Rev. Mat. Iberoam. **34** (2018), no. 4, 1609–1643
DOI 10.4171/RMI/1037

Congruences between modular forms modulo prime powers

Maximiliano Camporino and Ariel Pacetti

Abstract. Given a prime $p \geq 5$ and an abstract odd representation ρ_n with coefficients modulo p^n (for some $n \geq 1$) and big image, we prove the existence of a lift of ρ_n to characteristic 0 whenever local lifts exist (under minor technical conditions). Moreover, our results allow to chose the lift's inertial type at all primes but finitely many (where the lift is of Steinberg type).

We apply this result to the realm of modular forms, proving a level lowering theorem modulo prime powers and providing examples of level raising. An easy application of our main result proves that given a modular eigenform f whose Galois representation is not induced from a character (i.e., f has no inner twists), for all primes p but finitely many, and for all positive integers n, there exists an eigenform $g \neq f$, which is congruent to f modulo p^n.

1. Introduction

The aim of the present article is to deal with congruences between modular forms (even more generally between abstract Galois representations) modulo prime powers. For that purpose we adapt the arguments of [13] and [14] with the extra care of the problems coming from semisimplification issues. Let $\mathbb{F}$ be a finite field of residual characteristic p, $W(\mathbb{F})$ its ring of Witt vectors and $\rho_n \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(W(\mathbb{F})/p^n)$ be a continuous representation. We denote by $\overline{\rho_n}$ its reduction modulo p.

Theorem A. *Let $\mathbb{F}$ be a finite field of characteristic $p \geq 5$. Let $\rho_n \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(W(\mathbb{F})/p^n)$ be a continuous representation ramified at a finite set of primes S satisfying the following properties*:

- *the image of $\overline{\rho_n}$ is big, i.e., $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho_n})$ and $\mathrm{Im}(\overline{\rho_n}) = \mathrm{GL}_2(\mathbb{F})$ if $p = 5$,*
- *ρ_n is odd,*

Mathematics Subject Classification (2010): Primary 11F33; Secondary 11F80.
Keywords: Modular forms, Galois representations.

- *the restriction* $\overline{\rho_n}|_{G_p}$ *is not twist equivalent to the trivial representation nor the indecomposable unramified representation given by* $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$,
- ρ_n *does not ramify at* 2.

Let P *be a finite set of primes containing* S*, and for every* $\ell \in P$, $\ell \neq p$*, assume there exists a local deformation* $\rho_\ell \colon G_\ell \to W(\mathbb{F})$ *of* $\rho_n|_{G_\ell}$*. At the prime* p*, assume there exists a local deformation* ρ_p *of* $\rho_n|_{G_p}$ *which is ordinary or crystalline with Hodge–Tate weights* $\{0, k\}$*, with* $2 \leq k \leq p-1$.

Then there is a finite set Q *of auxiliary primes* $q \not\equiv \pm 1 \pmod{p}$ *and a modular representation*

$$\rho : G_{P \cup Q} \longrightarrow \mathrm{GL}_2(W(\mathbb{F})),$$

such that:

- *the reduction modulo* p^n *of* ρ *is* ρ_n,
- $\rho|_{I_\ell} \simeq \rho_\ell|_{I_\ell}$ *for every* $\ell \in P$, $\ell \neq p$,
- $\rho|_{G_p}$ *has the same type as* ρ_p*, i.e., if* ρ_p *is ordinary,* $\rho|_{G_p}$ *is ordinary while if* ρ_p *is crystalline,* $\rho|_{G_p}$ *is crystalline with the same Hodge–Tate weights,*
- $\rho|_{G_q}$ *is a ramified representation of Steinberg type for every* $q \in Q$.

Although for the applications we have in mind, we focused in the case of odd representations (which by Serre's conjectures are modular), with some extra hypotheses as in [13] one can get a result for any abstract representation with big image.

Remark 1.1. The main theorems of this article concern global representations modulo p^n, and their deformations. We do not consider the problem of classifying local representations modulo p^n nor the problem of determining which ones do lift to characteristic zero, which are very subtle problems. The hypothesis that a local lift exists and is given for each ramified prime plays a crucial role in our proofs.

Remark 1.2. In the work [9], while trying to give another proof of the Taylor–Wiles theorem, they do consider lifts of the reduction modulo p^n of a global representation ρ, so their Step 1 is a weaker version of our Theorem A. Since they only need a lift to exist, they can choose the inertia type at all primes but the auxiliary ones which makes the computations much easier. Sections 4, 5 and 6 of the present article deal with the difficulties that arise while allowing any local deformation at inertia.

Remark 1.3. Theorem A is in the same spirit as Theorem 3.2.2 of [1], where only residual representations are considered. The advantage of working with the deformation ring itself (instead of constructing the deformation) is that no auxiliary set of primes is needed (i.e., one can take $Q = \emptyset$ in the main theorem) but one loses control on the coefficient ring (so the deformation obtained might have coefficients in a finite extension of $W(\mathbb{F})$). This phenomena only works while working modulo a prime ideal. For example, the elliptic curve $329a1$ is unramified at 7 modulo 9, but there are no newforms of level 47 congruent to it modulo 9 (see for example [6]).

Let $f \in S_k(\Gamma_0(N), \epsilon)$ $(k \geq 2)$ be a newform, with coefficient field K_f. Denote by $\mathcal{O}_f$ the ring of integers of K_f. If p is a prime number, let $\mathfrak{p}$ denote a prime ideal in $\mathcal{O}_f$ dividing p, $K_\mathfrak{p}$ denote the completion of K_f at $\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ its ring of integers. Finally let $\rho_{f,p}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_\mathfrak{p})$ denote its associated p-adic Galois representation. If n is a positive integer, let

$$\rho_n : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^n)$$

be its reduction modulo $\mathfrak{p}^n$.

Theorem B. *In the above hypothesis, let $n > 0$ be an integer and $p > \max(k, 3)$ be a prime such that*:

- *$p \nmid N$ or f is ordinary at p,*
- *$\mathrm{SL}_2(\mathcal{O}_\mathfrak{p}/\mathfrak{p}) \subseteq \mathrm{Im}(\overline{\rho_{f,p}})$, and $\mathrm{Im}(\overline{\rho_{f,p}}) = \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}/\mathfrak{p})$ if $p = 5$,*
- *p does not ramify in the field of coefficients of f,*
- *ρ_n does not ramify at 2.*

Let R be the set of ramified primes of ρ_n. If $N' = \prod_{\ell \in R} \ell^{v_\ell(N)}$, then there exist an integer r, a set $\{q_1, \ldots, q_r\}$ of auxiliary primes prime to N satisfying $q_i \not\equiv 1 \pmod{p}$ and a newform g, different from f, of weight k and level $N'q_1 \cdots q_r$ such that f and g are congruent modulo p^n. Furthermore, the form g can be chosen with the same restriction to inertia as that of f at the primes of R.

A direct application of Theorem B is a lowering the level result modulo prime powers. Such result is proven in [9] (Proposition 1, while proving the main theorem), and in [6] (Theorem 1), under the assumption that the primes losing ramification are not congruent to ± 1 modulo p.

Corollary 1.4 (Lowering the level)**.** *Let $f \in S_k(\Gamma_0(M), \varepsilon)$ be a newform, let $\mathfrak{p}$ be a prime of $\mathcal{O}_f$ above $p \in \mathbb{Q}$, and let $\rho_n\colon G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_f/\mathfrak{p}^n)$ be the reduction of its $\mathfrak{p}$-adic representation modulo $\mathfrak{p}^n$. Suppose that*:

- *$p \geq 5$,*
- *$2 \leq k \leq p - 1$,*
- *$\mathrm{SL}_2(\mathcal{O}_f/\mathfrak{p}) \subseteq \mathrm{Im}(\overline{\rho_n})$ and $\mathrm{Im}(\overline{\rho_n}) = \mathrm{GL}_2(\mathcal{O}_f/\mathfrak{p})$ if $p = 5$,*
- *p does not ramify in $\mathcal{O}_f$,*
- *ρ_n does not ramify at 2.*

If $\ell \mid M$ is such that ρ_n is unramified at ℓ, then the Hecke map factors through the ℓ-old quotient $\mathbb{T}_k^{\ell\text{-old}}(M, \ell)$, i.e., if $M = \ell^r M'$, with $\ell \nmid M'$, then there exists a representation $\rho_n\colon \mathbb{T}_k(M') \to \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}^n)$ isomorphic to ρ_n.

Proof. The proofs of [9] and [6] give the result for primes ℓ where ramification is lost and satisfy $\ell \not\equiv 1 \pmod{p}$. Theorem B allows us to move the ramification to some auxiliary set of controlled Steinberg primes. More concretely, if there exist some primes ℓ with $\ell \equiv \pm 1 \pmod{p}$ loosing ramification, Theorem B implies the existence of a form g congruent modulo $\mathfrak{p}^n$ with f, with good reduction at the primes ℓ and bad reduction at some extra set of Steinberg primes $q \not\equiv \pm 1 \pmod{p}$. The form g is now in the hypothesis of Dummigan's theorem, and the result follows.

Note that Theorem 1 in [6], as explained in Section 9 of the same article, takes a Galois representation as an input and returns a Hecke map from a subgroup with one prime ℓ removed from the level. Since we need to make repeated use of it (to remove all auxiliary primes), we need a similar statement that allows a Hecke map as an input. As was pointed out by Professor Dummigan, Theorem 1 of [6] holds in this more general situation with exactly the same proof. □

Corollary 1.5. *Let $k \geq 2$, N odd, and let $f \in S_k(\Gamma_0(N), \epsilon)$ be a newform whose Galois representation is not induced from a character (i.e., it has no inner twists). Then for all but finitely many prime numbers p, and for all positive integers n, there exists a weight k newform g (depending on p and n) different from f, which is congruent to f modulo p^n.*

Proof. Since f does not have inner twists, by Ribet's result ([16], Theorem 3.1) the residual image of the p-adic Galois representation attached to f is big modulo p for all but finitely many primes p. Then the set of primes p where any of the following properties hold is finite:

- $p \leq k$,
- the residual image of $\overline{\rho_{f,p}}$ is not big,
- p divides N (or if it does, f is not ordinary at p),
- p is ramified in the coefficient field of f,

All the other primes are in the hypothesis of Theorem B and the result follows. □

The proof of Theorem A follows the ideas of [14] and involves solving two different problems. One consists on constructing a finite set of auxiliary primes that converts the problem of lifting a global representation into the one of lifting many local ones. The other consists in solving the somewhat easier local lifting problems. Following the logical structure of [14], we deal with the local considerations first.

To solve the local lifting problems, for every prime $\ell \in P$ we need to find a set C_ℓ of deformations of $\rho_n|_{G_\ell}$ to $W(\mathbb{F})$ containing ρ_ℓ and a subspace $N_\ell \subseteq \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ of the right codimension such that: elements of N_ℓ preserve the reductions of C_ℓ (i.e., whenever ρ_m is the reduction of some $\rho \in C_\ell$ modulo p^m and $u \in N_\ell$ then $(1 + p^{m-1}u)\rho_m$ is the reduction of some other $\rho' \in C_\ell$) and any deformation ρ_m can be modified by an element not in N_ℓ to lie in C_ℓ. Furthermore, we also need all the deformations in C_ℓ to be isomorphic when restricted to I_ℓ. For each prime $\ell \in P$ the restriction of the global representation to a decomposition group at ℓ provide a mod p^n representation ρ_n and a local representation ρ_ℓ lifting $\rho_n|_{G_\ell}$. We proceed as follows:

1. We classify all the possible ρ_ℓ up to $\overline{\mathbb{Z}_p}$-isomorphism and all the possible $\overline{\rho_n}$ up to $\overline{\mathbb{F}}$-isomorphism.
2. For each pair of isomorphism classes for ρ_ℓ and $\overline{\rho_n}$ we try to construct a set C_ℓ (depending on the class of ρ_ℓ) of deformations with coefficients in $W(\mathbb{F})$ which are congruent to ρ_ℓ mod p^n and the corresponding subspace $N_\ell \subseteq \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ (depending on the class of $\overline{\rho_n}|_{G_\ell}$) preserving it.

While pursuing the second objective one flaw appears. There is one case (labeled Case 4 (1) in Section 4) for which the pair (C_ℓ, N_ℓ) satisfies the desired properties not modulo p^m for all $m \geq n$ but for all $m \geq n_0 > n$ (depending on $\overline{\rho_n}|_{G_\ell}$). To overcome this problem, we construct a lift of ρ_n to $W(\mathbb{F})/p^{n_0+1}$ (via a completely different argument explained in Section 6) and then we follow the ideas explained earlier.

Once the right local deformations classes are chosen (and the case of small exponents is handled), we need to construct two auxiliary sets of primes Q_1 and Q_2 (together with their respective sets C_q and subspaces N_q as for the primes in P) with the following roles:

- The set Q_1 has two main properties (see Fact 16 in [14]): it kills the global obstructions, that is, it is such that $\text{Ш}^1_{S\cup Q_1}((\text{Ad}^0\bar{\rho})^*) = 0$ (and therefore $\text{Ш}^2_{S\cup Q_1}(\text{Ad}^0\bar{\rho}) = 0$ by global duality), and it is such that the inflation map

$$\text{H}^2(G_S, \text{Ad}^0\bar{\rho}) \to \text{H}^2(G_{S\cup Q_1}, \text{Ad}^0\bar{\rho}),$$

  is an isomorphism.

- The set Q_2 gives an isomorphism

$$\text{H}^1(G_{S\cup Q_1\cup Q_2}, \text{Ad}^0\bar{\rho}) \to \bigoplus_{\ell\in S\cup Q_1\cup Q_2} \text{H}^1(G_\ell, \text{Ad}^0\bar{\rho})/N_\ell,$$

  without adding global obstructions, i.e., $\text{Ш}^2_{S\cup Q_1\cup Q_2} = 0$.

These auxiliary primes are essentially Ramakrishna's Q and T sets (in [14], with the same sets C_q and subspace N_q). Just some extra care needs to be taking while proving that $\rho_n|_{G_q}$ is the reduction of some $\rho \in C_q$ for every $q \in Q_1 \cup Q_2$.

With the local conditions and the auxiliary primes, the *inductive method* starts to work since each step only depends on hypotheses about the mod p reduction of our representation.

The inductive method works as follows: in virtue of $\text{Ш}^2_{S\cup Q_1}(\text{Ad}^0\bar{\rho}) = 0$, a global deformation to $W(\mathbb{F})/p^m$ lifts to $W(\mathbb{F})/p^{m+1}$ if and only if its restrictions to the primes of $P \cup Q_1 \cup Q_2$ lift to $W(\mathbb{F})/p^{m+1}$. For $m = n$ the local condition is automatic so there exists a lift ρ_{n+1} of ρ_n to $W(\mathbb{F})/p^{n+1}$. The problem is that ρ_{n+1} may not lift again, as it can be locally obstructed. In order to remove these local obstructions we use the fact that any local deformation for primes $\ell \in P\cup Q_1\cup Q_2$ can be modified by some element not in N_ℓ in order to be a reduction of some element of C_ℓ and therefore unobstructed. We will often refer to this as *adjusting a local deformation*. As we have an isomorphism between the global first cohomology group and the coproduct of the local first cohomology groups modulo N_ℓ, we can find an element $u \in \text{H}^1(G_\mathbb{Q}, \text{Ad}^0\bar{\rho})$ that adjusts ρ_{n+1} locally for every prime in $P \cup Q_1 \cup Q_2$ making $(1 + p^n u)\rho_{n+1}$ an unobstructed lift of ρ_n satisfying all the required local hypothesis (its restriction to G_ℓ lies in C_ℓ for all primes $\ell \in P$) and in particular it satisfies the condition at inertia. From here we can repeat the process of lifting and adjusting indefinitely, obtaining a lift to $W(\mathbb{F})$.

Theorem A follows from these ideas and some appropriate modularity lifting theorem (which explain the conditions imposed at p). Theorem B is an immediate consequence of Theorem A.

Notations and conventions. Throughout this work $G_{\mathbb{Q}}$ denotes the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If ℓ is a prime number, G_ℓ denotes a decomposition group of ℓ inside $G_{\mathbb{Q}}$. Inside this Galois group, σ and τ will stand for a Frobenius element and a tame inertia generator respectively. Whenever we need to make the dependency on q explicit, we will name a Frobenius element in G_q by Frob_q. We will denote by $\mathbb{F}$ a finite field of characteristic p and by $W(\mathbb{F})$ its ring of Witt vectors.

