$. Indeed, non-dihedralness implies that at least one of them is not 0 and if the other one is 0, then normality of H in G implies that ρ^{univ} is reducible, which is not possible.

Now suppose for $h \in H$, $\rho^{\mathrm{univ}}(h) = \begin{pmatrix} a(h) & b(h) \\ c(h) & d(h) \end{pmatrix}$. So $b(h) \in B$ and $c(h) \in C$. Let $\phi : B \to E$ be a non-trivial map of R^{univ}-modules. This defines a representation $\rho_\phi : H \to \mathrm{GL}_2(E)$ such that $\rho_\phi(h) = \begin{pmatrix} \overline{\chi}(h) & \phi(b(h)) \\ 0 & \overline{\chi}^\sigma(h) \end{pmatrix}$. So, this defines an element of $H^1(H, \overline{\chi}/\overline{\chi}^\sigma)$. Since the R^{univ}-span of $\rho^{\mathrm{univ}}(H)$ is $\begin{pmatrix} R^{\mathrm{univ}} & B \\ C & R^{\mathrm{univ}} \end{pmatrix}$, it follows that E-span of $\rho_\phi(H)$ contains all the diagonal matrices and $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. As $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ does not commute with all diagonal matrices, it follows that $\rho_\phi(H)$ is not abelian and hence, it defines a non-zero element of $H^1(H, \overline{\chi}/\overline{\chi}^\sigma)$. This finishes the proof of the theorem. $\qquad\square$

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 $\mathfrak{p}$ and by $G_{N_{\mathfrak{p}}}$ the decomposition group of $\mathfrak{p}$ inside G_N. 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).
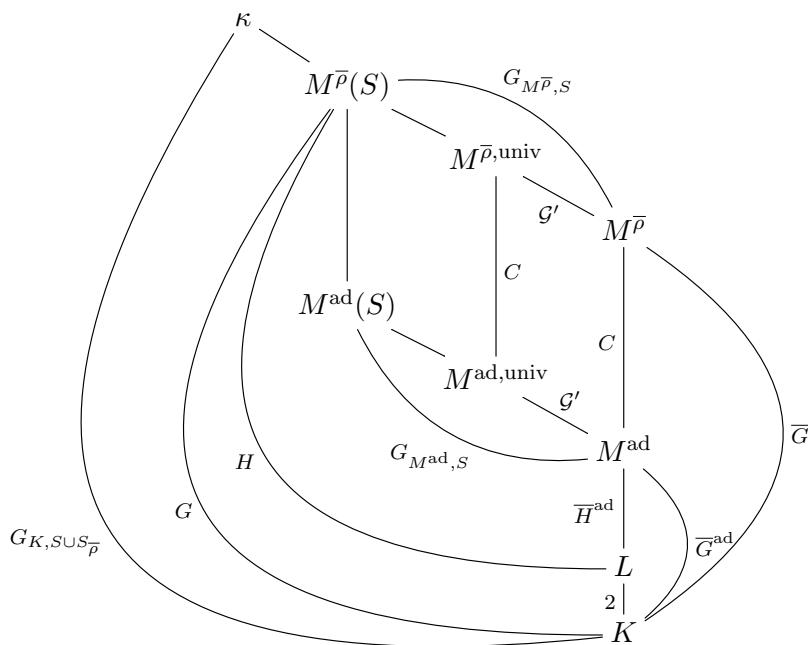
Note that the extensions $M^{\overline{p}}(S)$ and $M^{\mathrm{ad}}(S)$ of K are Galois. Put $G = \mathrm{Gal}(M^{\overline{p}}(S)/K)$ and $H = \mathrm{Gal}(M^{\overline{p}}(S)/L)$. Note that these pieces of notation exactly correspond to those of section 2.

Let $G_{M^{\mathrm{ad}},S} = \mathrm{Gal}(M^{\mathrm{ad}}(S)/M^{\mathrm{ad}})$ and $G_{M^{\mathrm{ad}},S}^{\mathrm{ab}}$ 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 $G_{M^{\mathrm{ad}},S}^{\mathrm{ab}}$ and hence, on the $\mathbb{F}_p$-vector space $\mathcal{G} := G_{M^{\mathrm{ad}},S}^{\mathrm{ab}}/(G_{M^{\mathrm{ad}},S}^{\mathrm{ab}})^p$ by conjugation.

Let S'' be the subset of S consisting of the finite primes q such that $\mu_p \subseteq M_{q'}^{\mathrm{ad}}$ 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 $\mathcal{M} = \ker\left(\mathcal{G} \twoheadrightarrow A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}})\right)$ 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 $M_{q'}^{\mathrm{ad}}$ 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 $M_{q'}^{\mathrm{ad}}$ 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 $\mu_p \subseteq M_{q'}^{\mathrm{ad}}$. 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). $\qquad\square$

For further analysis, we first define the following sets of finite 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 and $\overline{\chi}/\overline{\chi}^\sigma|_{D_\ell}$ is either $\chi_p^{(\ell)}$ or $(\chi_p^{(\ell)})^{-1}$. Note that this implies that ℓ is unramified in M^{ad} and for any prime λ of M^{ad} lying above ℓ, $M_\lambda^{\mathrm{ad}} = K_\ell(\mu_p)$.

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, $\mu_p \subseteq M_\lambda^{\mathrm{ad}}$ and $[M_\lambda^{\mathrm{ad}} : K_\ell] = 2$ (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, $\mathrm{Gal}(M_\lambda^{\mathrm{ad}}/K_\ell) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mu_p \subseteq M_\lambda^{\mathrm{ad}}$ (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 $\mu_p \subseteq M_{\lambda_0}^{\mathrm{ad}}$ for some prime λ_0 of M^{ad} lying above ℓ, then $\mu_p \subseteq M_\lambda^{\mathrm{ad}}$ 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

$$\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\mathcal{G}, I(\overline{\chi}/\overline{\chi}^\sigma)) \hookrightarrow \mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(\prod_{q \in S''} \mathrm{Ind}_{D_q}^{\overline{G}^{\mathrm{ad}}}(C(\chi_p^{(q)})_{\mathbb{F}_p}), I(\overline{\chi}/\overline{\chi}^\sigma))$$

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

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 $\mathrm{ad}(\rho)_{\mathbb{F}} \cong N_{\mathbb{F}} \oplus I(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}$ (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 $I(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}|_{D_q} = C(\overline{\chi}/\overline{\chi}^\sigma|_{D_q})_{\mathbb{F}} \oplus C(\overline{\chi}^\sigma/\overline{\chi}|_{D_q})_{\mathbb{F}}$. 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 $\overline{\chi}^\sigma/\overline{\chi}|_{D_q} = \chi_p^{(q)}$. 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, $I(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}|_{D_q}$ is $\mathbb{F}^2$ with D_q-action swapping the two standard basis vectors. So, if $p > 2$, then $I(\overline{\chi}/\overline{\chi}^\sigma)_{\mathbb{F}}|_{D_q} \cong C(1)_{\mathbb{F}} \oplus C(\epsilon)_{\mathbb{F}}$ 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. $\qquad\square$

