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 some technical conditions). Moreover, we can chose the inertial type of our lift 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. In particular, our method shows that given a modular eigenform f without Complex Multiplication or inner twists, for all primes p but finitely many, and for all positive integers n, there exists another 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 (and more generally, abstract representations) modulo prime powers. The main strategy of the paper is to adapt the arguments of [Ram99] and [Ram02] to this new setting, which is harder due to semisimplification problems. Let $\mathbb{F}$ be a finite field of residual characteristic p, and $\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}_2(W(\mathbb{F})/p^n)$ be a continuous representation. We denote by $\overline{\rho_n}$ its reduction modulo p.

If T is a finite set of primes, we denote by G_T the Galois group of $\mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$, where $\mathbb{Q}_T$ is the maximal extension of $\mathbb{Q}$ unramified outside T, and by $G_{\mathbb{Q}}$ we will denote the whole Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One of the main results of this work is the following.

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

- *The image is big, i.e. $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho_n})$.*
- *ρ_n is odd.*
- *The restriction $\overline{\rho_n}|_{G_p}$ is not twist equivalent to the trivial representation nor the indecomposable unramified representation given by $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$.*

Let P be a finite set of primes containing S, and for every $\ell \in P$, $\ell \neq p$, fix a deformation $\rho_\ell : G_\ell \to W(\mathbb{F})$ of $\rho_n|_{G_\ell}$. At the prime p, let ρ_p be a deformation 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 $\ell \in P$,*
- *$\rho|_{G_q}$ is a ramified representation of Steinberg type for every $q \in Q$.*

This result, contrary to the results of Ramakrishna, is only about odd representations (and hence modular by Serre's conjectures). In the even case, the exact same ideas plus some extra hypothesis (as in [Ram99]) give a result for any abstract representation with big image.

2010 *Mathematics Subject Classification.* 11F33; 11F80.

Key words and phrases. Modular Forms; Galois Representations.

MC was partially supported by a CONICET doctoral fellowship.

AP was partially supported by CONICET PIP 2010-2012 GI and FonCyT BID-PICT 2010-0681.

Remark. Theorem A is in the same spirit as Theorem 3.2.2 of [BD], where they only consider residual representations, and allow the coefficient field to grow. The advantage of their method is that it does not require to add extra ramification (so $Q = \emptyset$), but this phenomena only works while working modulo a prime. 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 [Dum05]).

For $f \in S_k(\Gamma_0(N), \epsilon)$ $(k \geq 2)$ 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, $K_\mathfrak{p}$ the completion at $\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ its ring of integers. Finally let $\rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_\mathfrak{p})$ 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. Applying Theorem A to this representation, we are able to derive the other main result of this paper.

Theorem B. *In the above hypothesis, let n be a positive integer and $p > k$ be a prime such that:*

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

Let R be the set of ramified primes of ρ_n. If $N' = \prod_{p \in R} p^{v_p(N)}$, then there exist an integer r, a set $\{q_1, \dots, q_r\}$ 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 $N'q_1 \dots q_r$ 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.

Keeping the same notation as in Theorem B, we get the following consequences.

Corollary 1.1 (Lowering the level)**.** *Let $f \in S_k(\Gamma_0(M), \varepsilon)$ be a newform, $\mathfrak{p}$ a prime of $\mathcal{O}_f$ above $p \in \mathbb{Q}$ and $\rho_n : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_f/\mathfrak{p}^n)$ be a modulo $\mathfrak{p}^n$ reduction of its $\mathfrak{p}$-adic representation. Suppose that:*

- *$p > 5$.*
- *$2 \leq k \leq p - 1$.*
- *$\mathrm{SL}_2(\mathcal{O}_f/\mathfrak{p}) \subseteq \mathrm{Im}(\overline{\rho_n})$.*
- *p does not ramify in $\mathcal{O}_f$.*

If $\ell \mid M$ is such that ρ_n is unramified at ℓ, then the Hecke map factors through the ℓ-old quotient $\mathbb{T}_k^{\ell\text{-}old}(M, \ell)$.