Regarding representations, ρ_n denotes a continuous representation $\rho_n\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(W(\mathbb{F})/p^n)$, ρ a continuous representation with coefficients in $W(\mathbb{F})$ ramifying at finitely many primes and $\overline{\rho}$ a representation modulo p. If ω is a character from $G_{\mathbb{Q}}$ to $\mathbb{F}$ we denote $\tilde{\omega}$ its Teichmüller lift.

We will denote by χ the p-adic cyclotomic character. If $\det\overline{\rho} = \omega\overline{\chi}^k$, with ω unramified at p, we will consider only deformations with fixed determinant $\tilde{\omega}\chi^k$ which allows to consider $\mathrm{Ad}^0\bar{\rho}$ instead of $\mathrm{Ad}\,\bar{\rho}$. If ρ is any continuous representation, $\mathbb{Q}(\rho)$ denotes the field fixed by its kernel. Given $\overline{\rho}$, after twisting it by a character of finite order we may, and will, suppose that $\overline{\rho}$ and $\mathrm{Ad}^0\bar{\rho}$ ramify at the same set of primes S. Finally, for a ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_p$, v will stand for the valuation that has value 1 at the uniformizer.

Acknowledgments. Special thanks go to Luis Dieulefait, for proposing us the problem of Corollary 1.5 (the starting point of the present article) as well as many discussions and suggestions he made which improved the exposition, and to Ravi Ramakrishna for many suggestions which not only improved the exposition, but also allowed to remove some technical conditions in a first version of this article. We thank Professor Dummigan for explaining us how to adapt his lowering the level results needed in Corollary 1.4, and Gabor Wiese for many corrections and comments, Panagiotis Tsaknias for pointing out the application of Theorem A to Corollary 1.4, and John Jones and Bill Allombert for helping us with the computational part of the example. At last, we would like to consider the referee for his/her suggestions and comments that improved the article quality.

2. Classification of residual representations and types of reduction

Recall the classification of mod p representations of G_ℓ, when $\ell \neq p$ (see for example [4], Chapter XVII, Section 2).

Proposition 2.1. *Let $\ell \neq 2$, be a prime number, with $\ell \neq p$. Then up to twist by a character of finite order any representation $\overline{\rho}\colon G_\ell \to \mathrm{GL}_2(\overline{\mathbb{F}})$ belongs to one of the following three types*:

- **Principal Series:** $\overline{\rho} \simeq \left(\begin{smallmatrix}\phi & 0\\ 0 & 1\end{smallmatrix}\right)$ *or* $\overline{\rho} \simeq \left(\begin{smallmatrix}1 & \psi\\ 0 & 1\end{smallmatrix}\right)$.
- **Steinberg:** $\overline{\rho} \simeq \left(\begin{smallmatrix}\chi & \mu\\ 0 & 1\end{smallmatrix}\right)$, *where* $\mu \in \mathrm{H}^1(G_\ell, \mathbb{F}(\chi))$ *and* $\mu|_{I_\ell} \neq 0$.

- **Induced:** $\overline{\rho} \simeq \mathrm{Ind}_{G_M}^{G_\ell}(\xi)$, *where* $M/\mathbb{Q}_\ell$ *is a quadratic extension and* $\xi\colon G_M \to \overline{\mathbb{F}}^\times$ *is a character not equal to its conjugate under the action of* $\mathrm{Gal}(M/\mathbb{Q}_\ell)$.

Here $\phi\colon G_\ell \to \overline{\mathbb{F}}^\times$ *is a multiplicative character and* $\psi\colon G_\ell \to \overline{\mathbb{F}}$ *is an unramified additive character.*

Remark 2.2. Any unramified representation is Principal Series, and can be of the form $\overline{\rho} \simeq \left(\begin{smallmatrix}\phi & 0\\ 0 & 1\end{smallmatrix}\right)$, with ϕ unramified or of the form $\overline{\rho} \simeq \left(\begin{smallmatrix}1 & \psi\\ 0 & 1\end{smallmatrix}\right)$, with $\psi : G_\ell \to \mathbb{F}$ an additive unramified character.

The same classification applies to continuous representations $\rho\colon G_\ell \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ modulo $\mathrm{GL}_2(\overline{\mathbb{Q}_p})$ equivalence, but to deal with reductions modulo prime powers we need a classification of representations with integer coefficients modulo $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$ equivalence. Let L be the coefficient field of ρ, $\mathcal{O}_L$ its ring of integers, and π be a local uniformizer. Let also $\mu \in \mathrm{H}^1(G_\ell, \mathbb{Z}_p(\chi))$ denote a generator of this.

Theorem 2.3. *Let* $\rho\colon G_\ell \to \mathrm{GL}_2(\overline{\mathbb{Z}_p})$ *be a continuous representation. Then, up to twist (by a finite order character times powers of the cyclotomic one) and* $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$ *equivalence, we have*:

- **Principal Series:** $\rho \simeq \left(\begin{smallmatrix}\phi & \pi^r(\phi-1)\\ 0 & 1\end{smallmatrix}\right)$, *with* $r \in \mathbb{Z}_{\leq 0}$ *satisfying* $\pi^r(\phi-1) \in \overline{\mathbb{Z}_p}$ *or* $\rho \simeq \left(\begin{smallmatrix}1 & \psi\\ 0 & 1\end{smallmatrix}\right)$.
- **Steinberg:** $\rho \simeq \left(\begin{smallmatrix}\chi & \pi^r\mu\\ 0 & 1\end{smallmatrix}\right)$, *with* $r \in \mathbb{Z}_{\geq 0}$.
- **Induced:** *There exists a quadratic extension* $M/\mathbb{Q}_\ell$ *and a character* $\xi\colon G_M \to \overline{\mathbb{Z}_p}^\times$ *not equal to its conjugate under the action of* $\mathrm{Gal}(M/\mathbb{Q}_\ell)$ *such that* $\rho \simeq \langle v_1, v_2\rangle_{\mathcal{O}_L}$, *where for* α *a generator of* $\mathrm{Gal}(M/\mathbb{Q}_\ell)$ *and* $\beta \in G_M$, *the action is given by*

$$\beta(v_1) = \xi(\beta)v_1, \quad \beta(v_2) = \xi^\alpha(\beta)v_2, \quad \alpha(v_1) = v_2 \quad \text{and} \quad \alpha(v_2) = \xi(\alpha^2)v_1,$$

or

$$\rho(\beta) = \begin{pmatrix}\xi(\beta) & (\xi(\beta) - \xi^\alpha(\beta))/\pi^r\\ 0 & \xi^\alpha(\beta)\end{pmatrix} \quad \text{and} \quad \rho(\alpha) = \begin{pmatrix}-a & (\xi(\alpha^2) - a^2)/\pi^r\\ \pi^r & a\end{pmatrix},$$

where ξ^α *is the character of* G_M *defined by* $\xi^\alpha(g) = \xi(\alpha g \alpha^{-1})$ *and* $a \in \mathcal{O}_L^\times$. *Observe that when* $M/\mathbb{Q}_\ell$ *is ramified we can take* α *and* β *to be a Frobenius element and a generator of the tame inertia of* G_ℓ, *respectively.*

Proof. Suppose that ρ is irreducible, and that the image lies in $\mathrm{GL}_2(\mathcal{O}_L)$ for $L/\mathbb{Q}_p$ finite. There exists a quadratic extension $M/\mathbb{Q}_\ell$ and a character $\xi\colon G_M \to \mathcal{O}_L^\times$ such that $\rho \simeq \mathrm{Ind}_{G_m}^{G_{\mathbb{Q}_\ell}} \xi$ (modulo $\mathrm{GL}_2(\mathbb{Q}_\ell)$ equivalence). Let $\{v_1, v_2\}$ be a basis of the underlying 2-dimensional $\mathbb{Q}_\ell$ vector space, where $v_2 = \alpha(v_1)$ for α a generator of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$. Let T be one invariant lattice for ρ. There exists a minimum $s \in \mathbb{Z}$ such that $w_1 = \pi^s v_1 \in T$. Re-scaling T we can assume that $s = 0$ (re-scaling the lattice does not affect the representation). Since $\alpha(T) \subseteq T$, $\langle v_1, v_2\rangle_{\mathcal{O}_L} \subseteq T$. If equality holds we get the first case.

Otherwise, we can extend v_1 to a basis of T by adding a vector $w \in T$ with $w \notin \langle v_1, v_2 \rangle_{\mathcal{O}_L}$. Write $w = \lambda_1 v_1 + \lambda_2 v_2$ with $\lambda_1, \lambda_2 \in \mathbb{Q}_p$. Notice that necessarily $v_\pi(\lambda_1) = v_\pi(\lambda_2) < 0$ (since $\alpha(v_2) = \xi(\alpha^2)v_1$, and $\xi(\alpha^2) \in \mathcal{O}_L^\times$). Changing v_1 and v_2 by a unit we can assume that $w = \pi^{-r}(-av_1 + v_2)$, with $r < 0$. The matrix giving the action of α in the basis $\{v_1, w\}$ is

$$\rho(\alpha) = \begin{pmatrix} -a & \pi^{-r}(\xi(\alpha^2) - a^2) \\ \pi^r & a \end{pmatrix}.$$

The computation for the action of β is similar.

If ρ is reducible (as a representation in $\mathrm{GL}_2(\overline{\mathbb{Q}_p})$), take an eigenvector in T, and extend it to a basis of T. Then the representation becomes (up to twist)

$$\rho \simeq \begin{pmatrix} \phi & * \\ 0 & 1 \end{pmatrix}.$$

If ϕ is trivial, then $*$ is an additive character, and we are in the first case. Otherwise, if ρ is principal series, it is equivalent (modulo $\mathrm{GL}_2(L)$) to $\left(\begin{smallmatrix} \phi & 0 \\ 0 & 1 \end{smallmatrix}\right)$, hence is of the form $\left(\begin{smallmatrix} \phi & u(\phi-1) \\ 0 & 1 \end{smallmatrix}\right)$. Since we want our representation to have integral coefficients we get the stated result. Finally, in the Steinberg case, our representation is $\mathrm{GL}_2(L)$-equivalent to $\left(\begin{smallmatrix} \chi & \mu \\ 0 & 1 \end{smallmatrix}\right)$. An easy computation shows it lies in our list. □

Remark 2.4. In the Principal Series case, if we take $r = 0$ we get $\rho \simeq \left(\begin{smallmatrix} \phi & \phi^{-1} \\ 0 & 1 \end{smallmatrix}\right)$, which is equivalent to $\left(\begin{smallmatrix} \phi & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We will consider this last class representative .

Although the possible reductions from types of $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$-equivalent representations to types of representations with coefficients in $\mathrm{GL}_2(\overline{\mathbb{F}_p})$ is well known to experts and most of the claims are in [2], the change of types are not explicitly described in that article, so we just give a short self contained description.

Recall the condition for a character to lose ramification:

Lemma 2.5. *Let $\xi\colon G_\ell \to \overline{\mathbb{Q}_p}^\times$ be a character and $\overline{\xi}$ its mod p reduction. If $\mathrm{Ker}(\xi|_{I_\ell}) \subsetneq \mathrm{Ker}(\overline{\xi}|_{I_\ell})$ then $\ell \equiv 1 \pmod p$.*

Remark 2.6. If $g \in I_\ell$ satisfies that $\xi(g) \neq 1$ and $\overline{\xi}(g) = 1$ then $\xi(g)^{\ell-1} = 1$.

Proposition 2.7. *Let ρ be as above. Then we have the following types of reduction*:

- *If ρ is Principal Series, then $\overline{\rho}$ is Principal Series or Steinberg, and the latter occurs only when $\ell \equiv 1 \pmod p$.*
- *If ρ is Steinberg, then $\overline{\rho}$ is Steinberg or Principal Series, and the latter occurs only when $\overline{\rho}$ is unramified.*
- *If ρ is Induced, then $\overline{\rho}$ is Induced, Steinberg or an unramified Principal Series. For the last two cases we must have $\ell \equiv -1 \pmod p$.*

Proof. If ρ is reducible, its reduction cannot be irreducible, which already excludes the case of a Principal Series or a Steinberg reducing to an Induced one. Besides this trivial observation, we study each case in detail.

• ρ *Principal Series:* in this case $\rho \simeq \left(\begin{smallmatrix}\phi & \lambda(\phi-1)\\ 0 & 1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & \phi\\ 0 & 1\end{smallmatrix}\right)$. If $\tilde{\rho} \simeq \left(\begin{smallmatrix}\phi & \lambda(\phi-1)\\ 0 & 1\end{smallmatrix}\right)$, the uniqueness of the semisimplification of the reduction implies that $\overline{\rho}^{ss} \simeq \left(\begin{smallmatrix}\overline{\phi} & 0\\ 0 & 1\end{smallmatrix}\right)$. If the reduction is of Steinberg type we need to have $\overline{\phi} = \chi$, so a character is losing ramification and this implies (by Lemma 2.5) that $\ell \equiv 1 \pmod{p}$.

If $\rho \simeq \left(\begin{smallmatrix}1 & \phi\\ 0 & 1\end{smallmatrix}\right)$ then it is unramified and so is its reduction, implying that it can only be Principal Series.

• ρ *Steinberg:* in this case $\rho \simeq \left(\begin{smallmatrix}\chi & \lambda u\\ 0 & 1\end{smallmatrix}\right)$ where $u \in \mathrm{H}^1(G_\ell, \mathbb{Z}_p(\chi))$ is the generator of the group. Its semisimplification is $\left(\begin{smallmatrix}\chi & 0\\ 0 & 1\end{smallmatrix}\right)$, which implies that if $\overline{\rho}$ is Principal Series then it is unramified.

• ρ *Induced:* in this case $\rho = \mathrm{Ind}_{G_M}^{G_{\mathbb{Q}_\ell}}(\xi)$, where $M/\mathbb{Q}_\ell$ is a quadratic extension and ξ is a character of G_M that does not descend to $G_{\mathbb{Q}_\ell}$. If the character $\overline{\xi}$ does not descend, then $\overline{\rho}$ is also irreducible hence Induced.

Suppose then that $\overline{\xi}$ does descend and, for a moment, that $\overline{\rho}$ ramifies (which implies, by assumption, that $\mathrm{Ad}^0\bar{\rho}$ ramifies). In this case the type of ρ changes when reducing. The semisimplification of the reduction we are considering is therefore

$$\overline{\rho}^{ss} \simeq \begin{pmatrix}\overline{\xi}\epsilon & 0\\ 0 & \overline{\xi}\end{pmatrix} = \overline{\xi} \otimes \begin{pmatrix}\epsilon & 0\\ 0 & 1\end{pmatrix},$$

where ϵ is the quadratic character associated to $M/\mathbb{Q}_\ell$.

If $\overline{\rho}$ is Principal Series, then ϵ has to be ramified, as we are assuming that $\mathrm{Ad}^0\bar{\rho}$ is ramified at ℓ, so $M/\mathbb{Q}_\ell$ is ramified. We claim (and will prove in the next lemma) that this case cannot happen, i.e., if $M/\mathbb{Q}_\ell$ is ramified, any character $\xi\colon G_M \to \overline{\mathbb{Z}_p}^\times$ that does not extend to G_ℓ satisfies that its reduction does not extend to G_ℓ either. Then the only case left is when $\overline{\rho}$ is Steinberg. In this is case, by looking at the semisimplifications we see that $\epsilon = \chi$, which only happens when $M/\mathbb{Q}_\ell$ is unramified and $\ell = -1 \pmod{p}$.

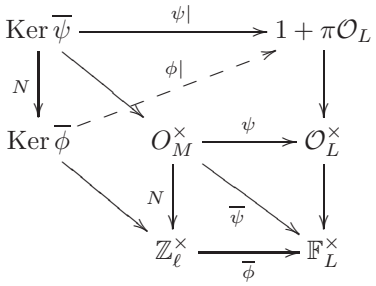
If $\overline{\rho}$ is unramified then ϵ has to be unramified as well, hence $M/\mathbb{Q}_\ell$ is an unramified extension. In this case, using the same argument as in Lemma 2.5, we conclude that $\ell^2 \equiv 1 \pmod{p}$. It is easy to prove that if $\ell \equiv 1 \pmod{p}$ then the character ξ extends to G_ℓ, therefore we necessarily have $\ell \equiv -1 \pmod{p}$. □

Lemma 2.8. *Let $M/\mathbb{Q}_\ell$ be a quadratic ramified extension and $\xi\colon G_M \to \overline{\mathbb{Z}_p}^\times$ be a character and $\overline{\xi}$ its reduction. If $\overline{\xi}$ extends to G_ℓ, then ξ does as well.*

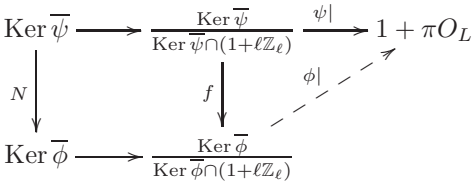
Proof. Let $L/\mathbb{Q}_p$ be a finite extension that contains the image of ξ, and π an uniformizer of this extension. Let $\alpha \in G_\ell$ be an element not in G_M and define $\xi^\alpha(x) = \xi(\alpha x \alpha^{-1})$. We know that ξ extends to G_ℓ if and only if $\xi = \xi^\alpha$.