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 either K is not totally real or $\overline{\rho}$ is not totally even (equivalently, if M^{ad} is not totally real), then either the existence of complex embeddings of K or 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 one 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 either K is not totally real or $\overline{\rho}$ is not totally even. From this logic, we also see that, if either K is not totally real or $\overline{\rho}$ 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]). $\qquad\square$

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. *Deformations of $\overline{\rho}$ belonging to $D_S(R)$ ($D_S^0(R)$) are said to be* relatively unramified outside S *(with constant determinant).*

Note that if $\rho \in D_S(R)$ and ℓ is a prime of K not contained in S, then $\rho|_{G_{K_\ell}}$ is often called a minimal deformation of $\overline{\rho}|_{G_{K_\ell}}$ in the literature (see [Maz97, Section 29]). Thus an element of $D_S(R)$ is a deformation of ρ which is minimally ramified at all primes not contained in S.

Remark 3.11. *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 representing D_S. 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. $\qquad\square$

Remark 3.12. *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 $G_{M^{\overline{\rho}}(S),L}^{\mathrm{ab},(p)}$ 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 $G_{M^{\overline{\rho}}(S),L}^{\mathrm{ab},(p)}$ 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 3.13. *Let S be a finite set of primes of K. Suppose the conditions given in Theorem 1.5 hold. Then $R_S^{\mathrm{univ}} \simeq W(\mathbb{F})[X_1, \cdots, X_{n'}]/((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_{n'})^{p^{e_{n'}}} - 1)$.*

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

Now suppose p is odd. In this case, we add an explicit description of $(R_S^{\mathrm{univ}})^0$. 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 $\mathrm{im}(\widehat{\det \overline{\rho}})$ 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, $(R_S^{\mathrm{univ}})^0 \simeq R_S^{\mathrm{univ}}/(X_{n+1}, \cdots, X_{n'}) \simeq W(\mathbb{F})[X_1, \cdots, X_n]/((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_n)^{p^{e_n}} - 1)$. $\square$

3.1 Application to the Boston–Fontaine–Mazur Conjecture

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 $\rho_S^{\mathrm{univ}} = \mathrm{Ind}_{G_{M^{\overline{\rho}}(S)/L}}^{G_{M^{\overline{\rho}}(S)/K}} (\chi^{\mathrm{univ}})$ where $\chi^{\mathrm{univ}} : \mathrm{Gal}(M^{\overline{\rho}}(S)/L) \to (R_S^{\mathrm{univ}})^\times$ is the universal deformation of $\overline{\chi}$. It follows, from the description of χ^{univ} in Proposition 2.1

and the discussion before Corollary 3.13, that χ^{univ} has finite image. Therefore, from the discussion before Definition 2.4, we see that ρ_S^{univ} has finite image. $\square$

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 [LMF, Number field 20.0.3590802812540187339238342949.1]).

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 $S \cap S_0 = \emptyset$. $\square$

Remark 3.15. *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], Corollary 1.7(b) clearly does not satisfy those 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 Corollary 1.7(a) does not satisfy the hypotheses of [AC14, Corollary 3] either.*

3.2 Application to a question of Greenberg and Coleman

The main purpose of this section is to prove a result similar to [CWE, Corollary 1.3.2] using the main results of this article.

Set-up 3.16. *Let $p > 2$ be a prime and $\mathbb{F}$ be a finite field of characteristic p. We keep Notation 3.1 and Set-up 3.2 throughout this section with $K = \mathbb{Q}$. Let $\overline{\rho} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F})$ be an absolutely irreducible, odd dihedral representation. So, $\overline{\rho} = \mathrm{Ind}_{G_L}^{G_\mathbb{Q}}(\overline{\chi})$ for some quadratic extension L of $\mathbb{Q}$ and character $\overline{\chi} : G_L \to \mathbb{F}^\times$. Let N be the tame Artin conductor of $\overline{\rho}$. Moreover, assume that*

1. *L is a quadratic imaginary number field,*

2. *p is split in L,*

3. $\overline{\rho}|_{G_{\mathbb{Q}_p}}$ *is a sum of two* distinct *characters,*

4. *If $\ell \neq p$ is a prime such that $\overline{\rho}$ is ramified at ℓ and $\overline{\rho}|_{G_{\mathbb{Q}_\ell}} = \eta \oplus \psi$, then $\eta\psi^{-1} \neq \omega_p^{(\ell)}, (\omega_p^{(\ell)})^{-1}$, where $\omega_p^{(\ell)}$ is the mod p cyclotomic character of $G_{\mathbb{Q}_\ell}$,*

5. *If ℓ is a prime such that $p|\ell-1$, $\overline{\rho}$ is ramified at ℓ, ℓ is not split in L and $\overline{\rho}|_{G_{\mathbb{Q}_\ell}}$ is reducible, then $\overline{\rho}|_{G_{\mathbb{Q}_\ell}}$ is a sum of a ramified and an unramified character.*

6. *If ℓ is a prime such that $p|\ell+1$ and ℓ is ramified in L, then $\mathrm{ad}(\overline{\rho})(G_{\mathbb{Q}_\ell}) \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Let S_0 be the set of primes of $\mathbb{Q}$ defined just before Proposition 3.4. Let S be a finite set of primes of $\mathbb{Q}$ such that $S_{\overline{\rho}} \cup \{p\} \subset S$. Let $T := S \setminus (S \cap S_0)$. Let $G_S^{p-\mathrm{ab}}$ be the maximal continuous quotient of $\mathrm{Gal}(M^{\overline{\rho}}(T)/\mathbb{Q})$ in which the image of $G_{\mathbb{Q}_p}$ is abelian. Note that $G_S^{p-\mathrm{ab}}$ satisfies the finiteness condition Φ_p of Mazur and $\overline{\rho}$ factors through $G_S^{p-\mathrm{ab}}$ due to assumption 2 above. After considering $\overline{\rho}$ as a representation of $G_S^{p-\mathrm{ab}}$, let $R^{\mathrm{univ},S}$ be the universal deformation ring of $\overline{\rho}$ with universal deformation $\rho_S^{\mathrm{univ},p-\mathrm{ab}}$.