Proof. The proof consists on combining the result for primes $\ell \not\equiv 1 \pmod{p}$ (which was proved in [Dum05], Theorem 1), with Theorem B that allows us to move the ramified primes to a situation where we get more control on the extra Steinberg ramification. Specifically, if $\ell \equiv 1 \pmod{p}$, then by Theorem B, we can find a form g with the same ramification as f, but without ℓ in the level at the cost of adding many Steinberg primes $q \not\equiv 1 \pmod{p}$. But these extra primes in the level of the form g satisfy the hypotheses of Dummigan's Theorem, so we can remove them as well. □

Corollary 1.2. *Let $f \in S_k(\Gamma_0(N), \epsilon)$, $k \geq 2$ be a newform which has no complex multiplication or 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 our form does not have complex multiplication or inner twists, by Ribet's result ([Rib85], Theorem 3.1) the image is big modulo p for all but finitely many primes p. We avoid the primes without big image as well as those smaller than the weight. We also discard the primes p that ramify in the field of coefficients of f and the ones in the level (or the non-ordinary ones), and we are in the hypothesis of the previous Theorem. □

The proof of Theorem A follows the ideas of [Ram02]. This means that it is divided into two parts. On the one hand we need to add auxiliary primes that allow us to convert the problem of lifting a global representation into the one of lifting many local ones. On the other hand, we need

to solve the local problems. Following the logical structure of [Ram02], we deal with the local considerations first.

In this case, we essentially have to prove Proposition 1.6 of [Ram02] in our setting. 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 $N_\ell \subseteq \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ of certain dimension such that its elements preserve the reductions of N_ℓ, i.e. such that whenever ρ_m is the reduction of some $\tilde{\rho} \in C_\ell$ modulo p^m and $u \in N_\ell$ then $(1 + p^{m-1}u)\rho_m$ is the reduction of some other $\tilde{\rho}' \in C_\ell$. In order to get the full statement of our Theorem A we also need all the deformations in C_ℓ to be isomorphic when restricted to I_ℓ.

Once we picked these local deformations classes, we need to construct two auxiliary sets of primes, Q_1 and Q_2 (these are Ramakrishna's Q and T) together with their respective sets C_q and subspaces N_q as for the primes in P, that satisfy the following conditions:

- The set Q_1 morally has two main properties (see Fact 16 [Ram02]): it kills the global obstructions, i.e. is such that $Ш^1_{S\cup Q_1}((Ad^0\bar{\rho})^*) = 0$ and therefore $Ш^2_{S\cup Q_1}(Ad^0\bar{\rho}) = 0$, and the inflation map
$$\mathrm{H}^2(G_S, Ad^0\bar{\rho}) \to \mathrm{H}^2(G_{S\cup Q_1}, Ad^0\bar{\rho}),$$
is an isomorphism.
- The set Q_2 gives an isomorphism
$$\mathrm{H}^1(G_{S\cup Q_1\cup Q_2}, Ad^0\bar{\rho}) \to \bigoplus_{\ell\in S\cup Q_1\cup Q_2} \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})/N_\ell.$$
without adding global obstructions, i.e. $Ш^2_{S\cup Q_1\cup Q_2} = 0$.

These auxilliary primes are essentially the same as in [Ram02], we use the same sets C_q and subspace N_q. We only need to have a little extra care when proving that $\rho_n|_{G_q}$ is the reduction of some $\tilde{\rho} \in C_q$ for every $q \in Q_1 \cup Q_2$.

Once we have solved the local problems and found the auxiliary primes, the inductive method starts to work. The key observation here is that this inductive step only depends on hypotheses about the reduction mod p of our representation, which tells us that no matter at which power of p we start lifting, it will work perfectly.

The inductive argument works as follows: in virtue of the isomorphisms between local and global second cohomology groups, 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 local first cohomology groups modulo N_ℓ, we can find an element $u \in \mathrm{H}^1(G_\mathbb{Q}, Ad^0\bar{\rho})$ 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. From here we can repeat the process of lifting and adjusting indefinitely, finally getting a lift to $W(\mathbb{F})$.

Finally, to get Theorem A we need to prove modularity for the constructed representation, this follows from the appropriate modularity lifting theorem, using the conditions we chose for the representation at p.

Theorem B is an immediate consequence of Theorem A. The fact $f \neq g$ will follow from the fact that both forms have different levels, as the auxilliary primes involved necessarily ramify. If there are no auxilliary primes, we add a ramified prime into the set P.

Notations and conventions: throughout this work we will denote by $G_\mathbb{Q}$ the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If ℓ is a prime, we denote by G_ℓ a decomposition group of ℓ inside $G_\mathbb{Q}$. We will denote by $\mathbb{F}$ a finite field of characteristic p and by $W(\mathbb{F})$ its ring of Witt vectors.