Via local class field theory, the character ξ corresponds to a character ψ defined over $M^\times$ and ξ^α corresponds to $\psi^\alpha(x) = \psi(\alpha(x))$, so ξ extends to G_ℓ if and only if ψ factors through the norm map $N_{M/\mathbb{Q}_\ell} : M^\times \to \mathbb{Q}_\ell^\times$. Recall that by hypotheses $\psi = \psi^\alpha \pmod{\pi}$ and we want to prove that $\psi = \psi^\alpha$. Let $\overline{\phi}$ be the factorization of $\overline{\psi}$ through the norm map.

If we restrict to the inertia subgroup we have the following picture:



We are going to construct the dashed arrow $\phi|$ of the diagram above. Observe that $\psi|$ factors through $\operatorname{Ker}\overline{\psi}/(\operatorname{Ker}\overline{\psi}\cap(1+\ell\mathbb{Z}_\ell))\subseteq\mathbb{F}_\ell^\times$ (since $1+\pi\mathcal{O}_L$ is a pro-p-group), so we have



where the down arrow f is $f(x)=x^2$ (since $M/\mathbb{Q}_\ell$ is ramified). So we can define the dashed arrow $\phi|$ as $\phi|(x)=\sqrt{\psi|(x)}$ where $\sqrt{\ }\colon 1+\pi\mathcal{O}_L\to 1+\pi\mathcal{O}_L$ is the morphism that assigns to every $x\in 1+\pi\mathcal{O}_L$ its square root in $1+\pi\mathcal{O}_L$ (which exists and is unique by Hensel's lemma). This makes the diagram commutative and proves that ϕ can be extended in $\operatorname{Ker}\overline{\phi}$.

To prove that ψ factors through the norm map, define $\iota(x)=\psi^\alpha\psi^{-1}$. We know that $\iota\colon\mathcal{O}_M^\times\to 1+\pi\mathcal{O}_L$ and that $\iota(\operatorname{Ker}\overline{\xi})=1$. Then it factors through $\overline{\iota}\colon\mathcal{O}_M^\times/\operatorname{Ker}\overline{\psi}\to 1+\pi\mathcal{O}_L$, but $\mathcal{O}_M^\times/\operatorname{Ker}\overline{\psi}\subseteq\mathbb{F}_L^\times$ and the only element of order p^n-1 inside $1+\pi\mathcal{O}_L$ is 1, so ι must be trivial and therefore $\psi=\psi^\alpha$ when restricted to $\mathcal{O}_M^\times$. To deduce that $\psi=\psi^\alpha$ from this, we need to check it for the uniformizer, which is $\sqrt{\delta\ell}$ with δ equal to 1 or to a non-square in $\mathbb{Q}_\ell$. But

$$\psi^\alpha(\sqrt{\delta\ell})=\psi(\alpha(\sqrt{\delta\ell}))=\psi(-\sqrt{\delta\ell})=\psi(-1)\,\psi(\sqrt{\delta\ell})=\psi(\sqrt{\delta\ell}),$$

where the last equality follows from $\psi(-1)=\phi(N(-1))=\phi(1)=1$, because $-1\in\mathcal{O}_M^\times$. Then ξ extends to G_ℓ. □

Remark 2.9. Since we are only considering representations with unramified coefficient field, and $p\geq 5$, this rules out most change of type cases while reducing.

Proposition 2.10. *Let $p\geq 5$ and let $\rho\colon G_\ell\to\mathrm{GL}_2(W(\mathbb{F}))$ be a continuous representation.*

- *If ρ has type a ramified Principal Series, then $\overline{\rho}^{ss}$ is ramified.*
- *If ρ has type an Induced representation, then $\overline{\rho}^{ss}$ is ramified.*

Proof. For the first case, assume that $\overline{\rho}^{ss}$ is unramified, and ρ is Principal Series with character ϕ. Then $\overline{\phi}|_{I_\ell} = 1$ and Remark 2.6 implies that $\ell \equiv 1 \pmod{p}$ and $\phi(\tau)$ has order a power of p. Therefore the eigenvalues of $\rho(\tau)$ generate a totally ramified extension of $\mathbb{Q}_p$ of degree at least $p-1$, which is clearly impossible as they also have to satisfy a polynomial of degree 2 over some unramified extension of $\mathbb{Q}_p$ and $p > 3$.

For the second case, assume that $\overline{\rho}^{ss}$ is unramified and ρ is induced with character ξ. Then necessarily $\overline{\xi} = \overline{\xi^\sigma}$, implying that the character $\psi = \xi/\xi^\sigma$ loses all of its ramification when reduced. Again Remark 2.6 implies that $\psi(\tau)$ has order a power of p implying that it generates a totally ramified extension of degree at least $p-1 > 2$. But $\psi(\tau)$ is the quotient of the eigenvalues of $\rho(\tau)$, so it lies in an extension of degree 2 of some unramified extension of $\mathbb{Q}_p$ which is absurd. □

3. Local cohomological dimensions

To apply Ramakrishna's method in our situation, we need to compute $d_i = \dim \mathrm{H}^i(G_\ell, \mathrm{Ad}^0\bar{\rho})$ for $i = 1, 2$. For each mod p representation type we choose a basis of the underlying space and compute d_0 and d_0^* (where $d_i^* = \dim \mathrm{H}^i(G_\ell, (\mathrm{Ad}^0\bar{\rho})^*)$). By local Tate duality, $d_2 = d_0^*$, and then we can derive d_1 from the local Euler–Poincaré characteristic (which is zero).

Ramified Principal Series case: $\overline{\rho} = \left(\begin{smallmatrix} \phi & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with ϕ a ramified multiplicative character. It easily follows that $\mathrm{Ad}^0\bar{\rho} \simeq \mathbb{F} \oplus \mathbb{F}(\phi) \oplus \mathbb{F}(\phi^{-1})$. As ϕ is ramified, $\mathbb{F}(\phi)$ (resp. $\mathbb{F}(\phi^{-1})$) is not isomorphic to $\mathbb{F}$ nor $\mathbb{F}(\chi)$. So we have two cases:

(1) $\ell \equiv 1 \pmod{p}$ then $d_0 = 1$, $d_2 = 1$ and therefore $d_1 = 2$.

(2) $\ell \not\equiv 1 \pmod{p}$ then $d_0 = 1$, $d_2 = 0$ and therefore $d_1 = 1$.

The Steinberg case: taking $\{e_{01}, e_{10}, e_{00} - e_{11}\}$ as a basis for the space of trace zero matrices and explicitly computing the action of $\mathrm{Ad}^0\bar{\rho}$ on them, we obtain the following values for d_i:

(1) If $\ell \equiv 1 \pmod{p}$ then $d_0 = 1$, $d_2 = 1$ and therefore $d_1 = 2$.

(2) If $\ell \equiv -1 \pmod{p}$ then $d_0 = 0$, $d_2 = 1$ and therefore $d_1 = 1$.

(3) If $\ell \not\equiv \pm 1 \pmod{p}$ then $d_0 = 0$, $d_2 = 0$ and therefore $d_1 = 0$.

The Induced case: recall the following lemma (see [14], Lemma 4).

Lemma 3.1. *Let $M/\mathbb{Q}_\ell$ be a quadratic extension and $\overline{\rho}\colon G_\ell \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be twist-equivalent to $\mathrm{Ind}_{G_M}^{G_\ell}\,\xi$, with ξ a character of G_M which is not equal to its conjugate under the action of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$. Then $\mathrm{Ad}^0\bar{\rho} \simeq A_1 \oplus A_2$, with A_i an absolutely irreducible G_ℓ-module of dimension i and $\mathrm{H}^0(G_\ell, \mathrm{Ad}^0\bar{\rho}) = 0$. Moreover, $\mathrm{H}^2(G_\ell, \mathrm{Ad}^0\bar{\rho}) = 0$ unless $M/\mathbb{Q}_\ell$ is not ramified and $\ell \equiv -1 \pmod{p}$, in which case it is one dimensional.*

So for the Induced case we have two possibilities:

(1) If $\ell \equiv -1 \pmod{p}$ and $M/\mathbb{Q}_\ell$ is unramified then $d_0 = 0$, $d_2 = 1$ and therefore $d_1 = 1$.

(2) If $\ell \not\equiv -1 \pmod{p}$ or $M/\mathbb{Q}_\ell$ is ramified then $d_0 = 0$, $d_2 = 0$ and therefore $d_1 = 0$.

Unramified case: if $\overline{\rho}$ is unramified, we consider the following three cases according to the image of Frobenius:

(1) $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. In this case $\mathrm{Ad}^0\bar{\rho} \simeq \mathbb{F}^3$, thence we have two possibilities:

- $\ell \equiv 1 \pmod{p}$ then $d_0 = 3$, $d_2 = 3$ and therefore $d_1 = 6$.
- $\ell \not\equiv 1 \pmod{p}$ then $d_0 = 3$, $d_2 = 0$ and therefore $d_1 = 3$.

(2) $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\alpha \not\equiv 1 \pmod{p}$. We have that $\mathrm{Ad}^0\bar{\rho} \simeq \mathbb{F} \oplus \mathbb{F}(\phi) \oplus \mathbb{F}(\phi^{-1})$, with $\phi \neq 1$ and $\phi = \chi$ only if $\alpha \equiv \ell \pmod{p}$. We distinguish the cases:

- $\ell \equiv -1 \pmod{p}$ and $\ell \equiv \alpha, \alpha^{-1} \pmod{p}$ then $d_0 = 1$, $d_2 = 2$ and therefore $d_1 = 3$.
- $\ell \equiv -1 \pmod{p}$ and $\ell \not\equiv \alpha, \alpha^{-1} \pmod{p}$ then $d_0 = 1$, $d_2 = 0$ and therefore $d_1 = 1$.
- $\ell \not\equiv -1 \pmod{p}$ and $\ell \equiv \alpha, \alpha^{-1}$ or $1 \pmod{p}$ then $d_0 = 1$, $d_2 = 1$ and therefore $d_1 = 2$.
- $\ell \not\equiv -1 \pmod{p}$ and $\ell \not\equiv \alpha, \alpha^{-1}$ or $1 \pmod{p}$ then $d_0 = 1$, $d_2 = 0$ and therefore $d_1 = 1$.

(3) $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. An easy computation shows that:

- If $\ell \equiv 1 \pmod{p}$ then $d_0 = d_2 = 1$ and therefore $d_1 = 2$.
- If $\ell \not\equiv 1 \pmod{p}$ then $d_0 = 1$, $d_2 = 0$ and therefore $d_1 = 1$.

4. The sets C_ℓ

In order to apply Ramakrishna's method we need to define for each prime $\ell \in P$ a set C_ℓ of deformations of $\rho_n|_{G_\ell}$ (containing ρ_ℓ) and a subspace $N_\ell \subseteq \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ of dimension $d_1 - d_2$ such that $\rho_n|_{G_\ell}$ can be successively deformed to an element of C_ℓ by deforming from $W(\mathbb{F})/p^m$ to $W(\mathbb{F})/p^{m+1}$ with adjustments at each step made only by a multiple of an element $h \notin N_\ell$. Extra care must be taken to pick the set C_ℓ such that all its elements restricted to the inertia subgroup agree up to isomorphism with ρ_ℓ.

As mentioned in the introduction it is enough to do this for each possible pair of $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$ and $\mathrm{GL}_2(\overline{\mathbb{F}})$-isomorphism classes for ρ_ℓ and $\overline{\rho}$ respectively and construct the set C_ℓ containing ρ_ℓ in such a way that all its members are congruent modulo p^n. Note that all the deformations of C_ℓ must have coefficients in $W(\mathbb{F})$ (and not in a bigger ramified extension). If the image of ρ_ℓ is not irreducible (like in the Principal Series case) the classification representatives of Theorem 2.3 might live in a bigger extension than $W(\mathbb{F})$. This will force us to do some extra

calculations in the Principal Series case. In the Steinberg case this is not a problem since the representatives have coefficients in $\mathbb{Z}_p$ and a change of basis matrix can be found with coefficients in $W(\mathbb{F})$, while in the Induced case the definition of C_ℓ and N_ℓ is trivial (so it does not depend on the representative chosen).

The main difference with [14] is that in Case 4 (1) we can only construct the pair (C_ℓ, N_ℓ) for exponents higher than a certain n_0, so the inductive method of [14] works from n_0 on. We take a different approach for lifting ρ_n between p^n and p^{n_0} (see Section 5).

Remark 4.1. During the process of lifting and adjusting, we need to work with local deformations, as well as with the restriction to local Galois groups of representations modulo p^m. To avoid extra notation, we make some abuse of notation: we say a that representation ρ_m modulo p^m restricted to G_ℓ belongs to C_ℓ if there exists a deformation in C_ℓ congruent to it modulo p^m.

Remark 4.2. Whenever $d_2 = 0$ or $d_2 = d_1$ the problem is trivial. In the first case we need $\dim(N_\ell) = d_1 - d_2 = d_1$, so the only possible choice is $N_\ell = \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$. With this subspace we cannot adjust at all (as we have to take an element not in N_ℓ) but this is not a problem as $d_2 = 0$ implies that all the deformations of $\overline{\rho}$ are unobstructed and we can take C_ℓ as the set of all possible deformations of ρ_n to $W(\mathbb{F})$. We still have to check that these deformations agree when restricted to inertia. In the second case, we need $\dim(N_\ell) = d_1 - d_2 = 0$, hence $N_\ell = \{0\}$. This means that we have the whole group $\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ available to adjust at every step. Then we can take any set C_ℓ and the N_ℓ-preserving-C_ℓ condition will automatically hold. We take $C_\ell = \{\rho_\ell\}$.

Lemma 4.3. *If there exists a subspace $N_\ell \subset \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ of codimension d_2 which preserves reduction of elements in C_ℓ the second condition is automatically fulfilled, i.e., given a deformation ρ_m modulo p^m which is the reduction modulo p^{m-1} of an element in C_ℓ but is not the reduction of an element in C_ℓ modulo p^m, there exists $h' \notin N_\ell$ such that $h' \cdot \rho_m \in C_\ell$.*

Proof. By hypothesis $\rho_m \equiv \rho' \pmod{p^{m-1}}$, with $\rho' \in C_\ell$. Then there exists $h + h' \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$, with $h \in N_\ell$ and $h' \notin N_\ell$, such that $(h + h') \cdot \rho_m \equiv \rho' \pmod{p^m}$. But then $h' \cdot \rho_m \equiv -h \cdot \rho' \pmod{p^m}$, so the claim follows from the hypothesis on N_ℓ. □

Case 1: $\overline{\rho}$ is ramified Principal Series. When $\overline{\rho}$ is ramified Principal Series, ρ_ℓ can only be Principal Series. Nevertheless, the cohomology groups are different depending on whether $\ell \equiv 1 \pmod{p}$ or not. Recall that the representatives for the equivalence classes were (up to twist) $\rho_\ell \simeq \left(\begin{smallmatrix} \phi & \pi^r(\phi-1) \\ 0 & 1 \end{smallmatrix}\right)$ with $r \leq 0$ such that $\pi^r(\phi-1)$ lies in $\overline{\mathbb{Z}_p}$. If $r \neq 0$, $\pi \mid (\phi-1)$ and therefore its reduction is not a ramified Principal Series (the residual case $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ is unramified or Steinberg according to our classification). Then up to twist $\rho_\ell \simeq \left(\begin{smallmatrix} \phi & 0 \\ 0 & 1 \end{smallmatrix}\right)$ over $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$ which implies that $\rho_\ell \simeq \left(\begin{smallmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{smallmatrix}\right)$ over $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$ and we have the following cases:

(1) If $\ell \not\equiv 1 \mod p$, $d_0 = d_1 = 1$ and $d_2 = 0$. Then, as explained in Remark 4.2, $N_\ell = \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ and C_ℓ is the full set of deformations to characteristic zero. To

check that all the elements of C_ℓ agree up to isomorphism when restricted to I_ℓ, we need to describe the set C_ℓ. If we define a morphism $\eta : G_\ell \to G_\ell/I_\ell \simeq \hat{\mathbb{Z}} \to \mathbb{Z}/p\mathbb{Z}$, then the element

$$h(g) = \begin{pmatrix} \eta(g) & 0 \\ 0 & -\eta(g) \end{pmatrix}$$

generates $\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ and this implies that every lift is Principal Series, as the set $\lambda h \cdot \psi_s$, where ψ is the Teichmüller lift of $\overline{\rho}$ and λ is a scalar, exhausts all the possible reductions. In particular, the restriction to inertia is the same for all of them.