Proposition 3.17. *Let S be a finite set of primes of $\mathbb{Q}$ such that $S_{\overline{\rho}} \cup \{p\} \subset S$. If $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$, then $\rho_S^{\mathrm{univ},p-\mathrm{ab}}$ is dihedral.*

Proof. By Theorem 1.4, it suffices to prove that any deformation $\rho : G_S^{p-\mathrm{ab}} \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ of $\overline{\rho}$ is dihedral. Now the existence of a non-dihedral deformation $\rho : G_S^{p-\mathrm{ab}} \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ of $\overline{\rho}$ implies that $H^1(G_S^{p-\mathrm{ab}}, I(\overline{\chi}/\overline{\chi}^\sigma)) \neq 0$. So we will prove that all infinitesimal $G_S^{p-\mathrm{ab}}$-deformations of $\overline{\rho}$ are dihedral by proving that $H^1(G_S^{p-\mathrm{ab}}, I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$.

Suppose $H^1(G_S^{p-\mathrm{ab}}, I(\overline{\chi}/\overline{\chi}^\sigma)) \neq 0$ and let ϕ be a non-zero element of $H^1(G_S^{p-\mathrm{ab}}, I(\overline{\chi}/\overline{\chi}^\sigma))$. Let $\rho : G_S^{p-\mathrm{ab}} \to \mathrm{GL}_2(\mathbb{F}[X]/(X^2))$ be a deformation of $\overline{\rho}$ corresponding to ϕ and let M^ρ be the extension of $\mathbb{Q}$ fixed by $\ker(\rho)$.

Note that M^ρ is an abelian p-extension of $M^{\overline{\rho}}$ unramified outside primes of $M^{\overline{\rho}}$ lying above T and $\mathrm{Gal}(M^\rho/M^{\overline{\rho}}) \simeq I(\overline{\chi}/\overline{\chi}^\sigma)$ as $\mathbb{F}_p[\overline{G}]$-modules. As the image of $G_{\mathbb{Q}_p}$ in $\mathrm{Gal}(M^\rho/\mathbb{Q})$ is abelian, it follows, from the assumptions 2 and 3, that any prime of $M^{\overline{\rho}}$ lying above p splits completely in M^ρ. Hence, $M^\rho \subset M^{\overline{\rho}}(T \setminus \{p\})$. Denote $T \setminus \{p\}$ by T'.

From the proof of Theorem 1.5, it follows that there exists an abelian p-extension $M^{\mathrm{ad},\rho}$ of M^{ad} such that $M^\rho = M^{\overline{\rho}}M^{\mathrm{ad},\rho}$, $M^{\mathrm{ad},\rho} \subset M^{\mathrm{ad}}(T')$ and $\mathrm{Gal}(M^{\mathrm{ad},\rho}/M^{\mathrm{ad}}) \simeq I(\overline{\chi}/\overline{\chi}^\sigma)$ as $\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]$-modules. This implies that $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(G_{M^{\mathrm{ad}},T'}^{\mathrm{ab}}/(G_{M^{\mathrm{ad}},T'}^{\mathrm{ab}})^p, I(\overline{\chi}/\overline{\chi}^\sigma)) \neq 0$. However, as $p \notin T'$, $T' \cap S_0 = \emptyset$ and $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$, we get a contradiction from Proposition 3.4. Hence, it follows that $H^1(G_S^{p-\mathrm{ab}}, I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$ which implies the proposition. $\square$

Remark 3.18. *Note that $\rho_S^{\mathrm{univ},p-\mathrm{ab}}$ is the universal nearly ordinary p-locally split representation (in the sense of [GV11]) relatively unramified outside $S \setminus (S \cap S_0)$.*

If f is a classical modular eigenform of level $\Gamma_1(M)$, denote the p-adic Galois representation attached to it by ρ_f and the corresponding semi-simple residual representation by $\overline{\rho}_f$. We now prove Theorem 1.8.

Proof of Theorem 1.8. Let S' be the set of prime divisors of M. Since ρ_f is a lift of $\overline{\rho}$, by Proposition 3.17 with $S = S' \cup \{p\}$, it suffices to prove that ρ_f factors through $G_S^{p-\mathrm{ab}}$. So we need to prove that there is no ramification above $M^{\overline{\rho}}$ above primes in $S' \cap S_0$ and that the image of $G_{\mathbb{Q}_p}$ is abelian. The latter is satisfied because $\rho_f|_{G_{\mathbb{Q}_p}}$ is a sum of two characters. Hence, we only need to prove that if $\ell \in S' \cap S_0$, then $\rho_f(I_\ell) \simeq \overline{\rho}(I_\ell)$.

Suppose $\ell \in S'$ is split in L. So we have $\overline{\rho}|_{G_{\mathbb{Q}_\ell}} = \overline{\chi}|_{G_{\mathbb{Q}_\ell}} \oplus \overline{\chi}^\sigma|_{G_{\mathbb{Q}_\ell}}$. By the third hypothesis of the theorem, we get that $\overline{\chi}/\overline{\chi}^\sigma|_{G_{\mathbb{Q}_\ell}} \neq \omega_p^{(\ell)}, (\omega_p^{(\ell)})^{-1}$. Therefore, we get that $\ell \notin S_1$ and hence, $S' \cap S_1 = \emptyset$.

Note that for $\ell \in S_2$, we have $p|\ell - 1$ because the third hypothesis of the theorem excludes $L_\lambda = \mathbb{Q}_\ell(\mu_p)$. By Assumption 4 and 5, along with the fourth hypothesis of the theorem, we get

$$S' \cap S_2 = \{\ell | M \text{ such that } p|\ell - 1, \ell \text{ is ramified in } L \text{ and } |\mathrm{ad}(\overline{\rho})(D_\ell)| = 2\}.$$

Indeed the definition of S_2, along with Assumption 4, implies that if $\ell \in S' \cap S_2$, then $\ell|M, p|\ell-1, \ell$ is not split in L and $|\mathrm{ad}(\overline{\rho})(D_\ell)| = 2$. Now the assumption $\ell \nmid M/N$ and 5 implies that ℓ is ramified in L.

Let now $\ell \in S' \cap S_2$. Then $\overline{\rho}|_{G_{\mathbb{Q}_\ell}} = \eta \oplus \epsilon\eta$ where η is an unramified character and ϵ is the character corresponding to a ramified quadratic extension of $\mathbb{Q}_\ell$. The unramifiedness of η follows from Assumption 5. So, we get that $\ell|N$ but $\ell^2 \nmid N$. Hence, from the fourth hypothesis of the theorem, we get that $\ell^2 \nmid M$. Hence, $\rho_f|_{G_{\mathbb{Q}_\ell}}$ is not irreducible. As $\epsilon \neq 1$, we see, by the local Langlands correspondence, that $\rho_f|_{G_{\mathbb{Q}_\ell}}$ is a sum of two characters χ_1 and χ_2 lifting η and $\epsilon\eta$, respectively. As M is the tame Artin conductor of ρ_f, it follows that χ_1 is unramified at ℓ. As $\det(\rho_f|_{I_\ell}) = \widehat{\det(\overline{\rho}|_{I_\ell})}$, it follows that $\rho_f|_{I_\ell} \simeq \overline{\rho}|_{I_\ell}$.

Finally, suppose $S' \cap S_3 \neq \emptyset$ and let $\ell \in S' \cap S_3$. Then $p|\ell+1, \ell$ is ramified in L and $\mathrm{ad}(\overline{\rho})(G_{\mathbb{Q}_\ell}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But this contradicts the hypothesis (6). Hence, we get that $S' \cap S_3 = \emptyset$. $\qquad\square$

Remark 3.19. *Note that the conditions given in Set-up (3.16) on $\overline{\rho}$ and the conditions in Theorem 1.8 are slightly weaker than the conditions appearing in [CWE, Corollary 1.3.2]. Indeed, in [CWE, Corollary 1.3.2], they assume that the tame level of the modular form is the same as the tame Artin conductor of $\overline{\rho}$. The assumption $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) = 0$ appearing in Theorem 1.8 is the same as the assumption $X(\psi^-) = 0$ appearing in [CWE, Corollary 1.3.2]. The asumptions (1), (2) and (3) of Set-up (3.16) are present in [CWE, Corollary 1.3.2]. Observe that the assumptions (4), (5) and (6) of Set-up (3.16) are satisfied when $\overline{\chi}$ is a character of G_L such that the conductors of $\overline{\chi}$ and $\overline{\chi}^\sigma$ are coprime. Indeed, if the conductors of $\overline{\chi}$ and $\overline{\chi}^\sigma$ are co-prime, then we get that if $\ell|N$, then $\overline{\rho}|_{G_{\mathbb{Q}_\ell}} \simeq \phi \oplus \eta$, where exactly one of ϕ and η is a ramified character (see [CWE, Lemma 2.3.4]). This assumption on $\overline{\chi}$ is also present in [CWE] (see [CWE, Section 1.2.3]). Hence, Theorem 1.8 implies [CWE, Corollary 1.3.2].*

Remark 3.20. *The arguments of [CWE] rely crucially on an 'R = $\mathbb{T}$' theorem that they prove ([CWE, Theorem 5.5.1]). However, our approach relies mainly on the group theoretic arguments and on proving that universal any nearly ordinary p-locally split deformation of $\overline{\rho}$ is dihedral. However, if the universal nearly ordinary p-locally split deformation of $\overline{\rho}$ is not dihedral, we cannot say anything conclusive regarding the question of Greenberg. So our argument does not yield anything when* $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^{\sigma})) \neq 0$. *Hence, we cannot prove [CWE, Theorem 1.3.4, Theorem 1.4.4] using our methods.*

Remark 3.21. *Suppose that in Set-up 3.16, we assume that L is a real quadratic field, but that all the other assumptions hold. Then the above arguments shows that if f is an eigenform satisfying the hypotheses of Theorem 1.8, then ρ_f is dihedral and induced from a character of G_L. But as L is a real quadratic field, this would immediately imply that f has weight 1 as there is no Real Multiplication in weights greater than 1.*

This proves that if f has weight greater than 1 and satisfies the hypotheses 1, 3 and 4 of Theorem 1.8, then $\rho_f|_{G_{\mathbb{Q}_p}}$ is not a sum of two characters and f does not have complex multiplication. This answers the question of Coleman-Greenberg in some more cases.

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

In this section, we let K be a totally real field and L/K a quadratic extension, which is not necessarily totally imaginary. We furthermore fix an absolutely irreducible dihedral representation $\overline{\rho} : G_K \rightarrow \mathrm{GL}_2(\mathbb{F})$ which we assume to be totally odd. As before, let R be a complete Noetherian local ring with residue field $\mathbb{F}$ and let $\rho : G_K \rightarrow \mathrm{GL}_2(R)$ be a dihedral deformation of $\overline{\rho}$ of the form $\mathrm{Ind}_{G_L}^{G_K}(\chi)$. We assume ρ to be unramified at the primes above p and of finite image. We write $H = G_L$ and $G = G_K$.

The first aim of this section is to prove that ρ is modular of parallel weight one. Below a comparison theorem with a universal deformation ring is deduced under certain conditions. The modularity is based on the following well-known lemma.

Lemma 4.1. *Let $\chi : G_L \rightarrow (\overline{\mathbb{Q}_p})^{\times}$ 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 tame Artin conductor of ρ. Then there exists a Hilbert modular eigenform f over K of parallel weight one of level $\Gamma_1(D)$ 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]). □

Let $S_1(\Gamma_1(\mathfrak{n}), \overline{\mathbb{Q}}_p)$ denote the space of parallel weight one cuspidal Hilbert modular forms over K of level $\Gamma_1(\mathfrak{n})$ with coefficients in $\overline{\mathbb{Q}}_p$ (for example, via a fixed isomorphism $\mathbb{C} \cong \overline{\mathbb{Q}}_p$). Further, let $\mathbb{T}_{1,\mathfrak{n}}$ be the $W(\mathbb{F})$-algebra generated by the Hecke operators $T_\mathfrak{q}$ for primes $\mathfrak{q} \nmid \mathfrak{n}p$ acting faithfully on $S_1(\Gamma_1(\mathfrak{n}), \overline{\mathbb{Q}}_p)$.

Proposition 4.2. *Let $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ be an absolutely irreducible, totally odd, dihedral representation. Let R be a complete Noetherian local ring with residue field $\mathbb{F}$ and let $\rho : G_K \to \mathrm{GL}_2(R)$ be a dihedral deformation of $\overline{\rho}$ with finite image. Suppose ρ is unramified at all the primes above p. Then there is an ideal $\mathfrak{n}_\rho$ of K coprime to p and a quotient $\mathbb{T}_{\mathrm{dih},\rho}$ of $\mathbb{T}_{1,\mathfrak{n}_\rho}$, as well as a Galois representation $\rho_{\mathrm{dih}} : G_K \to \mathrm{GL}_2(\mathbb{T}_{\mathrm{dih},\rho})$ and a homomorphism $\mathbb{T}_{\mathrm{dih},\rho} \to R$ such that*

1. *$\mathbb{T}_{\mathrm{dih},\rho}$ is a complete Noetherian local $W(\mathbb{F})$-algebra with residue field $\mathbb{F}$,*

2. *ρ_{dih} is a deformation of $\overline{\rho}$,*

3. *ρ factors as*
$$\rho : G_K \xrightarrow{\rho_{\mathrm{dih}}} \mathrm{GL}_2(\mathbb{T}_{\mathrm{dih},\rho}) \to \mathrm{GL}_2(R).$$

The Galois representation ρ_{dih} is unramified outside $p\mathfrak{n}_\rho$ and characterised by the property
$$\mathrm{Tr}(\rho_{\mathrm{dih}}(\mathrm{Frob}_\mathfrak{q})) = T_\mathfrak{q}$$
for all primes $\mathfrak{q} \nmid p\mathfrak{n}_\rho$.