(2) If $\ell \equiv 1 \pmod p$ the picture is slightly different since $d_0 = 1$, $d_1 = 2$ and $d_2 = 1$ so N_ℓ is one dimensional. Observe that the isomorphism between ρ_ℓ and the representative of its $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$-equivalence class may not be realized over $W(\mathbb{F})$.

If the image of ψ_1 lies in $W(\mathbb{F})$, then the isomorphism is realized over $W(\mathbb{F})$ and the same element h defined above lies inside $\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$. We take $N_\ell = \langle h \rangle$, and $C_\ell = \left\{ \left(\begin{smallmatrix} \psi_1\gamma & 0 \\ 0 & \psi_2\gamma^{-1} \end{smallmatrix} \right) : \gamma \text{ unramified character} \right\}$. Clearly $\rho_\ell \in C_\ell$ and N_ℓ preserves reduction of elements of C_ℓ (which is enough by Lemma 4.3). Note that all the elements in C_ℓ have the same restriction to inertia.

If the image of ψ_1 does not lie in $W(\mathbb{F})$ then ρ_ℓ is not isomorphic to $\left(\begin{smallmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{smallmatrix} \right)$ over $W(\mathbb{F})$ and we cannot use the previous choice. Instead, we take a canonical form for ρ_ℓ over $W(\mathbb{F})$. Assume that $\psi_1(\sigma) = \alpha$ and $\psi_2(\sigma) = \beta$, then the matrix $C = \left(\begin{smallmatrix} -\beta & -\alpha \\ 1 & 1 \end{smallmatrix} \right)$ conjugates $\left(\begin{smallmatrix} \psi_1(\sigma_\ell) & 0 \\ 0 & \psi_2(\sigma_\ell) \end{smallmatrix} \right)$ into $\left(\begin{smallmatrix} 0 & -\alpha\beta \\ 1 & \alpha+\beta \end{smallmatrix} \right) \in \mathrm{GL}_2(W(\mathbb{F}))$. Therefore we can assume (applying a change of basis) that $\rho_\ell(\sigma) = \left(\begin{smallmatrix} 0 & -\alpha\beta \\ 1 & \alpha+\beta \end{smallmatrix} \right)$. Let $N_\ell = \langle (\alpha - \beta) C h C^{-1} \rangle$, where h is the element defined before, and let C_ℓ be the set of deformations to $W(\mathbb{F})$ of the form $C \left(\begin{smallmatrix} \psi_1\gamma & 0 \\ 0 & \psi_2\gamma^{-1} \end{smallmatrix} \right) C^{-1}$, with $\gamma \colon G_\ell \to \overline{\mathbb{Z}_p}$ an unramified character. The factor $\alpha - \beta$ forces the element generating N_ℓ to have coefficients in $W(\mathbb{F})$. It can be easily checked that whenever ρ_m is the reduction of some element in C_ℓ and $u \in N_\ell$ then $(1 + p^{m-1}u)\rho_m$ is again the reduction of an element of C_ℓ.

Case 2: $\overline{\rho}$ is Steinberg. If $\overline{\rho}$ is of Steinberg type then Proposition 2.7 and Proposition 2.10 imply that ρ_ℓ can only be Steinberg.

(1) If $\ell \not\equiv \pm 1 \pmod p$, $d_0 = d_1 = d_2 = 0$, so there is only one deformation at each p^n. We take $C_\ell = \{\rho_\ell\}$, which is the only deformation of $\overline{\rho}$ to $W(\mathbb{F})$.

(2) If $\ell \equiv -1 \pmod p$, $d_1 = d_2 = 1$ and $d_0 = 0$. As explained in Remark 4.2, $N_\ell = \{0\}$ and $C_\ell = \{\rho_\ell\}$.

(3) If $\ell \equiv 1 \pmod p$, we take the element $j \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ given by 0 at the wild inertia subgroup and by

$$j(\sigma) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad j(\tau) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Let $N_\ell = \langle j \rangle$ and C_ℓ the set of lifts ρ satisfying

$$\rho(\sigma) = \begin{pmatrix} \ell & * \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\tau) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

This set is formed by deformations which are isomorphic when restricted to inertia, and N_ℓ preserves its reductions.

Case 3: $\overline{\rho}$ is Induced. If $\overline{\rho}$ is Induced then the only possibility for ρ_ℓ is also being of Induced type.

(1) If $\ell \equiv -1 \pmod{p}$ and $M/\mathbb{Q}_\ell$ is unramified, $d_0 = 0$, $d_1 = d_2 = 1$ so Remark 4.2 applies.

(2) If $\ell \not\equiv -1 \pmod{p}$ or $M/\mathbb{Q}_\ell$ is ramified, $d_0 = d_1 = d_2 = 0$, so there is only one lift at every step (the reduction of ρ_ℓ). We take $C_\ell = \{\rho_\ell\}$.

Case 4: $\overline{\rho}$ is unramified. If ρ_ℓ is also unramified, we simply take C_ℓ to be all the unramified lifts of $\overline{\rho}$ and N_ℓ the unramified part of $\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$. It can be easily checked that N_ℓ has the correct dimension.

It remains to define the sets C_ℓ for the primes at which ρ_ℓ ramifies and $\overline{\rho}$ does not. By Proposition 2.10 this can only happen when ρ_ℓ is Steinberg, i.e., $\rho_\ell = \left(\begin{smallmatrix}\chi & *\\ 0 & 1\end{smallmatrix}\right)$, with $*|_{I_\ell} \neq 0 \pmod{p^n}$. The sets C_ℓ depend on the image of σ. Recall that the eigenvalues of $\overline{\rho}(\sigma)$ are 1 and ℓ.

(1) If $\overline{\rho}(\sigma) = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$, $\ell \equiv 1 \pmod{p}$ so $d_1 = 6$ and $d_2 = 3$. Therefore N_ℓ has dimension 3. In the previous cases, we have built sets C_ℓ of deformations of ρ_n that depend on $d_2 - d_1$ parameters, which in this case does not seem to be possible. However, as pointed to us by Ravi Ramakrishna, one can construct elements which are not cohomologically trivial for the residual representation, but give isomorphic lifts modulo big powers of p that depend on the lift ρ_ℓ, as in Section 4 of [7]. Let C_ℓ be the set of deformations of ρ_n satisfying

$$\rho(\sigma) = \begin{pmatrix}\ell & *\\ 0 & 1\end{pmatrix} \quad \text{and} \quad \rho(\tau) = \begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}.$$

This set is preserved by the elements $u_1, u_2 \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ defined by

$$u_1(\sigma) = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \quad u_1(\tau) = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},$$

and

$$u_2(\sigma) = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \quad u_2(\tau) = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}.$$

We still need one extra element of $\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ preserving C_ℓ. Recall that ρ_ℓ satisfies

$$\rho_\ell(\sigma) = \begin{pmatrix}\ell & x\\ 0 & 1\end{pmatrix} \quad \text{and} \quad \rho_\ell(\tau) = \begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix},$$

with $y \neq 0$. Let $n_0 = \min(v(x), v(y), v(\ell - 1))$.

Lemma 4.4. *There exists an element $\nu \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ not in $\langle u_1, u_2\rangle$ such that whenever ρ_m is the reduction modulo p^m of some element in C_ℓ, with $m \geq n_0 + 1$, then $(1 + p^{m-1}\nu)\rho_m$ is the same deformation as ρ_m.*

Proof. The proof is divided into several cases.

We first define $g_1, g_2, g_3 \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ as

$$g_1(\sigma) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad g_1(\tau) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$
$$g_2(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g_2(\tau) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$
$$g_3(\sigma) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad g_3(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We now enumerate a list of cases (depending on the valuations of x, y and $\ell-1$) and for each of them specify an element ν and a matrix C congruent to the identity modulo p such that $C^{-1}\rho_m C = (1+p^{m-1}\nu)\rho_m$. Write $C = \left(\begin{smallmatrix} 1+p\alpha & p\beta \\ p\gamma & 1+p\delta \end{smallmatrix}\right)$. In each case we will give the values of α, β, γ and δ and leave to the reader to check that $C^{-1}\rho_m C = (1+p^{m-1}\nu)\rho_m$ in each of them.

- If $v(y) < v(x)$ and $v(y) < v(\ell-1)$: take $\nu = g_3$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma y = p^{m-2} \pmod{p^{m-1}}$ and $\gamma x = \gamma(\ell-1) = 0 \pmod{p^{m-1}}$.
- If $v(x) < v(y)$ and $v(x) < v(\ell-1)$: take $\nu = g_2$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma x = p^{m-2} \pmod{p^{m-1}}$ and $\gamma y = \gamma(\ell-1) = 0 \pmod{p^{m-1}}$.
- If $v(\ell-1) < v(x)$ and $v(\ell-1) < v(x)$: take $\nu = g_1$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma(\ell-1) = -p^{m-2} \pmod{p^{m-1}}$ and $\gamma x = \gamma y = 0 \pmod{p^{m-1}}$.
- If $v(y) = v(\ell-1)$ and $v(y) < v(x)$: then $y = \lambda(\ell-1)$. Take $\nu = g_1 - \lambda g_3$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma(\ell-1) = -p^{m-1} \pmod{p^{m-1}}$ and $\gamma x = 0 \pmod{p^{m-1}}$.
- If $v(y) = v(x)$ and $v(y) < v(\ell-1)$: then $y = \lambda x$. Take $\nu = g_2 + \lambda g_3$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma x = p^{m-2} \pmod{p^{m-1}}$ and $\gamma(\ell-1) = 0 \pmod{p^{m-1}}$.
- If $v(x) = v(\ell-1)$ and $v(x) < v(y)$: then $x = \lambda(\ell-1)$. Take $\nu = g_1 - \lambda g_2$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma(\ell-1) = -p^{m-2} \pmod{p^{m-1}}$ and $\gamma y = 0 \pmod{p^{m-1}}$.
- If $v(x) = v(\ell-1) = v(y)$: then $x = \lambda_1(\ell-1)$ and $y = \lambda_2(\ell-1)$. Take $\nu = g_1 - \lambda_1 g_2 - \lambda_2 g_3$ and C satisfying $\alpha = \delta$, $\beta = 0$, $\gamma(\ell-1) = -p^{m-2} \pmod{p^{m-1}}$. □

Let $N_\ell = \langle u_1, u_2, \nu \rangle$, for the element ν of Lemma 4.4. It preserves the set C_ℓ for all exponents $m > n_0$. For smaller exponents, the reduction of ρ_ℓ modulo p^m is trivial, and as the trivial deformation does not have any equivalent deformation other than itself, it is impossible to find an element ν as before in those cases.

(2) If $\overline{\rho}(\sigma_\ell) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$, with $\alpha \neq 1$, necessarily $\ell \equiv \alpha \pmod{p}$ so $d_1 = 3$ and $d_2 = 2$ if $\ell \equiv -1 \pmod{p}$ and $d_1 = 2$ and $d_2 = 1$ otherwise. In both cases, let $u \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ be given by $u(\sigma_\ell) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $u(\tau_\ell) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, and take $N_\ell = \langle u \rangle$.

Define the set C_ℓ of deformations ρ that satisfy

$$\rho(\sigma_\ell) = \rho_\ell(\sigma_\ell) \quad \text{and} \quad \rho(\tau_\ell) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Clearly N_ℓ preserves C_ℓ.

(3) If $\overline{\rho}(\sigma_\ell) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, necessarily $\ell \equiv 1 \pmod{p}$, so $d_1 = 2$ and $d_2 = 1$. Let $u \in \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ be given by $u(\sigma_\ell) = 0$ and $u(\tau_\ell) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and take $N_\ell = \langle u \rangle$. This subspace preserves the set C_ℓ of deformations ρ satisfying

$$\rho(\sigma_\ell) = \rho_\ell(\sigma_\ell) \quad \text{and} \quad \rho(\tau_\ell) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Remark 4.5. If we allow ramification in the coefficient field then the cases ruled out by Proposition 2.10 may happen. Most of them correspond to cases like the first unramified case, where a trick like in [7] needs to be used. It is worth pointing out that in such cases we can construct the corresponding sets C_ℓ and subspaces N_ℓ but the global arguments below do not adapt well to that situation. See Remark 5.10.

4.1. The case $\ell = p$

In this case we will pick C_p exactly as in [14] (*local at p considerations*), with the observation that in the supersingular case, it follows from the work done in [12] that the lifts picked have the same Hodge–Tate weights as ρ_p (which lie in the interval $[0, p-1]$) and are crystalline. Note that in each case considered by Ramakrishna, ρ_p is always trivially contained in C_p.

5. Auxiliary primes

The sets Q_1 and Q_2 mentioned in the introduction consist of *nice primes* with some extra conditions. Recall that nice primes (as introduced in [10]) are primes $q \not\equiv \pm 1 \pmod{p}$ such that $\overline{\rho}$ is not ramified at q and $\overline{\rho}(\sigma)$ has different eigenvalues of ratio q, i.e., $\bar{\rho}(\sigma) = \left(\begin{smallmatrix} qx & 0 \\ 0 & x \end{smallmatrix}\right)$ and $\bar{\rho}(\tau) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For these primes the cohomological dimensions are $\dim \mathrm{H}^0(G_q, \mathrm{Ad}^0\bar{\rho}) = 1$, $\dim \mathrm{H}^1(G_q, \mathrm{Ad}^0\bar{\rho}) = 2$ and $\dim \mathrm{H}^2(G_q, \mathrm{Ad}^0\bar{\rho}) = 1$. The set C_q consists of deformations ρ such that

$$\rho(\tau) = \begin{pmatrix} 1 & px \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\sigma) = \begin{pmatrix} q & py \\ 0 & 1 \end{pmatrix}. \tag{5.1}$$

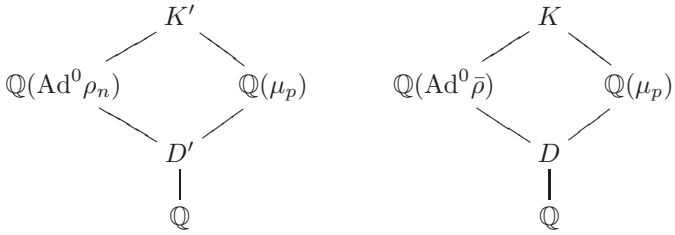
These two conditions define a tamely ramified deformation of $\overline{\rho}$. Clearly the set C_q is preserved by a subspace $N_q \subseteq \mathrm{H}^1(G_q, \mathrm{Ad}^0\bar{\rho})$ of codimension 1 given by $j(\sigma) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $j(\tau) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

There are two main goals we want to achieve in this section. Firstly, we would like to prove that auxiliary primes do exist for representations with coefficients in $W(\mathbb{F})/p^n$. In particular we need to check that there are primes q such that $\rho_n|_{G_q}$ sends a Frobenius and a generator of the tame inertia to the matrices defined in (5.1) modulo p^n.

Secondly, we need to reprove the properties of the auxiliary primes we are going to use in our context, although they look similar to the arguments in [14].

5.1. Existence of auxiliary primes modulo p^n

We claim that there are infinitely many nice primes. Following [13] and [14], let μ_p be a primitive p-th root of unity, $D = \mathbb{Q}(\mathrm{Ad}^0\bar{\rho}) \cap \mathbb{Q}(\mu_p)$, $K = \mathbb{Q}(\mathrm{Ad}^0\bar{\rho})\mathbb{Q}(\mu_p)$, $D' = \mathbb{Q}(\mathrm{Ad}^0\rho_n) \cap \mathbb{Q}(\mu_p)$ and $K' = \mathbb{Q}(\mathrm{Ad}^0\rho_n)\mathbb{Q}(\mu_p)$, which fit in the following diagram:



Via the Artin map, the properties of a nice prime translate into the following:

- $q \not\equiv \pm 1 \pmod{p}$ is equivalent to Frob_q not being the identity nor complex conjugation in $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$,
- q being an auxiliary prime is equivalent to being unramified in $\mathbb{Q}(\mathrm{Ad}^0\rho_n)$, $q \not\equiv \pm 1 \pmod{p}$ and Frob_q lies in the conjugacy class of an element $\overline{M} \in \mathrm{Im}(\mathrm{Ad}^0\rho_n)$, where M is a diagonal matrix with elements of ratio q in the diagonal.