Proof. We will refer to $\mathbb{T}_{\mathrm{dih},\rho}$ as just $\mathbb{T}_{\mathrm{dih}}$ throughout the proof for the ease of notation. The strategy is to factor the representation ρ via a ring S which will contain the Hecke algebra $\mathbb{T}_{\mathrm{dih}}$. We fix a field isomorphism $\overline{\mathbb{Q}}_p \cong \mathbb{C}$. Since ρ is assumed to be dihedral, there exists a quadratic extension L of K and a character $\chi : G_L \to R^\times$ such that $\rho = \mathrm{Ind}_{G_L}^{G_K}(\chi)$. We first factor χ uniquely as a product $\chi = \widehat{\overline{\chi}} \cdot \psi$, where $\widehat{\overline{\chi}}$ has prime-to p order (equal to the order of $\overline{\chi}$ and dividing the order of $\mathbb{F}^\times$) and the order of ψ is a power of p. As ρ is assumed to have finite image, we see that ψ is a character of finite order.

Let $U \subseteq R^\times$ be the image of ψ, that is, U is a finite p-group. Let $S := W(\mathbb{F})[U]$ be the group ring over the Witt vectors of $\mathbb{F}$. By the universal property of Witt vectors, we have a natural morphism $\epsilon : W(\mathbb{F}) \to R$. Consequently, $\widehat{\overline{\chi}}$ factors via ϵ:
$$\widehat{\overline{\chi}} : H \xrightarrow{\widehat{\overline{\chi}}} W(\mathbb{F}) \xrightarrow{\epsilon} R^\times.$$

Furthermore, by the universal property of group rings, we obtain a unique morphism $\delta : W(\mathbb{F})[U] \to R$ which is the identity on U and given by ϵ on $W(\mathbb{F})$. We can hence also factor ψ as
$$\psi : H \to U \xrightarrow{\mathrm{incl}} W(\mathbb{F})[U]^\times \xrightarrow{\delta} R^\times.$$

Denote by $\psi_S : H \to W(\mathbb{F})[U]^\times$ the composition of the first two maps. Defining $\chi_S := \widehat{\overline{\chi}} \cdot \psi_S : H \to W(\mathbb{F})[U]$, allows us to factor χ as
$$\chi : H \xrightarrow{\chi_S} W(\mathbb{F})[U]^\times \xrightarrow{\delta} R^\times.$$

30

We will now factor this map at $W(\mathbb{F})[U]$ towards a Hecke algebra.

In order to do so, we consider the homomorphism of $W(\mathbb{F})[U]$-algebras

$$\lambda : W(\mathbb{F})[U] \hookrightarrow \overline{\mathbb{Q}}_p[U] \xrightarrow{\sum_{u \in U} r_u u \mapsto (\sum_{u \in U} r_u \alpha(u))_\alpha} \prod_\alpha \overline{\mathbb{Q}}_p^{(\alpha)},$$

where α runs through all $\overline{\mathbb{Q}}_p^\times$-valued characters of the abelian group U and $\overline{\mathbb{Q}}_p^{(\alpha)}$ is the unique $\overline{\mathbb{Q}}_p$-vector space of dimension 1 with U-action via the character α. The first map is the natural inclusion and the second one is an isomorphism by standard characteristic zero representation theory of finite groups.

We first factor at $W(\mathbb{F})[U]$ using any of the characters α individually by letting

$$\rho_\alpha := \mathrm{Ind}_H^G(\widehat{\overline{\chi}} \cdot (\alpha \circ \psi_S)) : G \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p).$$

This is a deformation of $\overline{\rho}$. Let $\mathfrak{n}_\alpha$ be the tame Artin conductor of ρ_α. Then $\mathfrak{n}_\alpha$ is coprime to p and, as ρ is unramified at all primes above p, ρ_α is unramified outside primes dividing $n_\alpha \infty$. Moreover, we have for all prime ideals $\mathfrak{q} \nmid \mathfrak{n}_\alpha$:

$$\mathrm{Tr}(\rho_\alpha(\mathrm{Frob}_\mathfrak{q})) = \begin{cases} \widehat{\overline{\chi}}(\mathrm{Frob}_{\mathfrak{q}_1}) \cdot \alpha(\psi_S(\mathrm{Frob}_{\mathfrak{q}_1})) + \widehat{\overline{\chi}}(\mathrm{Frob}_{\mathfrak{q}_2}) \cdot \alpha(\psi_S(\mathrm{Frob}_{\mathfrak{q}_2})) & \text{if } \mathfrak{q}\mathcal{O}_L = \mathfrak{q}_1 \mathfrak{q}_2, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 4.1, there is a unique cuspidal Hilbert modular eigenform $f_\alpha \in S_1(\Gamma_1(\mathfrak{n}_\alpha), \overline{\mathbb{Q}}_p)$, the cuspidal parallel weight one space of level $\Gamma_1(\mathfrak{n}_\alpha)$, such that $T_\mathfrak{q} f_\alpha = \mathrm{Tr}(\rho_\alpha(\mathrm{Frob}_\mathfrak{q})) \cdot f_\alpha$ for all prime ideals $\mathfrak{q} \nmid \mathfrak{n}_\alpha$.

We now use standard arguments to 'interpolate all these f_α's' and introduce Hecke algebras for that reason. Let $\mathfrak{n}$ be the least common multiple of the ideals $\mathfrak{n}_\alpha$, running over all characters α. Let $W = \langle f_\alpha \mid \alpha : U \to \overline{\mathbb{Q}}_p^\times \rangle_{\overline{\mathbb{Q}}_p}$ be the $\overline{\mathbb{Q}}_p$-vector subspace of $S_1(\Gamma_1(\mathfrak{n}), \overline{\mathbb{Q}}_p)$ generated by the f_α. It is stable under all Hecke operators $T_\mathfrak{q}$ for $\mathfrak{q}$ running through the primes not dividing $p\mathfrak{n}$. Let $\mathbb{T}_{\mathrm{dih}}$ be the quotient of $\mathbb{T}_{1,\mathfrak{n}}$ acting faithfully on W.

Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ containing the $T_\mathfrak{q}$-eigenvalues of all $f_\alpha \in W$ for all primes $\mathfrak{q} \nmid \mathfrak{n}p$ and let $\mathfrak{m}$ be its maximal ideal. Now $\mathbb{T}_{\mathrm{dih}}$ is a subring of the $\mathcal{O}$-linear endomorphisms of the $\mathcal{O}$-span of all $f_\alpha \in W$. Since $\mathcal{O}$ is finite over $W(\mathbb{F})$ and the $\mathcal{O}$-span of all $f_\alpha \in W$ is finite over $\mathcal{O}$, we see that $\mathbb{T}_{\mathrm{dih}}$ is finite over $W(\mathbb{F})$. Hence, it is a complete Noetherian $W(\mathbb{F})$-algebra.

Since for any prime $\mathfrak{q} \nmid \mathfrak{n}p$, the $T_\mathfrak{q}$-eigenvalues of all f_α's are congruent modulo $\mathfrak{m}$, it follows, from the Deligne–Serre lemma, that $\mathbb{T}_{\mathrm{dih}}$ is local. Let $\mathfrak{m}'$ be its maximal ideal. Now, for any prime $\mathfrak{q} \nmid \mathfrak{n}p$, the image of $T_\mathfrak{q}$ modulo $\mathfrak{m}'$ is the same as the image of the $T_\mathfrak{q}$-eigenvalue of f_α modulo $\mathfrak{m}$ for any α. Hence, the image of $T_\mathfrak{q}$ modulo $\mathfrak{m}'$ is $\mathrm{Tr}(\overline{\rho}(\mathrm{Frob}_\mathfrak{q}))$ for all primes $\mathfrak{q} \nmid \mathfrak{n}p$ and, hence, lies in $\mathbb{F}$. Therefore, it follows that the residue field of $\mathbb{T}_{\mathrm{dih}}$ is $\mathbb{F}$.

In order to describe $\mathbb{T}_{\mathrm{dih}}$ explicitly, we use that 'multiplicity one' applied to the newforms f_α provides an injective $W(\mathbb{F})$-algebra homomorphism

$$\beta : \mathbb{T}_{\mathrm{dih}} \xrightarrow{T_\mathfrak{q} \mapsto \left(\mathrm{Tr}(\rho_\alpha(\mathrm{Frob}_\mathfrak{q})) \right)_\alpha} \prod_\alpha \overline{\mathbb{Q}}_p^{(\alpha)}.$$

By the description of $\operatorname{Tr}(\rho_\alpha(\operatorname{Frob}_{\mathfrak{q}}))$ above we obtain the crucial containment

$$\operatorname{im}(\beta) \subseteq \operatorname{im}(\lambda).$$

We may thus factor β as

$$\beta : \mathbb{T}_{\mathrm{dih}} \xrightarrow{\beta'} W(\mathbb{F})[U] \xrightarrow{\lambda} \prod_\alpha \overline{\mathbb{Q}}_p^{(\alpha)}.$$

In view of the above formulas, we explicitly have

$$\beta'(T_{\mathfrak{q}}) = \widehat{\overline{\chi}}(\operatorname{Frob}_{\mathfrak{q}_1}) \cdot \psi_S(\operatorname{Frob}_{\mathfrak{q}_1}) + \widehat{\overline{\chi}}(\operatorname{Frob}_{\mathfrak{q}_2}) \cdot \psi_S(\operatorname{Frob}_{\mathfrak{q}_2}) = \chi_S(\operatorname{Frob}_{\mathfrak{q}_1}) + \chi_S(\operatorname{Frob}_{\mathfrak{q}_2})$$

if $\mathfrak{q}\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$ and $\beta'(T_{\mathfrak{q}}) = 0$ otherwise. Consequently, $\delta(\beta'(T_{\mathfrak{q}})) = \operatorname{Tr}(\rho(\operatorname{Frob}_{\mathfrak{q}}))$ for all primes $\mathfrak{q}$ not dividing $\mathfrak{n}p$.

Now, the representation ρ_α takes values in $\operatorname{GL}_2(\mathcal{O})$ for all $f_\alpha \in W$ and $\operatorname{im}(\beta)$ also lies in $\prod_\alpha \mathcal{O}^{(\alpha)}$. Consider $\rho' = \prod_\alpha \rho_\alpha : G_K \to \prod_\alpha \operatorname{GL}_2(\mathcal{O})$. Note that $\rho_\alpha \pmod{\mathfrak{m}} = \overline{\rho}$ is absolutely irreducible. Now by the Chebotarev density theorem, $\operatorname{Tr}(\rho'(g)) \in \operatorname{im}(\beta)$ for all $g \in G_K$. Hence, applying [Car94, Théorème 2] to ρ', we obtain a Galois representation

$$\rho_{\mathrm{dih}} : G_K \to \operatorname{GL}_2(\mathbb{T}_{\mathrm{dih}})$$

which is unramified outside $\mathfrak{n}$ and satisfies $\operatorname{Tr}(\rho_{\mathrm{dih}}(\operatorname{Frob}_{\mathfrak{q}})) = T_{\mathfrak{q}}$ for all prime ideals $\mathfrak{q}$ not dividing $p\mathfrak{n}$.

Finally, we consider the composition

$$r : G_K \xrightarrow{\rho_{\mathrm{dih}}} \operatorname{GL}_2(\mathbb{T}_{\mathrm{dih}}) \xrightarrow{\beta'} \operatorname{GL}_2(W(\mathbb{F})[U]) \xrightarrow{\delta} \operatorname{GL}_2(R).$$

We see $\operatorname{Tr}(r(\operatorname{Frob}_{\mathfrak{q}})) = \operatorname{Tr}(\rho(\operatorname{Frob}_{\mathfrak{q}}))$ as well as $\operatorname{Tr}(\rho_{\mathrm{dih}}(\operatorname{Frob}_{\mathfrak{q}})) \pmod{\mathfrak{m}'} = \operatorname{Tr}(\overline{\rho}(\operatorname{Frob}_{\mathfrak{q}}))$ for all primes $\mathfrak{q} \nmid p\mathfrak{n}$. By [Car94, Théorème 1] we obtain that r and ρ are isomorphic and $\rho_{\mathrm{dih}} \pmod{\mathfrak{m}'}$ and $\overline{\rho}$ are isomorphic, proving the proposition. $\qquad\square$

We next apply this result to prove an '$R = \mathbb{T}$' theorem for the case that the universal deformation is dihedral. We first strive at a large generality.

Definition 4.3. *Let* **P** *be a property that a deformation of* $\overline{\rho}$ *may (or not) satisfy. We say that* **P** *is a deformation condition if* $\overline{\rho}$ *satisfies* **P**, **P** *only depends on the equivalence class of the representation and there exists a deformation* $\rho_{\mathbf{P}}^{\mathrm{univ}} : G \to \operatorname{GL}_2(R_{\mathbf{P}}^{\mathrm{univ}})$ *of* $\overline{\rho}$ *that is universal for the property* **P** *in the sense that for exactly those* $\rho : G \to \operatorname{GL}_2(R)$ *having property* **P**, *there is a unique morphism* $\phi : R_{\mathbf{P}}^{\mathrm{univ}} \to R$ *such that* $\rho = \phi \circ \rho_{\mathbf{P}}^{\mathrm{univ}}$.