Therefore, if we prove that there is an element $\alpha \in \mathrm{Gal}(K'/\mathbb{Q})$ such that $\alpha|_{\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})} = t \neq \pm 1$ and $\alpha|_{\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\rho_n)/\mathbb{Q})} = \overline{M}$ where M is diagonal with elements of ratio t in its diagonal, then Chebotarev's theorem implies the result.

Proposition 5.1. *There exists* $c = a \times b \in \mathrm{Gal}(K'/\mathbb{Q}) \subseteq \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\rho_n)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ *such that* a *comes from an element* $M \in \mathrm{Im}(\rho_n) \simeq \mathrm{Gal}(\mathbb{Q}(\rho_n)/\mathbb{Q})$ *which has different eigenvalues with ratio* $b \in \mathbb{F}_p^\times \simeq \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, $b \neq \pm 1$.

The proof mimics the arguments given in [13] for finding such elements with a slightly modification on their proof of the so-called Theorem 2. Recall the following result (Lemma 3, IV-23 in[1] [18]).

Lemma 5.2. *Let* $p \geq 5$ *and let* $\mathbb{F}$ *be a finite field of characteristic* p. *Let* $H \subseteq \mathrm{GL}_2(W(\mathbb{F}))$ *be a closed subgroup and let* $\overline{H}$ *be its projection to* $\mathrm{GL}_2(\mathbb{F})$. *If* $\mathrm{SL}_2(\mathbb{F}) \subseteq \overline{H}$ *then* $\mathrm{SL}_2(W(\mathbb{F})) \subseteq H$.

This has the following easy consequences:

Corollary 5.3. *If* $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho})$ *then* $\mathrm{SL}_2(W(\mathbb{F})/p^n) \subseteq \mathrm{Im}(\rho_n)$.

Proof. Denote by $\pi\colon W(\mathbb{F}) \to W(\mathbb{F})/p^n$ the projection, then this follows applying Lemma 5.2 with $H = \pi^{-1}(\mathrm{Im}(\rho_n)) \subseteq W(\mathbb{F})$, which is closed as $G_\mathbb{Q}$ is compact. □

[1]Actually, Lemma 3 is stated and proved in [18] for $\mathbb{F} = \mathbb{F}_p$ but the same proof holds for an arbitrary finite field of characteristic p.

The following lemma gives the existence of the element c.

Lemma 5.4. *Let D' be the field defined before. If $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho})$, then $[D' : \mathbb{Q}] \leq 2$, and moreover $\mathrm{PSL}_2(\mathbb{F}) \subseteq \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/D')$.*

Proof. Observe that $[\mathbb{Q}(\mathrm{Ad}^0\rho_n) : \mathbb{Q}(\mathrm{Ad}^0\bar{\rho})] = p^*$ which is coprime with $[\mathbb{Q}(\mu_p) : \mathbb{Q}]$. This implies that $D' = \mathbb{Q}(\mathrm{Ad}^0\rho_n) \cap \mathbb{Q}(\mu_p) = \mathbb{Q}(\mathrm{Ad}^0\bar{\rho}) \cap \mathbb{Q}(\mu_p)$. Now both $\mathrm{PSL}_2(\mathbb{F}) \subseteq \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/D')$ and $[\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}) \cap \mathbb{Q}(\mu_p) : \mathbb{Q}] = 1$ or 2 follow from Lemma 18 of [13], as we have proved that the field D' is the same as the field D of that lemma. □

Proof of Proposition 5.1. If $\mathbb{F} \neq \mathbb{F}_5$, let $x \in \mathbb{F}^\times$ be any element such that $x^2 \in \mathbb{F}_p^\times$ and $x^2 \neq \pm 1$ (observe that this exists for any $\mathbb{F} \neq \mathbb{F}_5$). Let $\tilde{x} \in W(\mathbb{F})/p^n$ be a lift of x, $b \in \{1, \ldots, p-1\} \subseteq W(\mathbb{F})/p^n$ be congruent to x^2 modulo p and $M = \left(\begin{smallmatrix} \tilde{x} & 0 \\ 0 & \tilde{x}^{-1} \end{smallmatrix}\right) \in \mathrm{SL}_2(W(\mathbb{F})/p^n) \subseteq \mathrm{Im}(\rho_n)$. Then $c = (\overline{M}, b) \in \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\rho_n)/D') \times \mathrm{Gal}(\mathbb{Q}(\mu_p)/D')$ is such an element.

For $p = 5$, we imposed $\overline{\rho}$ to be surjective. We have two possible scenarios:

• If $D' = \mathbb{Q}$ then $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ and we can find the element c by taking a pair $(\overline{M}, b)$ where $M = \left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(W(\mathbb{F})/p^n) = \mathrm{Im}(\rho_n)$ and $b \equiv q \neq \pm 1 \pmod 5$.

• If $D' \neq \mathbb{Q}$ then $[D' : \mathbb{Q}] = 2$. Then $\mathrm{PSL}_2(\mathbb{F}_5) \subseteq \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/D')$, from Lemma 5.1. As $\mathrm{PSL}_2(\mathbb{F}_5) \subset \mathrm{PGL}_2(\mathbb{F}_5)$ with index 2, $\mathrm{PSL}_2(\mathbb{F}_5) = \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/D')$. On the other hand, $\mathrm{Gal}(\mathbb{Q}(\mu_p)/D') \subseteq \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \simeq \mathbb{F}_5^\times$ with index 2, so $\mathrm{Gal}(\mathbb{Q}(\mu_p)/D') \simeq \{\pm 1\}$. With this information we know that the pair $(\overline{M}, b)$, for $M = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $b = 3$, defines an element in $\mathrm{Gal}(K'/\mathbb{Q})$, as both elements coincide when restricted to D' (both act non trivially). □

Remark 5.5. The element c constructed in Proposition 5.1 is not the same as the one in [13]. In fact they live in different Galois groups, the first one lying in $\mathrm{Gal}(K'/\mathbb{Q})$ and the second one in $\mathrm{Gal}(K/\mathbb{Q})$. However, it is true that the projection of the element we constructed through the map $\mathrm{Gal}(K'/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ is an element like the one defined by Ramakrishna. In particular, both elements act in the same way on $\mathrm{Ad}^0\bar{\rho}$ (as the action of our c is through this projection). To avoid confusion we denote the projection by $\tilde{c}$.

5.2. Properties of auxiliary primes

The auxiliary primes must also fulfill some requirements like the ones in Fact 16 and Lemma 14 of [14]. Concretely, for different non-zero elements $f \in \mathrm{H}^1(G_P, \mathrm{Ad}^0\bar{\rho})$ and $g \in \mathrm{H}^1(G_P, (\mathrm{Ad}^0\bar{\rho})^*)$, the auxiliary prime q should satisfy $f|_{G_q} = 0$ or $f|_{G_q} \notin N_q$ and $g|_{G_q} \neq 0$ at the same time.

If $f \in \mathrm{H}^1(G_P, \mathrm{Ad}^0\bar{\rho})$, then $f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))}$ is a homomorphism, so we can associate an extension $\widetilde{L_f}/\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})$ fixed by its kernel. Also let $L_f = \widetilde{L_f}K = \widetilde{L_f}(\mu_p)$. Analogously, for $g \in \mathrm{H}^1(G_P, (\mathrm{Ad}^0\bar{\rho})^*)$ we define $M_g/\mathbb{Q}((\mathrm{Ad}^0\bar{\rho})^*)$ as the fixed field by the kernel of $g|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}((\mathrm{Ad}^0\bar{\rho})^*))}$. Notice that we can obtain information

about $f|_{G_q}$ or $g|_{G_q}$ by looking at the conjugacy class of Frob_q in $\mathrm{Gal}(L_f/\mathbb{Q})$ or $\mathrm{Gal}(M_g/\mathbb{Q})$.

Let $f_1, \dots, f_{r_1}$ and $g_1, \dots, g_{r_2}$ be bases for $\mathrm{H}^1(G_P, \mathrm{Ad}^0\bar{\rho})$ and $\mathrm{H}^1(G_P, (\mathrm{Ad}^0\bar{\rho})^*)$ respectively. Define L to be the composition of the fields L_{f_i}, M the composition of the M_{g_j}, and $F = LM$. The following lemma is a summary of results about these extensions from [13].

Lemma 5.6. *Let f_i and g_j as above.*

(1) *For every f_i, we have $\mathrm{Gal}(L_{f_i}/K) \simeq \mathrm{Ad}^0\bar{\rho}$ as $G_{\mathbb{Q}}$-modules, and for every g_j, we have $\mathrm{Gal}(M_{g_j}/K) \simeq (\mathrm{Ad}^0\bar{\rho})^*$.*

(2) $\mathrm{Gal}(L/K) \simeq \prod \mathrm{Gal}(L_{f_i}/K) \simeq (\mathrm{Ad}^0\bar{\rho})^{r_1}$ *and* $\mathrm{Gal}(M/K) \simeq \prod \mathrm{Gal}(M_{g_j}/K) \simeq ((\mathrm{Ad}^0\bar{\rho})^*)^{r_2}$. *Also $M \cap L = K$ so $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$.*

(3) *The exact sequences*

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1,$$

and

$$1 \longrightarrow \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(M/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1,$$

both split, hence $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathrm{Gal}(F/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$.

Proof. The first claim is Lemma 9, the second is Lemma 11 and the last one is Lemma 13 of [13] with two remarks:

– In [13] these results are proved for the representation $\widetilde{\mathrm{Ad}}^0\bar{\rho}$, which is the descent of $\mathrm{Ad}^0\bar{\rho}$ to its minimal field of definition. As we are assuming that $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho})$, we have that $\mathrm{Ad}^0\bar{\rho}$ is already defined in its minimal field of definition, because of Lemma 17 of [13].

– In [13] these lemmas are proved for $P = S$ the set of ramification of $\mathrm{Ad}^0\bar{\rho}$, but the same proofs work for any $P \supseteq S$. □

Finally, we can read properties of $f|_{G_q} \in \mathrm{H}^1(G_q, \mathrm{Ad}^0\bar{\rho})$ from the class of Frob_q in $\mathrm{Gal}(L_f/\mathbb{Q}) \simeq \mathrm{Gal}(L_f/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$. Recall that the element $c \in \mathrm{Gal}(K'/\mathbb{Q})$ constructed in the previous section acts on $\mathrm{Ad}^0\bar{\rho}$ through the projection to $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/\mathbb{Q})$.

Proposition 5.7. *Let $q \in \mathbb{Q}$ be a prime, let $f \in \mathrm{H}^1(G_P, \mathrm{Ad}^0\bar{\rho})$ and let $g \in \mathrm{H}^1(G_P, (\mathrm{Ad}^0\bar{\rho})^*)$.*

(1) *If Frob_q lies in the conjugacy class of $0 \rtimes \tilde{c} \in \mathrm{Gal}(L_f/\mathbb{Q})$ then $f|_{G_q} = 0$. The same holds for g in $\mathrm{Gal}(M_g/\mathbb{Q})$.*

(2) *There are nontrivial elements $\alpha \in \mathrm{Ad}^0\bar{\rho}$ on which c acts trivially and if Frob_q lies in the conjugacy class of $\alpha \rtimes \tilde{c} \in \mathrm{Gal}(L_f/\mathbb{Q})$ then $f|_{G_q} \notin N_q$.*

(3) *There are nontrivial elements $\beta \in (\mathrm{Ad}^0\bar{\rho})^*$ on which c acts trivially and if Frob_q lies in the conjugacy class of $\beta \rtimes \tilde{c} \in \mathrm{Gal}(M_g/\mathbb{Q})$ then $g|_{G_q} \neq 0$.*

Proof. See Lemmas 14, 15 and 16, and Corollaries 1 and 2 of [13], noting that in our setting $\mathrm{Ad}^0\bar{\rho} = \widetilde{\mathrm{Ad}}^0\bar{\rho}$, so the proof of the existence of α and β is almost trivial. □

Corollary 5.8. *There exists primes q such that $\overline{\rho}(\mathrm{Frob}_q)$ has different eigenvalues of ratio q and such that for the basis elements any of the following conditions can be achieved: $f_i|_{G_q} = 0$ or $f_i|_{G_q} \notin N_q$ and $g_j|_{G_q} = 0$ or $g_j|_{G_q} \neq 0$.*

Proof. Pick an element

$$\Omega = \omega \rtimes \tilde{c} \in \mathrm{Gal}(F/\mathbb{Q}) \simeq \Big(\prod_{i=1}^{r_1} \mathrm{Gal}(L_{f_i}/\mathbb{Q}) \times \prod_{j=1}^{r_2} \mathrm{Gal}(M_{g_j}/\mathbb{Q})\Big) \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

where ω has coordinates 0 or α whether we want $f_i|_{G_q}$ to be 0 or not in N_q in the first product and 0 or β whether we want $g_j|_{G_q}$ to be 0 or not 0 in the second one. Then any q such that Frob_q lies in the conjugacy class of Ω works. □

We need the same to hold for ρ_n, i.e., the auxiliary primes q must satisfy the same conditions and $\rho_n(\mathrm{Frob}_q)$ must have different eigenvalues of ratio q. Proposition 5.1 implies that any q whose Frobenius element lies in the conjugacy class of c satisfies this extra condition. Therefore, we only need to check that there is an element θ in $\mathrm{Gal}(K'F/\mathbb{Q})$ such that $\theta|_{K'} = c$ and $\theta|_F = \Omega$.

Observe that $\Omega|_K = \tilde{c} = c|_K$, a necessary condition. It is enough to prove that $K' \cap F = K$, as any pair of elements in $\mathrm{Gal}(K'/\mathbb{Q})$ and $\mathrm{Gal}(F/\mathbb{Q})$ that are equal when restricted to $K' \cap F$ define an element in $\mathrm{Gal}(K'F/\mathbb{Q})$.

Lemma 5.9. *$K' \cap F = K$.*

Proof. Let $\mathcal{H} = \mathrm{Gal}(K'/K) \subseteq \mathrm{PGL}_2(W(\mathbb{F})/p^n)$ and $\pi_1 : \mathrm{PGL}_2(W(\mathbb{F})/p^n) \to \mathrm{PGL}_2(\mathbb{F})$. Observe that H consists of the classes of matrices in $\mathrm{Im}(\rho_n)$ which are trivial in $\mathrm{PGL}_2(\mathbb{F})$, i.e., $\mathcal{H} = \mathrm{Im}(\mathrm{Ad}^0\rho_n) \cap \mathrm{Ker}(\pi_1)$.

Let $\mathrm{PSL}_2(W(\mathbb{F})/p^n)$ denote the image of $\mathrm{SL}_2(W(\mathbb{F})/p^n)$ in $\mathrm{PGL}_2(W(\mathbb{F})/p^n)$. By hypotheses $\mathrm{PSL}_2(W(\mathbb{F})/p^n) \subseteq \mathrm{Im}(\mathrm{Ad}^0\rho_n) \subseteq \mathrm{PGL}_2(W(\mathbb{F})/p^n)$, and therefore $\mathrm{PSL}_2(W(\mathbb{F})/p^n) \cap \mathrm{Ker}(\pi_1) \subseteq \mathcal{H} \subseteq \mathrm{Ker}(\pi_1)$. As $[\mathrm{PSL}_2(W(\mathbb{F})/p^n) : \mathrm{PGL}_2(W(\mathbb{F})/p^n)] = 2$ and $\mathrm{Ker}(\pi_1)$ is a p group, we have that $\mathcal{H} = \mathrm{Ker}(\pi_1)$.

Recall that $\mathrm{Gal}(F/K) \simeq (\mathrm{Ad}^0\bar{\rho})^r \times (\mathrm{Ad}^0\bar{\rho}^*)^s$ as $\mathbb{Z}[G_{\mathbb{Q}}]$-module and by Lemma 7 of [13], this is its decomposition as $\mathbb{Z}[G_{\mathbb{Q}}]$ simple modules. This implies that if $K' \cap F \neq K$ then $\mathrm{Ad}^0\bar{\rho}$ or $(\mathrm{Ad}^0\bar{\rho})^*$ appear as a quotient of $\mathrm{Gal}(K'/K)$.