See [Maz97, Section 23] for an alternate description of deformation conditions.

Theorem 4.4. *Let* **P** *be a deformation condition in the sense of Definition 4.3. Suppose that* $\rho_{\mathbf{P}}^{\mathrm{univ}}$ *is dihedral and unramified above* p. *Let* $\mathbb{T}_{\mathrm{dih}} := \mathbb{T}_{\mathrm{dih},\rho_{\mathbf{P}}^{\mathrm{univ}}}$ *be the Hecke algebra of parallel weight one attached to* $\rho_{\mathbf{P}}^{\mathrm{univ}}$ *by Proposition 4.2. Let* $\psi : \mathbb{T}_{\mathrm{dih}} \to R_{\mathbf{P}}^{\mathrm{univ}}$ *and* ρ_{dih} *be the associated ring homomorphism and Galois representation, respectively. Suppose further that* ρ_{dih} *also satisfies* **P**.

Then $R_{\mathbf{P}}^{\mathrm{univ}} \cong \mathbb{T}_{\mathrm{dih}}$.

Proof. As $\rho_{\mathbf{P}}^{\mathrm{univ}}$ is dihedral and unramified at p, it follows, by global class field theory, that it has finite image (see Proposition 2.1 and the discussion before Corollary 3.13). Hence, we can appeal to Proposition 4.2. Since ρ_{dih} satisfies $\mathbf{P}$, there is a morphism $\phi : R_{\mathbf{P}}^{\mathrm{univ}} \to \mathbb{T}_{\mathrm{dih}}$ such that $\rho_{\mathrm{dih}} = \phi \circ \rho_{\mathbf{P}}^{\mathrm{univ}}$. As $\mathbb{T}_{\mathrm{dih}}$ is generated by $T_{\mathfrak{q}} = \mathrm{Tr}(\rho_{\mathbb{T}_{\mathrm{dih}}}(\mathrm{Frob}_{\mathfrak{q}})) = \phi(\mathrm{Tr}(\rho_{\mathbf{P}}^{\mathrm{univ}}(\mathrm{Frob}_{\mathfrak{q}})))$ for primes $\mathfrak{q} \nmid p\mathfrak{n}$, the map ϕ is surjective. By Proposition 4.2, we know that $\psi \circ \rho_{\mathrm{dih}} = \rho_{\mathbf{P}}^{\mathrm{univ}}$. So, the composition $R_{\mathbf{P}}^{\mathrm{univ}} \xrightarrow{\phi} \mathbb{T}_{\mathrm{dih}} \xrightarrow{\psi} R_{\mathbf{P}}^{\mathrm{univ}}$ sends $\rho_{\mathbf{P}}^{\mathrm{univ}}$ to itself, *i.e.* $\psi \circ \phi : R_{\mathbf{P}}^{\mathrm{univ}} \to R_{\mathbf{P}}^{\mathrm{univ}}$ is a morphism such that $\psi \circ \phi \circ \rho_{\mathbf{P}}^{\mathrm{univ}} = \rho_{\mathbf{P}}^{\mathrm{univ}}$. Hence, the universality of $R_{\mathbf{P}}^{\mathrm{univ}}$ implies that $\psi \circ \phi$ is the identity morphism. This proves that ϕ is also injective. $\qquad\square$

Set-up 4.5. *We continue to assume Set-up 3.2 in the above setting. 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. Let D be the tame Artin conductor of $\overline{\rho}$.*

For the rest of this section, we specialise Set-up 3.2 as indicated in section 1.5:

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].

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 $[K_\ell(\mu_p) : K_\ell] = 2$. Note that the definition of vexing primes makes sense for any absolutely irreducible $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$. Recall that for an absolutely irreducible $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ and a finite set of primes S of K, we have defined R_S^{univ} (resp. ρ_S^{univ}) to be the universal deformation ring (resp. universal deformation) of $\overline{\rho}$ relatively unramified outside S and $(R_S^{\mathrm{univ}})^0$ (resp. $(\rho_S^{\mathrm{univ}})^0$) to be its constant determinant counterpart (see §3). We will now define minimal deformation problems, following [CG18].

Definition 4.6. *Let R be an object of $\mathcal{C}$ and let $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ be an absolutely irreducible representation satisfying assumption (5) of Set-up 4.5. 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 $\overline{\rho}$ is ramified at ℓ and $\overline{\rho}|_{G_{K_\ell}}$ is not absolutely irreducible, then ρ^{I_ℓ} is a rank 1 direct summand of ρ as an R-module.*

For $K = \mathbb{Q}$ and odd $\overline{\rho}$, 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 $\rho^{\min}$.

Lemma 4.7. *Let $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ be an absolutely irreducible representation satisfying assumptions (4) and (5) of Set-up 4.5. Let D be the tame Artin conductor of $\overline{\rho}$ and 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, $R^{\min} \simeq (R_S^{\mathrm{univ}})^0$. $\qquad\square$

Proposition 4.8. *Let $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ be a dihedral representation satisfying all the assumptions of Set-up 4.5. Then $\rho^{\min}$ is dihedral.*

Proof. From Lemma 4.7, we know that $R^{\min} \simeq (R_S^{\mathrm{univ}})^0$, where S is 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. Moreover, the proof of Lemma 4.7 implies that this isomorphism takes $\rho^{\min}$ to $(\rho_S^{\mathrm{univ}})^0$. Let S_1, S_2, S_3 and S_0 be the set of primes of K defined in §3 right after Proposition 3.3. We keep using Notation 3.1 and prove that $S \cap S_0 = \emptyset$. 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 $S \cap S_0 = \emptyset$. This allows us to apply Theorem 1.5 to conclude that ρ_S^{univ} is dihedral. The result follows. $\qquad\square$