Assume that $K' \cap F \neq K$ and that there is a surjective morphism $\varpi\colon \mathcal{H} \to \mathrm{Ad}^0\bar{\rho}$. Let $\pi_2\colon \mathrm{PGL}_2(W(\mathbb{F})/p^n) \to \mathrm{PGL}_2(W(\mathbb{F})/p^2)$ and let $\mathcal{N} = \ker(\pi_2) \subset \mathcal{H}$. We claim that $\varpi(\mathcal{N}) = 0$. Any matrix $\mathrm{Id} + p^2M \in \mathrm{GL}_2(W(\mathbb{F})/p^n)$ is the p-th power of some matrix $\mathrm{Id} + pN \in \mathrm{GL}_2(W(\mathbb{F})/p^n)$. Therefore, if $\mathrm{Id} + p^2M \in \mathcal{N}$ we have that

$$\varpi(\mathrm{Id} + p^2M) = \varpi((\mathrm{Id} + pN)^p) = p\,\varpi(\mathrm{Id} + pN) = 0.$$

This implies that ϖ factors through $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\rho_2)/K)$, where $\mathrm{Ad}^0\rho_2$ is the reduction mod p^2 of $\mathrm{Ad}^0\rho_n$. Since $\#\,\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\rho_2)/K) = \#(\mathrm{Im}(\mathrm{Ad}^0\rho_2) \cap \mathrm{Ker}(\pi_1)) \leq$

$(\#\mathbb{F})^3$ and $\#\mathrm{Ad}^0\bar{\rho} = (\#\mathbb{F})^3$ we necessarily have $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\rho_2)/\mathbb{Q}) = \mathrm{Gal}(L_f/\mathbb{Q})$ for some $f \in \mathrm{H}^1(G_\mathbb{Q}, \mathrm{Ad}^0\bar{\rho})$. But this cannot happen since it would imply that the image of $\mathrm{Ad}^0\rho_2$ splits, which is impossible as it contains $\mathrm{PSL}_2(W(\mathbb{F})/p^2)$ when $p \geq 7$ or $\mathrm{PGL}_2(W(\mathbb{F})/p^2)$ when $p = 5$.

The case where there is a surjection $\pi\colon \mathcal{H} \to (\mathrm{Ad}^0\bar{\rho})^*$ works the same. □

Remark 5.10. As we mentioned before, this global argument does not adapt to the cases when the coefficient field is ramified. Specifically, Lemma 5.9 above is no longer true if we allow the coefficients to ramify, as the extension corresponding to $\mathrm{Ad}^0\rho_2$ corresponds to an element of $\mathrm{H}^1(G_\mathbb{Q}, \mathrm{Ad}^0\bar{\rho})$. Then we cannot apply Chebotarev's theorem to find auxiliary primes which are nontrivial in the element of the cohomology corresponding to $\mathrm{Ad}^0\rho_2$, so we do not get an isomorphism between local and global deformations.

We end this section with a key property about auxiliary primes that will allow us to get the desired local to global isomorphism for H^1. For an element $\tau \in \mathrm{Gal}(L/K)$ we define the Chebotarev set T_τ as the set of nice primes for ρ_n such that $\mathrm{Frob}_q \in \mathrm{Gal}(K/\mathbb{Q}) \rtimes \mathrm{Gal}(L/K)$ has its second coordinate equal to τ (the first one is determined as we are asking q to be nice for ρ_n).

Proposition 5.11. *For any $\tau \in \mathrm{Gal}(L/K)$ as above we have that*

$$\mathrm{H}^1(G_{P\cup T_\tau}, \mathrm{Ad}^0\bar{\rho}) \longrightarrow \bigoplus_{\ell\in P} \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$$

is a surjection.

Proof. This is essentially Proposition 10 of [14], except that we are asking for a condition on $\mathrm{Gal}(K'/\mathbb{Q})$ rather than $\mathrm{Gal}(K/\mathbb{Q})$ (the set T_τ is composed by primes that are nice for ρ_n). Nevertheless, the same proof applies as the main argument is that for any $g \in \mathrm{H}^1(G_{P\cup T_\tau}, (\mathrm{Ad}^0\bar{\rho})^*)$ there are primes $q \in T_\tau$ such that $g|_{G_q} \neq 0$ and this is Proposition 5.7. □

6. The small exponent case

So far we have focused on constructing an appropriate set of deformation conditions and auxiliary primes for the inductive method to work, but as was already noticed, the set C_ℓ and subspace N_ℓ of Case 4 (1) only work for powers p^m such that ρ_ℓ is not trivial modulo p^{m-1}.

It might be the case that there is a prime ℓ such that ρ_n is trivial (not only unramified) at ℓ, but the local deformation ρ_ℓ is ramified. In this case, the argument fails. To bypass this obstacle, we rely on a result by Khare, Larsen and Ramakrishna (the main idea appeared first in [10] but it is better explained in [15]), where they prove that given ρ_n a global mod p^n deformation, one can lift ρ_n a finite number of powers of p, controlling local types at a finite set of primes, at the cost of adding at each lifting step a finite number of ramified primes.

Proposition 6.1. *Let $\rho_n\colon G_P \to \mathrm{GL}_2(W(\mathbb{F})/p^n)$, with big image (i.e., $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho})$) and $z = (z_\ell)_{\ell\in P} \in \oplus_{\ell\in P}\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ be any element. Then one of the following holds*:

- *There is a nice prime q and an element $h \in \mathrm{H}^1(G_{P\cup\{q\}}, \mathrm{Ad}^0\bar{\rho})$ such that the image of h in $\oplus_{\ell\in P}\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ is z and $h|_{G_q} \in N_q$.*
- *There are two nice primes q_1 and q_2, and an element $h \in \mathrm{H}^1(G_{P\cup\{q_1,q_2\}}, \mathrm{Ad}^0\bar{\rho})$ such that the image of h in $\oplus_{\ell\in P}\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ is z and $h|_{G_{q_i}} \in N_{q_i}$.*

Proof. See Proposition 3.6 of [15]. □

The application of this result to our setting is the following.

Proposition 6.2. *Let $\rho_n\colon G_S \to \mathrm{GL}_2(W(\mathbb{F})/p^n)$ and $\rho_\ell\colon G_\ell \to \mathrm{GL}_2(W(\mathbb{F}))$ for $\ell \in P$ as in Theorem A. Assume that $\mathrm{Ш}^2_P(\mathrm{Ad}^0\bar{\rho}) = 0$. Then for any exponent $s > n$ there is a finite set of primes P' (depending on s) containing P and a deformation*

$$\rho_s : G_{P'} \to \mathrm{GL}_2(W(\mathbb{F})/p^s)$$

such that:

- *ρ_s lifts ρ_n,*
- *$\rho_\ell \equiv \rho_s|_{G_\ell} \pmod{p^s}$,*
- *the primes $q \in P'\backslash P$ are nice for ρ_n and $\rho_s|_{G_q}$ is a reduction of a member of C_q.*

Proof. By induction in s. If $s = n$ the statement is trivial. Assume that the result holds for an exponent s. We want to prove that it is also true for $s+1$.

Let ρ_n and ρ_ℓ for every $\ell \in P$ as in the statement of the proposition. Applying our inductive hypothesis we get a deformation $\rho_s\colon G_{P'} \to \mathrm{GL}_2(W(\mathbb{F})/p^s)$ lifting ρ_n and satisfying the local conditions. As $\rho_\ell \bmod p^s$ lifts to $W(\mathbb{F})/p^{s+1}$ for all $\ell \in P$ and $\rho_s|_{G_q}$ is the reduction of some member of C_q for all $q \in P'\backslash P$, the deformation ρ_s is locally unobstructed and the hypothesis $\mathrm{Ш}^2_P(\mathrm{Ad}^0\bar{\rho}) = 0$ implies that ρ_s lifts to a $\widetilde{\rho_{s+1}} : G_{P'} \to \mathrm{GL}_2(W(\mathbb{F})/p^{s+1})$.

We need to adjust $\widetilde{\rho_{s+1}}$ such that $\rho_{s+1}|_{G_\ell} \equiv \rho_\ell \pmod{p^s}$ for all $\ell \in P$. Since ρ_ℓ are deformation, there exists an element $z = (z_\ell)_{\ell\in P} \in \oplus_{\ell\in P}\mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$ that such that, for all

$$(\mathrm{Id}+p^s z_\ell)\widetilde{\rho_{s+1}}|_{G_\ell} = \rho_\ell \,(\mathrm{mod}\, p^{s+1})\,\forall \ell \in P, \text{ and } (\mathrm{Id}+p^s z_q)\widetilde{\rho_{s+1}}|_{G_q} \in C_q\,\forall q \in P'\backslash P.$$

Then by Proposition 6.1 there exists a global element to adjust by as claimed. □

Remark 6.3. During the lifting process (as in the last proposition), the ramification set P could get bigger at each step into a new ramification P'. A crucial fact that we widely used is that if $P \subset P'$ then $\mathrm{Ш}^2_P(\mathrm{Ad}^0\bar{\rho}) = 0$ implies $\mathrm{Ш}^2_{P'}(\mathrm{Ad}^0\bar{\rho}) = 0$.

7. Proof of main theorems

Proof of Theorem A. For each prime $\ell \in P$ such that ρ_ℓ is ramified let n_0 be the least exponent such that ρ_ℓ modulo p^{n_0} is non-trivial. In Section 4 we constructed for each $\ell \in P$ a pair (C_ℓ, N_ℓ) such that N_ℓ preserves the modulo p^m reductions of elements in C_ℓ for all $m > n_0$. If $n_0 \neq n$, i.e., if there exists a prime ℓ for which $\rho_n|G_\ell$ is trivial but ρ_ℓ is ramified, we apply Proposition 6.2 to lift ρ_n to exponent $n_0 + 1$. From this exponent, the inductive method does work, so we can mimic the proof of Theorem 1 of [14].

Let

$$r = \dim_{\mathbb{F}} Ш^2_P(\mathrm{Ad}^0\bar{\rho}) = \dim_{\mathbb{F}} Ш^1_P((\mathrm{Ad}^0\bar{\rho})^*),$$

and let $\{g_1, \dots, g_r\}$ be a basis of $Ш^1_P((\mathrm{Ad}^0\bar{\rho})^*)$. Let $\{f_1, \dots, f_r\}$ be a linearly independent set in $\mathrm{H}^1(G_P, \mathrm{Ad}^0\bar{\rho})$. For each $i = 1, \dots, r$ let q_i be a nice prime such that:

$$f_i|_{G_{q_i}} \notin N_{q_i}, \quad g_i|_{G_{q_i}} \neq 0, \quad f_j|_{G_{q_i}} = g_j|_{G_{q_i}} = 0 \text{ for } j \neq i.$$

Such primes exists by virtue of Corollary 5.8 and Lemma 5.9. Let $Q_1 = \{q_1, \dots, q_r\}$ so that $Ш^2_{P\cup Q_1}(\mathrm{Ad}^0\bar{\rho}) = 0 = Ш^1_{P\cup Q_1}((\mathrm{Ad}^0\bar{\rho})^*)$. With this choice, the inflation map $\mathrm{H}^1(G_P, \mathrm{Ad}^0\bar{\rho}) \to \mathrm{H}^1(G_{P\cup Q_1}, \mathrm{Ad}^0\bar{\rho})$ is an isomorphism by the same dimension counting as in the proof of Fact 16 in [14]. Let $P' = P \cup Q_1$.

Next we need a set of auxiliary primes Q_2 such that the restriction map

$$\mathrm{H}^1(G_{P'\cup Q_2}, \mathrm{Ad}^0\bar{\rho}) \to \bigoplus_{\ell \in P'\cup Q_2} \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})/N_\ell,$$

is an isomorphism. Let $\{f_1, \dots, f_d\}$ be a basis of the preimage of $\oplus_{\ell\in P'} N_\ell$ under the restriction map $\mathrm{H}^1(G_{P'}, \mathrm{Ad}^0\bar{\rho}) \to \oplus_{l\in P'} \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$. Using the identification of Lemma 5.6, for $1 \leq i \leq d$, let α_i be an element of $\mathrm{Gal}(L/K)$ all whose entries are 0 except the i-th which is a nonzero element in which $\tilde{c}$ acts trivially. Let T_i be the Chebotarev set attached to α_i (i.e., the set of nice primes whose Frobenius class in $\mathrm{Gal}(L/\mathbb{Q})$ lies in the class of $c \rtimes \alpha_i$). Proposition 5.11 implies that the map

$$\mathrm{H}^1(G_{P'\cup T_i}, \mathrm{Ad}^0\bar{\rho}) \to \oplus_{\ell\in P} \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})$$

is surjective. By Lemma 14 in [14], we can pick a prime $q_i \in T_i$ such that if $Q_2 = \{q_1, \dots, q_d\}$, then the map

$$\mathrm{H}^1(G_{P'\cup Q_2}, \mathrm{Ad}^0\bar{\rho}) \to \oplus_{\ell\in P'} \mathrm{H}^1(G_\ell, \mathrm{Ad}^0\bar{\rho})/N_\ell,$$

is surjective. It is easy to see that with this set Q_2 is the desired one. Then the process of lifting and adjusting proves the existence of the lift $\rho\colon G_{P\cup Q} \to \mathrm{GL}_2(W(\mathbb{F}))$.

To prove modularity, we know that ρ is odd and has big residual image hence it is residually modular (by Serre's conjectures), so we can use the appropriate modularity lifting theorem: the ordinary case follows from Theorem 5.2 of [19] while the supersingular case follows from Theorem 3.6 of [5].

Regarding the conditions at inertia of the lift, for every $\ell \in P$ the lift ρ satisfies $\rho|_{G_\ell} \in C_\ell$. For primes ℓ where $\rho_n|_{G_\ell}$ is ramified, the condition holds automatically since all deformations in C_ℓ have isomorphic restrictions to inertia. In the case where ρ_n is unramified and ρ_ℓ is Steinberg, observe that the set C_ℓ contains a unique unramified deformation. Since ρ is modular, if it were not ramified at ℓ, then the eigenvalues of $\rho(\mathrm{Frob}_\ell)$ should have the same absolute value but all deformations in C_ℓ have Frobenius eigenvalues q and 1. □

Recall the hypothesis of our second result: let $f \in S_k(\Gamma_0(N), \epsilon)$ be a newform, eigenform for the Hecke operators, with coefficient field K_f and ring of integers $\mathcal{O}_f$. Let $\mathfrak{p}$ a prime ideal in $\mathcal{O}_f$ dividing a rational prime p and $K_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ their respective completions at $\mathfrak{p}$. Let

$$\rho_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^n),$$

be the reduction modulo $\mathfrak{p}^n$ of one of its p-adic Galois representation (which depends on the choice of a basis).

Proof of Theorem B. We want to apply Theorem A to ρ_n, with local deformations $\rho_{f,p}|_{I_\ell}$ at the primes dividing N'. Clearly the second and third hypothesis of Theorem A hold (from the fact that $p > k$) and the hypothesis $p \nmid N$ or f being ordinary at p implies that $\rho_{f,p}|_{I_p}$ can be taken as a deformation at p. Then by Theorem A there exists a modular representation ρ which is congruent to $\rho_{f,p}$ modulo p^n, and of conductor dividing $N'q_1 \dots q_r$. By the choice of the inertia action, the conductor of ρ has the same valuation as the ρ_n one at the primes dividing N', so we only need to show that all the primes q_i are ramified ones. But if this is not the case, by the choice of the sets C_{q_i}, and looking at the action of Frobenius, it would contradict Weil's conjectures, since the roots of the Frobenius' characteristic polynomial would be 1 and q, which do not have the same absolute value.

If ρ_f does not lose ramification while reduced modulo p^n it might happen that $r = 0$ so the newform g obtained would be equal to f. If this is the case, we apply Theorem A with $P = S \cup \{q\}$, q being in the hypotheses of auxiliary primes and

$$\rho_q = \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$$

with $*$ ramified (up to twist). □

8. An example

We end this article with an explicit example of Theorem A for level raising modulo p^2. For an elliptic curve $E/\mathbb{Q}$ of prime conductor $\mathfrak{q}$ and full image at $p = 5$, i.e., $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_5)$, we construct a newform in $S_2(\Gamma_0(\mathfrak{q}\mathfrak{r}))$ (for some prime $\mathfrak{r}$) which is congruent to E modulo 25. The choices $p = 5$ and prime conductor are used to make the cohomological dimensions as small as possible.

Let ρ_5 be the 5-adic Galois representation attached to E (by looking at the Galois action on the Tate module). The adjoint representation of its residual

representation is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5)$ which is isomorphic to S_5, the symmetric group in 5 elements. We need to compute $\mathrm{H}^1(G_S, \mathrm{Ad}^0\bar{\rho})$ and $\mathrm{H}^2(G_S, \mathrm{Ad}^0\bar{\rho})$ for $S = \{5, \mathfrak{q}\}$. Recall the following results:

- If $\ell \not\equiv \pm 1 \pmod{p}$ then $\mathrm{H}^2(G_\ell, \mathrm{Ad}^0\bar{\rho}) = 0$ (see Section 3, or [13] Proposition 2).
- If $\overline{\rho_5}$ is flat, and $\overline{\rho_5}|_{G_5}$ is indecomposable, then $\mathrm{H}^2(G_5, \mathrm{Ad}^0\bar{\rho}) = 0$ (see [14], Table 3).

Let $r = \dim Ш^1_S((\mathrm{Ad}^0\bar{\rho})^*)$, and let s be the number of primes for which $H^2(G_\ell, \mathrm{Ad}^0\bar{\rho}) \neq 0$. Then

- $\dim \mathrm{H}^1(G_S, \mathrm{Ad}^0\bar{\rho}) = r + s + 2$,
- $\dim \mathrm{H}^2(G_S, \mathrm{Ad}^0\bar{\rho}) = r + s$.

(See Lemma in page 139 of [14].)

8.1. Some group theory

Recall from Lemma 9 (of [13]) that the elements in $\mathrm{H}^1(G_S, \mathrm{Ad}^0\bar{\rho})$ (respectively, in $\mathrm{H}^1(G_S, \mathrm{Ad}^0\bar{\rho}^*)$) give extensions M of $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})$ (respectively, $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}^*)$) whose Galois group over $\mathbb{Q}$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5) \ltimes M_2^0(\mathbb{F}_5)$ (the 2×2 matrices with zero trace). The problem is that $\mathrm{PGL}_2(\mathbb{F}_5)$ has order 120 and is very non-abelian (nor solvable), hence nowadays we cannot do class field theory in such extensions. To overcome this problem we study the groups involved so as to work with smaller extensions of $\mathbb{Q}$.

Lemma 8.1. *Let H be a subgroup of S_5 and let $V \subseteq M_2^0(\mathbb{F}_5)$ be an H-stable subspace. Then $H \ltimes V$ is a subgroup of $S_5 \ltimes M_2^0(\mathbb{F}_5)$. Furthermore, if $V \subseteq W$, then $H \ltimes V$ is a normal subgroup of $H \ltimes W$ if and only if H acts trivially on W/V.*

Proof. The first claim is clear from the definition of a semi-direct product. For the second claim, note that conjugation acts in the following way

$$(h, w)(g, v)(h, w)^{-1} = (hgh^{-1}, w + h \cdot v - (hgh^{-1}) \cdot w).$$

Since hgh^{-1} varies over all elements of H, the subgroup is normal if and only if $w - h \cdot w \in V$ for all $h \in H$. □

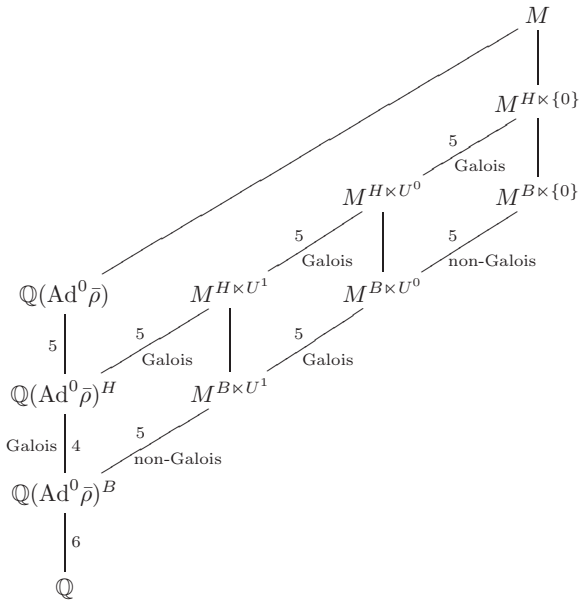
Let H be the unipotent subgroup of $\mathrm{PGL}_2(\mathbb{F}_5)$ given by matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and let $B \subset \mathrm{PGL}_2(\mathbb{F}_5)$ the Borel subgroup (of upper triangular matrices). Clearly $|H| = 5$, $|B| = 20$ and $H \triangleleft B$. For both H and B, $M_2^0(\mathbb{F}_5)$ has the following stable submodules filtration:

$$0 \subseteq U^0 \subseteq U^1 \subseteq M_2^0(\mathbb{F}_5),$$

where U^1 is the subspace of upper triangular matrices and U^0 is the subspace of strictly upper triangular matrices. The group H acts trivially on all quotients of

this filtration and B acts trivially on U^1/U^0. Using Lemma 8.1 we get the following Hasse diagram:

(8.1)



Remark 8.2. The Galois closure of $M^{H\ltimes U^1}$ is M, since it is easy to check that the intersection of all Galois conjugates of $H \ltimes U^1$ in $S_5 \ltimes M_2^0(\mathbb{F}_5)$ is trivial.

We also consider the subgroup $S_3 \times C_2$ (where C_n denotes the cyclic group of order n). If we identify

$$S_3 \times C_2 = \left\langle \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix} \right\rangle \times \left\langle \begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix} \right\rangle$$

in $\mathrm{PGL}_2(\mathbb{F}_5)$, the action decomposes as

$$\left\langle \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix} \right\rangle \oplus \left\langle \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

The action in the 1-dimensional subspace (which can be identified with the quotient) is non-trivial. Nevertheless its restriction to the cyclic subgroup of order 6 is trivial (such group is the stabilizer of the matrix $\left(\begin{smallmatrix} 4 & 1 \\ 1 & 1 \end{smallmatrix}\right)$). It is clear that the intersection of its conjugates is trivial (since A_5 is the only normal subgroup of S_5 and the action of S_5 in $M_2^0(\mathbb{F}_5)$ is irreducible).

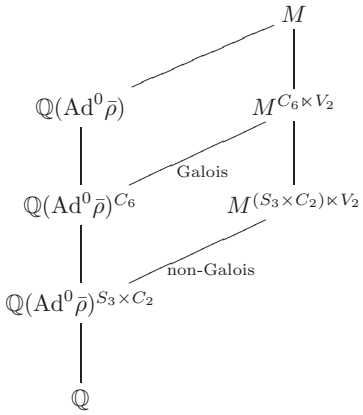
Lemma 8.3. $(C_3 \times C_2) \ltimes V_2 \lhd (S_3 \times C_2) \ltimes M_2^0(\mathbb{F}_5)$.

Proof. Lemma 8.1 implies that

$$(C_3 \times C_2) \ltimes V_2 \lhd (C_3 \times C_2) \ltimes M_2^0(\mathbb{F}_5),$$

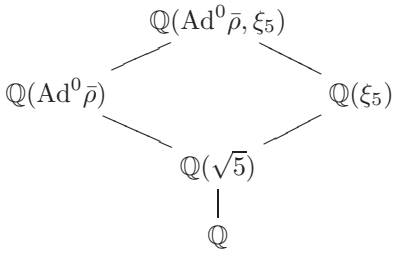
but since $C_3 \lhd S_3$, the same proof gives the statement. □

For such group, we get the following Hasse diagram:



To compute with the adjoint representation, we must add the 5-th roots of unity. The Hasse diagram is the following:

(8.2)



Then $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}^*)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho},\xi_5)/\mathbb{Q}) \simeq C_4 \ltimes A_5$, where the action is through the projection $C_4 \to C_2$, and the latter action is the classical isomorphism $S_5 \simeq C_2 \ltimes A_5$. This Galois group also acts on $M_2^0(\mathbb{F}_5)$, where the C_4 part acts as $\mathbb{F}_5^\times$ (which corresponds to the mod 5-cyclotomic character action), and A_5 as before. To compute the Shafarevich group $Ш^1(G_S, \mathrm{Ad}^0\bar{\rho}^*)$, we do a similar trick as before, we consider the subgroup $C_4 \ltimes C_3$ (which also satisfies that the intersection of its conjugates is trivial), which is an extension of the previous cyclic group of order 6, and get exactly the same degree 20 extension.

8.2. A specific example

In this section we will use many computations that were done using PARI/GP [11]. Consider the elliptic curve

$$E_{89b1} : y^2 + xy = x^3 + x^2 - 2$$

Let $\rho_{E,5}$ denote the representation attached to the 5-adic Tate module of E. The residual representation has full image (using Sage [17]), so if we look at the representation on the 5^2 torsion points, we get a representation that is in the hypothesis

of Theorem A. The residual adjoint representation corresponds to a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$ and ramified at 5 and 89. We can search for such extensions (they are the Galois closure of a degree 5 extension) in Jones–Roberts tables (see [8]), and get 12 such extensions, given by the polynomials:

$$\begin{aligned}
&x^5 - x^4 + 5x^3 - x^2 + 6x + 1, && x^5 + 10x^3 - 20x^2 + 45x - 148,\\
&x^5 - 5x^3 - 5x^2 - 5x - 6, && x^5 - 30x^2 - 30x - 97,\\
&x^5 - 125x^2 + 375x + 425, && x^5 + 445x - 445,\\
&x^5 - 890x^2 - 4005x - 5429, && x^5 - 890x^2 + 9790x + 10591,\\
&x^5 - 445x^2 + 20915x + 159132, && x^5 + 50x^3 - 125x^2 + 350x - 680,\\
&x^5 - 50x^3 - 325x^2 - 375x - 5220, && x^5 + 200x^3 - 1625x^2 + 9575x - 176395,\\
&x^5 - 200x^3 - 375x^2 + 22925x - 81155.
\end{aligned}$$

To know which one corresponds to our elliptic curve, we just compute the order of Frobenius at $3, 7, 11$ and 13, which are $6, 4, 3$ and 6 respectively. If we compute the inertial degree at those primes in the above extensions, we see that the only extension with those inertial degrees is the one corresponding to $x^5 + 445x - 445$.

Lemma 8.4. *The representation $\overline{\rho}_{E,5}$ satisfies the following properties*:

- *The extensions corresponding to its image and the adjoint image ramify at* 89.
- *If we restrict the representation to the decomposition group at* 5, *it is ordinary and indecomposable.*

Proof. The first fact can be checked by computing the field discriminant (note that the scalar matrices correspond to an extension unramified at 89). Nevertheless, this is a more general statement, since if the residual representation is unramified at 89, by Ribet's lowering the level theorem, there should exist a weight 2 and level 1 modular form, which is not the case. To prove the second statement, we know that the representation is ordinary because $a_5(E) = -2$ (it is not divisible by 5). If the restriction to inertia at 5 were decomposable, then the order of inertia would be 4, but 5 ramifies completely in the degree 5 extension computed above. □

The degree 20 subextension of $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ is given by the polynomial

$$\begin{aligned}
P(x) = {} & x^{20} + 45822985000\,x^{16} + 245086878906250\,x^{14} + 535483380861855000000\,x^{12}\\
& + 670170049528361372070312 5\,x^{10} + 232361959662822291573095703125\,x^8\\
& + 259620852509525077791732177734375 00\,x^6\\
& - 403189903768430226056054371193847656250\,x^4\\
& + 464093901354840961393978389407043457031 2500\,x^2\\
& + 966893698176577013809175970469023745422363 28125.
\end{aligned}$$

Lemma 8.5. $\dim \mathrm{H}^2(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_{E,5}) = 0$ *and* $\dim \mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_{E,5}) = 2$.

Proof. Recall that $\dim \mathrm{H}^2(G_S, \mathrm{Ad}^0\bar{\rho}_E) = r + s$ and $\dim \mathrm{H}^1(G_S, \mathrm{Ad}^0\bar{\rho}_E) = r + s + 2$, where $r = \dim Ш^1_S((\mathrm{Ad}^0\bar{\rho}_E)^*)$ and s is the number of $\ell \in S$ such that $\dim \mathrm{H}^2(G_\ell, \mathrm{Ad}^0\bar{\rho}_E) \neq 0$.

It can be checked that E has split multiplicative reduction at 89, implying that the residual representation is Steinberg at 89.

As $89 \equiv -1 \pmod 5$, the comments at the beginning of Section 8 imply $\mathrm{H}^2(G_{89}, \mathrm{Ad}^0\bar{\rho}_E) = 0$ and since $\overline{\rho}_{E,5}|_{G_5}$ is indecomposable $\mathrm{H}^2(G_5, \mathrm{Ad}^0\bar{\rho}_E) = 0$ and $s = 0$. On the other hand, elements of $Ш^1_S((\mathrm{Ad}^0\bar{\rho}_E)^*)$ give rise to unramified degree 5 abelian extensions of $\mathbb{Q}((\mathrm{Ad}^0\bar{\rho}_E)^*)$ where the primes above 5 and 89 split completely. In particular, they are unramified extensions of $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)^{C_6}$ (see Diagram (8.2) and the discussion after it). Using PARI/GP [11] one can check that the class number of such degree 20 extension is 24, which is not divisible by 5, so Sha is trivial and $r = 0$. □

Remark 8.6. The same argument proves that $\dim \mathrm{H}^1(G_{\{5\}}, \mathrm{Ad}^0\bar{\rho}_E) = 2$, and by the inflation-restriction exact sequence, $\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E) \simeq \mathrm{H}^1(G_{\{5\}}, \mathrm{Ad}^0\bar{\rho}_E)$ so we restrict to elements which are unramified at 89.

Remark 8.7. In our hypothesis, the local $\mathrm{H}^1(G_5, \mathrm{Ad}^0\bar{\rho}_E)$ has dimension 3, and the subspace N_5 is that of finite flat group schemes which is 1 dimensional (by Table 3 of [14]).

Consider the map

$$\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E) \mapsto \mathrm{H}^1(G_5, \mathrm{Ad}^0\bar{\rho}_E)/N_5 \times \mathrm{H}^1(G_{89}, \mathrm{Ad}^0\bar{\rho}_E)/N_{89}. \tag{8.3}$$

Recall that $N_{89} = \mathrm{H}^1(G_{89}, \mathrm{Ad}^0\bar{\rho}_E)$, so we can just discard this term. Both spaces have dimension 2, so we need to compute the kernel of the map. Elements on the left give rise to degree 5 extensions of $L = \mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)^H$ that are unramified outside 5 and 89. A polynomial defining L is

$$\begin{aligned}
&x^{24} - 9901250\,x^{21} - 2291149250\,x^{20} - 110151406250\,x^{19} + 38233553109375\,x^{18}\\
&+ 23557750800468750\,x^{17} + 11619555204080093750\,x^{16} - 19413331678164062500\,x^{15}\\
&- 12542398375975805289062 5\,x^{14} - 51488038276826726562500000\,x^{13}\\
&- 10523678241093366455173828125\,x^{12} - 10613085707747871628823242 1875\,x^{11}\\
&- 17526325566077155347275909179 6875\,x^{10} + 44232966417342564073908569335937500\,x^{9}\\
&+ 22607278096633010862335357756591796875\,x^{8}\\
&+ 49189935957195016658726264040527343 7500\,x^{7}\\
&+ 28672677663271022255971277124009155273437 5\,x^{6}\\
&+ 61254459616385605854391463803496704101562500\,x^{5}\\
&+ 53469744741542985215386122652330757202148437 50\,x^{4}\\
&+ 33302448226823892464391700813613248825073242187 5\,x^{3}\\
&+ 53735066160353981335257513593580636940002441406250\,x^{2}\\
&+ 47159749715923474017432102814961482249259948730468 75\,x\\
&+ 18366906014479370755271795948977470947694778442382 8125
\end{aligned}$$

In order to replicate the proof of Theorem A, we need to understand the morphism (8.3). We thank Ravi Ramakrishna for the following observation.

Lemma 8.8. *The morphism* (8.3) *has one dimensional kernel.*

Proof. The domain of the morphism (8.3) is of dimension 2. We will see that its kernel is neither 0 nor 2 dimensional. The kernel gives the tangent space of the deformation problem corresponding to minimally ramified lifts of $\overline{\rho}_E$. If the morphism were injective, then the universal deformation ring should be isomorphic to $\mathbb{Z}_5$, and there should be a unique lift to any coefficient ring. However, it can be checked that there is a modular form of level 89 and weight 2 which is congruent to E modulo 5, therefore the kernel of the morphism (8.3) is not trivial.

On the other hand, since $N_{89} = \mathrm{H}^1(G_{89}, \mathrm{Ad}^0\bar{\rho}_E)$, the kernel consists of cocycles mapping to N_5 in $\mathrm{H}^1(G_5, \mathrm{Ad}^0\bar{\rho}_E)$. As the elements in $\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E)$ are only ramified at 5, if two linearly independent cocycles map to N_5 (which is one dimensional) we can take a linear combination of them mapping to zero. In particular, there exists an unramified extension of $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ which is not the case. □

Lemma 8.8 tells us that there is a cocycle κ in $\mathrm{H}^1(G_{5,89}, \mathrm{Ad}^0\bar{\rho}_E)$ that maps to $\mathrm{H}^1_{\mathrm{flat}}(G_5, \mathrm{Ad}^0\bar{\rho})$. We want to compute this extension. The following lemma describes the corresponding extensions.