Proof of Theorem 1.9. Let S be as in Proposition 4.8, so that we can describe $R^{\min}$ as $(R_S^{\mathrm{univ}})^0$. By Proposition 4.8 and Proposition 4.2, there exists a quotient $\mathbb{T}_{\mathrm{dih}}$ of $\mathbb{T}_{1,D'}$, a deformation $\rho_{\mathrm{dih}} : G_K \to \mathrm{GL}_2(\mathbb{T}_{\mathrm{dih}})$ of $\overline{\rho}$ and a map $\phi : \mathbb{T}_{\mathrm{dih}} \to R^{\min}$ such that $\phi \circ \rho_{\mathrm{dih}} = \rho^{\min}$. Here D' is an ideal of $\mathcal{O}_K$ such that $D|D'$ and D'/D is only divisible by primes lying in S. By construction the determinant of ρ_{dih} is equal to the Teichmüller lift of $\overline{\rho}$. By Proposition 4.8, $\rho^{\min}$ factors through $\mathrm{Gal}(M^{\overline{\rho}}(S)/K)$. Hence, from the proof of Proposition 4.2, it follows that ρ_{dih} factors through $\mathrm{Gal}(M^{\overline{\rho}}(S)/K)$. Hence ρ_{dih} a deformation of $\overline{\rho}$ that is relatively unramified outside S with constant determinant. In view of Proposition 4.8, ρ_{dih} is hence a minimal deformation of $\overline{\rho}$. Consequently, Theorem 4.4 finishes the proof. $\qquad\square$

Remark 4.9. *If $\mathrm{Hom}_{\mathbb{F}_p[\overline{G}^{\mathrm{ad}}]}(A(M^{\mathrm{ad}})/pA(M^{\mathrm{ad}}), I(\overline{\chi}/\overline{\chi}^\sigma)) \neq 0$, then, as seen in Remark 3.12, 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.*

Note that we can remove assumption 5 from Set-up 4.5 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 4.10. *Let $\overline{\rho}$ be a dihedral representation satisfying all the assumptions of Set-up 4.5 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 relatively 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 4.1, we conclude the existence of the parallel weight one eigenform f over K having the required property. $\square$

See [Cal18, Theorem 1.1] for a similar but much stronger result for $K = \mathbb{Q}$.

Remark 4.11. *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.

5.1 Examples of $\overline{\rho}$ such that $\rho_{S_\infty}^{\mathrm{univ}}$ is non-dihedral for $p = 2$

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:

$$
\begin{array}{ccccccccc}
& & & & \mathrm{Gal}(M/K) & & & & \\
& & & & \downarrow\sim & & & & \\
0 & \longrightarrow & V_4 & \longrightarrow & S_4 & \longrightarrow & S_3 & \longrightarrow & 0 \\
& & \downarrow{\mathrm{id}\oplus 0} & \quad\rho & \downarrow & \quad\overline{\rho} & \| & & \\
0 & \longrightarrow & I \oplus C(1) & \longrightarrow & \mathrm{SL}_2(\mathbb{F}_2[\epsilon]/(\epsilon^2)) & \longrightarrow & \mathrm{SL}_2(\mathbb{F}_2) & \longrightarrow & 0
\end{array}
$$

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 $\mathbb{Q}$.

36

5.2 Strategy for finding examples of $\overline{\rho}$ such that $\rho_{S_\infty}^{\mathrm{univ}}$ is dihedral for $p > 2$

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 an $\mathbb{F}_p[\mathrm{Gal}(M/L)]$-module. Let $\overline{\rho} := \mathrm{Ind}_{G_L}^{G_K}(\overline{\chi}^b)$ for any $b \in \mathbb{F}_q^\times$. In the notation of Set-up 2.6, $\overline{H}^{\mathrm{ad}} = \mathrm{Gal}(M/L)$ 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 of Set-up 2.6, $\overline{G}^{\mathrm{ad}} = \mathrm{Gal}(M/K)$. 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 $M_2 = L_2 M$ 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 allows us to derive concrete examples of dihedral $\overline{\rho}$ satisfying desired hypotheses by computing class numbers of abelian extensions. To be precise, after computing the class numbers, we got examples of both case (1) and case (2) (see §5.3, §5.4, §5.5 and §5.6). Thus we get examples of dihderal $\overline{\rho}$'s of both kinds, one where everywhere relatively unramified universal deformation of $\overline{\rho}$ is dihedral (case (1)) and one where it is not dihedral (case (2)). All computations were performed using Magma [BCP97] under the assumption of the Generalised Riemann Hypothesis (GRH).

5.3 Examples of cases (1) and (2) for $K = \mathbb{Q}$

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 66 others
3	5	all imaginary quadratic fields of class number 15 of abs. value of discriminants ≤ 19387	case (1): all 60 fields
7	3	all imaginary quadratic fields of class number 21 of abs. value of discriminants ≤ 14419	case (2): discriminant: -8059 case (1): all 41 others

3	7	all imaginary quadratic fields of class number 21 of abs. value of discriminants ≤ 5867	case (1): all 18 fields
11	3	all imaginary quadratic fields of class number 33 of abs. value of discriminants ≤ 28163	case (1): all 38 fields
3	11	all imaginary quadratic fields of class number 33 of abs. value of discriminants ≤ 1583	case (1): all 2 fields
7	5	all imaginary quadratic fields of class number 35 of abs. value of discriminants ≤ 16451	case (1): all 25 fields
5	7	all imaginary quadratic fields of class number 35 of abs. value of discriminants ≤ 4931	case (1): all 7 fields

5.4 Examples of case (1) for quadratic extensions of $\mathbb{Q}$

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 1.9) 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.

5.5 Examples of case (2) for $K = \mathbb{Q}$

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

5.6 Example of case (2) for real quadratic fields

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.

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).

[Bel19]   Joël Bellaïche. Image of pseudorepresentations and coefficients of modular forms modulo p. *Adv. Math.*, 353:647–721, 2019.

[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.

[Cal18]   Frank Calegari. Non-minimal modularity lifting in weight one. *J. Reine Angew. Math.*, 740:41–62, 2018.

[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.

[Col96]   Robert F. Coleman. Classical and overconvergent modular forms. *Invent. Math.*, 124(13):215–241, 1996.

[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.

[CWE]   Francesc Castella and Carl Wang-Erickson. Class groups and local indecomposability for non-CM forms (with an appendix by Haruzo Hida). *To appear in J. Eur. Math. Soc. (JEMS)*.

[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.

[GV04]   Eknath Ghate and Vinayak Vatsal. On the local bheaviour of ordinary λ-adic representations. *Ann. Inst. Fourier (Greenoble)*, 54(7):2143–2162, 2004.

[GV11]   Eknath Ghate and Vinayak Vatsal. Locally indecomposable galois representations. *Canad. J. Math.*, 63(2):277–297, 2011.

[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.

[Kis03]   Mark Kisin. Overconvergent modular forms and the fontaine-mazur conjecture. *Invent. Math.*, 153:373–454, 2003.

[LMF]   The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`.

[Maz89] B. Mazur. Deforming Galois representations. In *Galois groups over* **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.

[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.

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

Shaunak V. Deo
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400005
India
deoshaunak@gmail.com

Gabor Wiese
University of Luxembourg
Department of Mathematics
Maison du nombre

6, avenue de la Fonte

L-4364 Esch-sur-Alzette

Grand-Duchy of Luxembourg

`gabor.wiese@uni.lu`