Lemma 8.9. *A cocycle κ lies in $\mathrm{H}^1_{flat}(G_5, \mathrm{Ad}^0\bar{\rho})$ if and only if there is a prime above 5 in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})^B$ that does not ramify in $M^{B\ltimes U^0}$.*

Proof. Let $F = \mathbb{Q}(\mathrm{Ad}^0\bar{\rho})^B$ and $F' = M^{B\ltimes U^0}$. Recall that to a cocycle $\kappa \in \mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho})$ we attached the field M fixed by $\operatorname{Ker}\kappa|_{G_{\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})}} = \kappa|^{-1}_{G_{\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})}}(0)$. Since F is the field fixed by $G_F = \kappa|^{-1}_{G_F}(\mathrm{Ad}^0\bar{\rho})$ it can be easily seen that F' is the field fixed by $\kappa|^{-1}_{G_F}(U^0)$. Let I_5 be a inertia group at 5 in $\mathrm{Gal}(M/\mathbb{Q})$. By definition,

$$\mathrm{H}^1_{\mathrm{flat}}(G_5, \mathrm{Ad}^0\bar{\rho}) = \operatorname{Ker}\left(\mathrm{H}^1(G_5, \mathrm{Ad}^0\bar{\rho}) \to \mathrm{H}^1(I_5, \mathrm{Ad}^0\bar{\rho}/U^0)\right),$$

so $\kappa \in \mathrm{H}^1_{\mathrm{flat}}(G_5, \mathrm{Ad}^0\bar{\rho})$ if and only if there is a representative of the class such that $\kappa(I_5) \subseteq U^0$ which happens if and only if $I_5 \subseteq \kappa^{-1}(U^0)$. We claim that $I_5 \subseteq \kappa^{-1}(U^0)$ if and only if $I_5 \cap G_F \subseteq \kappa|^{-1}_{G_F}(U^0)$ if and only if $\kappa|_{G_F}(I_5 \cap G_F) \subseteq U^0$. This follows from the following facts:

- κ factors through $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/\mathbb{Q}) \ltimes \mathrm{Gal}(M/\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))$.
- The image of I_5 in $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/\mathbb{Q}) \ltimes \mathrm{Gal}(M/\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))$ is $\overline{\rho}(I_5) \ltimes \kappa(I_5)$.
- $\kappa(I_5 \cap \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/\mathbb{Q}) \ltimes 1) = \overline{\rho}(I_5) \ltimes 1 = \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/F) \simeq B \ltimes 1$.
- U^0 is stable under $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})/F) \simeq B$.

Summing up, $\kappa \in \mathrm{H}^1_{\mathrm{flat}}(G_5, \mathrm{Ad}^0\bar{\rho})$ if and only if $I_5 \cap G_F \subseteq \kappa|^{-1}_{G_F}(U^0)$ if and only if (since F' is the field fixed by $\kappa|^{-1}_{G_F}(U^0)$) the prime in F above 5 does not ramify in F'. □

Remark 8.10. The cocycle κ gives a non-abelian degree 25 extension of F (see Diagram (8.1)). Instead we compute it as a degree 5 abelian extension of L (which has degree 24) using the fact that it is unramified at a prime above 5 with ramification degree 4 in $L/\mathbb{Q}$.

To use class field theory, we bound the modulus exponent $e(\mathfrak{p})$ with the following result.

Proposition 8.11. *Let L/K be an abelian extension of prime degree p and $\mathfrak{p}$ a prime ideal of K. Let $e(\mathfrak{p}|p)$ denote the ramification degree of $\mathfrak{p}$ over the rational prime p. If $\mathfrak{p}$ ramifies in L/K, then*

$$\begin{cases} e(\mathfrak{p}) = 1 & \text{if } \mathfrak{p} \nmid p, \\ 2 \leq e(\mathfrak{p}) \leq \left\lfloor \frac{pe(\mathfrak{p}|p)}{p-1} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid p. \end{cases}$$

Proof. See Propositions 3.3.21 and 3.3.22 in [3]. □

The prime 5 factors as $\mathfrak{p}_{5,1}^{20}\mathfrak{p}_{5,2}^{4}$ in L, where each prime ideal $\mathfrak{p}_{5,i}$ has inertial degree 1. By Remark 8.6 we do not need to allow ramification at the prime 89. Recall that the extension attached to κ is unramified at $\mathfrak{p}_{5,2}$. Proposition 8.11 gives the modulus $\mathfrak{p}_{5,1}^{25}\mathfrak{p}_{5,2}^{0}$ whose class group (using PARI/GP [11]) is isomorphic to

$$C_{100} \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5.$$

From all these degree 5 extensions, we need to identify the ones that correspond to elements in $\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E)$ (which give extensions isomorphic to $M_2^0(\mathbb{F}_5)$). Let $\tilde{L}$ denote the abelian degree 5 extension $M^{H \ltimes U^1}$ of L attached to an extension M in $\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E)$.

Lemma 8.12. *If a rational prime p is unramified in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ and has a prime ideal of L over it with inertial degree 5, then it has inertial degree 5 in M.*

Proof. Let $\mathfrak{p}$ be a prime in M dividing the prime with inertial degree 5 in L. Since the maximal 5-Sylow subgroup of S_5 is cyclic of order 5, the decomposition group of p in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ is cyclic of order 5. Then the decomposition group $D(\mathfrak{p})$ is a subgroup $C_5 \ltimes M_2^0(\mathbb{F}_5)$. Since a cyclic group cannot be written as a semidirect product of groups whose orders are divisible by 5, $D(\mathfrak{p}) = C_5$. □

Test 1: for each prime p check whether it has inertial degree 5 in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ or not (by looking how the degree 5 polynomial splits modulo p). If it does, search for all primes in L with inertial degree 5, and restrict to the subspace of characters in the class group which are trivial on them.

This first test lowers the dimension drastically. With primes up to 300, we find that the subspace V which passes the test has dimension 2.

Lemma 8.13. *Let L/K be a Galois extension, and M/L be a Galois extension of prime degree p corresponding to a character χ. Consider the vector space obtained by evaluating the Galois conjugates of χ at all different prime ideals, and let r*

denote its dimension (as an $\mathbb{F}_p$ vector space). Then the Galois closure of M over K has degree p^r.

Proof. This is an easy exercise of Galois theory. □

Test 2: consider each character of V as a character on $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ by composing with the norm map to L. To compute the action of $\mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)/\mathbb{Q})$ on it, it is enough to determine its values at prime ideals which split completely in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)/\mathbb{Q}$ (they have density 1 in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$) where the Galois action becomes simpler. To compute the conjugates of the character, we compute the values that the character takes on the conjugates of these primes. Let $\alpha_1, \ldots, \alpha_5$, be the the roots of $Q(x) = x^5 + 445x - 445$ (so $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E) = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$) and let $L = \mathbb{Q}(\beta)$, where $\beta = P(\alpha_1, \ldots, \alpha_5)$ (in our case, we can take $P(x_1, \ldots, x_5) = x_1^2\, x_2 + x_2^2\, x_3 + x_3^2\, x_4 + x_4^2\, x_5 + x_5^2\, x_1$). Recall that any prime ideal $\mathfrak{q} \in \mathcal{O}_L$ which splits completely can be presented in the form $\mathfrak{q} = \langle \beta - a_\mathfrak{q}, q\rangle_{\mathcal{O}_L}$ where $q = \mathcal{N}(\mathfrak{q})$ and $a_\mathfrak{q} \in \mathbb{F}_q$. In particular, $a_\mathfrak{q}$ is the unique element in $\mathbb{F}_q$ which satisfies that $v_\mathfrak{q}(\beta - a_\mathfrak{q}) \geq 1$.

Note that since $Q(x)$ factors linearly modulo q (with roots $\tilde{\alpha_1}, \ldots, \tilde{\alpha_5}$), there is a match between $\{\alpha_i\}$ and $\{\tilde{\alpha_i}\}$ which makes $a_\mathfrak{q} = P(\tilde{\alpha_1}, \ldots, \tilde{\alpha_5})$ (since $\alpha_i - \tilde{\alpha_i} \in (q)$). Then if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)/\mathbb{Q})$ (which we identify with S_5), its action on $\mathfrak{q}$ is given by sending the ideal $\mathfrak{q}$ to the unique ideal $\tilde{\mathfrak{q}}$ such that $a_{\tilde{\mathfrak{q}}}$ equals $P(\tilde{\alpha}_{\sigma(1)}, \ldots, \tilde{\alpha}_{\sigma(5)})$.

With this procedure, we loop over all characters of V (up to powers, i.e., we can think of them as elements in $\mathbb{P}^2(\mathbb{F}_5)$) and compute the number of Galois conjugates of it at a finite list of primes (the first 5 splitting primes work) discarding the ones giving a vector space of dimension greater than 3. There are only 2 elements in $\mathbb{P}^4(\mathbb{F}_5)$ whose vector space has dimension smaller than 4. One of these elements corresponds to our cocycle κ.

To identify it, we need to run a not so rigorous test. Recall that we are searching for extensions whose Galois group is $S_5 \ltimes M_2^0(\mathbb{F}_5)$. Since we cannot compute the Galois closure of our degree 5 extensions, we use Chebotarev density theorem. If M is such an extension, and a prime number has inertial degree 6 in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$, then it might have inertial degree 6 or 30 in M. Furthermore, once we fixed an element in S_5 of order 6, it is easy to see that there are 100 choices (out of the 125) of elements in $S_5 \ltimes M_2^0(\mathbb{F}_5)$ of order 30 and 25 of order 6 whose projection to S_5 gives the chosen order 6 element, giving a density of 0.8.

Test 3: for the two characters, we check whether they are trivial or not at all primes with inertial degree 6 in $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ up to a given bound, say 10.000. For the first character, we find that 156 out of 208 primes have inertial degree bigger than 6 while in the second case the same happens for 24 out of 208 primes. This implies that the first character corresponds to the extension we are looking for.

Remark 8.14. One can make the third test complete by using some explicit version of Chebotarev density theorem but the range of computation will take too long without assuming for example Artin's conjectures.

We know that the image of (8.3) has dimension 1. In particular just one extra prime is enough to get an isomorphism. We search for a prime $q \not\equiv \pm 1 \pmod 5$ and

such that $a_q \equiv \pm(q+1) \pmod{25}$. The prime $q = 293$ satisfies both conditions, since $a_{293} = -6 \equiv -(293+1) \pmod{25}$.

Theorem 8.15. *There exists a weight* 2 *modular form of level* $89 \cdot 293$ *which is congruent modulo* 5^2 *to the modular form attached to* E_{89b1}.

Proof. In view of the previous discussion, we just need to check that 293 is the right choice for the map

$$\begin{aligned}&\mathrm{H}^1(G_{\{5,89,293\}}, \mathrm{Ad}^0\bar{\rho}_E)\\ &\quad\mapsto \mathrm{H}^1(G_5, \mathrm{Ad}^0\bar{\rho}_E)/N_5 \times \mathrm{H}^1(G_{89}, \mathrm{Ad}^0\bar{\rho}_E)/N_{89} \times \mathrm{H}^1(G_{293}, \mathrm{Ad}^0\bar{\rho}_E)/N_{293},\end{aligned}$$

to be an isomorphism. Since $293 \not\equiv \pm 1 \pmod 5$, $\dim \mathrm{H}^1(G_{\{5,89,293\}}, \mathrm{Ad}^0\bar{\rho}_E) = 3$. Let κ_{293} denote a non-zero element not in $\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E)$, and let κ_1, κ_2 be a basis of $\mathrm{H}^1(G_{\{5,89\}}, \mathrm{Ad}^0\bar{\rho}_E)$, such that $\kappa_2 = \kappa$ (the cycle unramified at $\mathfrak{p}_{5,2}$). Then in the basis $\{\kappa_1, \kappa_2, \kappa_3\}$ the linear transformation matrix looks like $\left(\begin{smallmatrix} a & 0 & b \\ c & 0 & d \\ e & f & g \end{smallmatrix}\right)$. To prove it is invertible, it is enough to prove that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible, and that f is non-zero.

Since the image of $\mathrm{H}^1(G_{\{5\}}, \mathrm{Ad}^0\bar{\rho}_E)$ in $\mathrm{H}^1(G_5, \mathrm{Ad}^0\bar{\rho}_E)$ is two dimensional, if κ_{293} restricted to G_5 is not linearly independent with them, there should exist an extension of $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ which is unramified outside 293, but using CFT one easily sees that there are no such extensions (the ray class group is isomorphic to $C_{3504} \times C_{12} \times C_2$). Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible.

To prove that $f \neq 0$, we need to check that the prime 293 does not split completely in the extension attached to the cocycle κ. Using the complete description of such cocycle (as a character of a class group) we evaluate it at the primes dividing 293 and see that it is trivial at 2 primes, and not trivial at the other 4 ones, which implies that 293 does not split completely from $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}_E)$ to M. This ends the proof. □

Remark 8.16. In this particular case, searching for the particular form is out of computational reach, as the level $89 \cdot 293$ is too big to compute the corresponding space.

References

[1] BREUIL, C. AND DIAMOND, F.: Formes modulaires de Hilbert modulo p et valeurs d'extensions entre caractères galoisiens. *Ann. Sci. Éc. Norm. Supér. (4)* **47** (2014), no. 5, 905–974.

[2] CARAYOL, H.: Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.* **59** (1989), no. 3, 785–801.

[3] COHEN, H.: *Advanced topics in computational number theory.* Graduate Texts in Mathematics 193, Springer-Verlag, New York, 2000.

[4] CORNELL, G., SILVERMAN, J. H. AND STEVENS, G.: *Modular forms and Fermat's last theorem.* (Papers from the Instructional Conference on Number Theory and Arithmetic Geometry, Boston, MA, 1995). Springer-Verlag, New York, 1997.

[5] Diamond, F., Flach, M. and Guo, L.: The Tamagawa number conjecture of adjoint motives of modular forms. *Ann. Sci. École Norm. Sup. (4)* **37** (2004), no. 5, 663–727.

[6] Dummingan, N.: Level-lowering for higher congruences of modular forms. Preprint, 2005. http://www.neil-dummigan.staff.shef.ac.uk/level18.pdf.

[7] Hamblen S. and Ramakrishna, R.: Deformations of certain reducible Galois representations. II.. *Amer. J. Math.* **130** (2008), no. 4, 913–944.

[8] Jones, J. W. and Roberts, D. P.: A database of number fields. http://hobbes.la.asu.edu/NFDB, 2013.

[9] Khare, C.: Modularity of p-adic Galois representations via p-adic approximations. *Théor. Nombres Bordeaux* **16** (2004), no. 1, 179–185.

[10] Khare, C., Larsen, M. and Ramakrishna, R.: Constructing semisimple p-adic Galois representations with prescribed properties. *Amer. J. Math.* **127** (2005), no. 4, 709–734.

[11] The PARI Group: PARI/GP, version 2.5.5. Univ. Bordeaux, 2013. Available from http://pari.math.u-bordeaux.fr/.

[12] Ramakrishna, R.: On a variation of Mazur's deformation functor. *Compositio Math.* **87** (1993), no. 3, 269–286.

[13] Ramakrishna, R.: Lifting Galois representations. *Invent. Math.* **138** (1999), no. 3, 537–562.

[14] Ramakrishna, R.: Deforming Galois representations and the conjectures of Serre and Fontaine–Mazur. *Ann. of Math. (2)* **156** (2002), no. 1, 115–154.

[15] Ramakrishna, R.: Constructing Galois representations with very large image. *Canad. J. Math.* **60** (2008), no. 1, 208–221.

[16] Ribet, K. A.: On l-adic representations attached to modular forms. II. *Glasgow Math. J.* **27** (1985), 185–194.

[17] The Sage Developers: SageMath, the Sage Mathematics Software System, version 8.4. http://www.sagemath.org, 2018.

[18] Serre, J. P.: *Abelian ℓ-adic representations and elliptic curves.* Second edition. Advanced Book Classics, Addison-Wesley Pub. Company, Redwood City, CA, 1989.

[19] Skinner, C. M. and Wiles, A. J.: Nearly ordinary deformations of irreducible residual representations. *Ann. Fac. Sci. Toulouse Math. (6)* **10** (2001), no. 1, 185–215.

Received July 21, 2016; revised April 20, 2017. Published online December 6, 2018.

Maximiliano Camporino: Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 1428 Buenos Aires, Argentina.
E-mail: maxicampo@gmail.com

Ariel Pacetti: FaMAF-CIEM, Universidad Nacional de Córdoba, 5000, Córdoba, Argentina.
E-mail: apacetti@famaf.unc.edu.ar

MC was partially supported by a CONICET doctoral fellowship. AP was partially supported by grants BID-PICT-2013-0294, PIP 2014-2016 11220130100073 and UBACyT-2014-2017-20020130100143BA.