By ρ_n we will denote a continuous representation
$$\rho_n : G_\mathbb{Q} \to \mathrm{GL}_2(W(\mathbb{F})/p^n).$$

By $\tilde{\rho}$ we will always denote a continuous representation with coefficients in $W(\mathbb{F})$ ramifying at finitely many primes and by $\overline{\rho}$ its reduction modulo p. If ω is a character from $G_{\mathbb{Q}}$ to $\mathbb{F}$, we denote by $\tilde{\omega}$ its Teichmuller 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 determinant $\tilde{\omega}\chi^k$. If ρ is any continuous representation, we denote by $\mathbb{Q}(\rho)$ 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 $Ad^0\bar{\rho}$ ramify at the same set of primes S.

Acknowledgments: Special thanks go to Luis Dieulefait, for proposing us the problem of Corollary 1.2 (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 the article. We also would like to thank Gabor Wiese for many corrections and comments, and Panagiotis Tsaknias for pointing out the application of Theorem A to Corollary 1.1. Finally, we would like to thank John Jones and Bill Allombert for helping us with the computational part of the example.

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 [CSS97], Section 2).

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

- **Principal Series:** $\rho \simeq \left(\begin{smallmatrix} \phi & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *or* $\rho \simeq \left(\begin{smallmatrix} 1 & \psi \\ 0 & 1 \end{smallmatrix}\right)$.
- **Steinberg:** $\rho \simeq \left(\begin{smallmatrix} \chi & \mu \\ 0 & 1 \end{smallmatrix}\right)$, *where $\mu \in \mathrm{H}^1(G_\ell, \mathbb{F}(\chi))$ and $\mu|_{I_\ell} \neq 0$.*
- **Induced:** $\rho \simeq \mathrm{Ind}_{G_M}^{G_\ell}(\xi)$, *where $M/\mathbb{Q}_\ell$ is a quadratic extension and $\xi : G_M \to \mathbb{F}^\times$ is a character not equal to its conjugate under the action of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$.*

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

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

The same classification applies for representations $\tilde{\rho} : G_\ell \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$, but since we need to study reductions modulo powers of a prime, we need to look at representations with integer coefficients modulo $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$ equivalence. Let L be the coefficient field of $\tilde{\rho}$, $\mathcal{O}_L$ its ring of integers, and π be a local uniformizer. Also let $\mu \in \mathrm{H}^1(G_\ell, \mathbb{Z}_p(\chi))$ be a generator of such $\mathbb{Z}_p$-module.

Proposition 2.2. *Let $\tilde{\rho} : G_\ell \to \mathrm{GL}_2(\overline{\mathbb{Z}_p})$ 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:** $\tilde{\rho} \simeq \left(\begin{smallmatrix} \phi & \pi^n(\phi-1) \\ 0 & 1 \end{smallmatrix}\right)$, *with $n \in \mathbb{Z}_{\leq 0}$ satisfying $\pi^n(\phi-1) \in \overline{\mathbb{Z}_p}$ or $\tilde{\rho} \simeq \left(\begin{smallmatrix} 1 & \psi \\ 0 & 1 \end{smallmatrix}\right)$.*
- **Steinberg:** $\tilde{\rho} \simeq \left(\begin{smallmatrix} \chi & \pi^n\mu \\ 0 & 1 \end{smallmatrix}\right)$, *with $n \in \mathbb{Z}_{\geq 0}$.*
- **Induced:** *There exists a quadratic extension $M/\mathbb{Q}_\ell$ and a character $\xi : G_M \to \overline{\mathbb{Z}_p}^\times$ not equal to its conjugate under the action of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$ such that $\tilde{\rho} \simeq \langle v_1, v_2 \rangle_{\mathcal{O}_L}$, where for σ a generator of $\mathrm{Gal}(M/\mathbb{Q}_p)$ and $\tau \in G_M$, the action is given by*

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

or

$$\tilde{\rho}(\tau) = \begin{pmatrix} \xi(\tau) & \frac{\xi(\tau)-\xi^\sigma(\tau)}{\pi^n} \\ 0 & \xi^\sigma(\tau) \end{pmatrix} \qquad \text{and} \qquad \tilde{\rho}(\sigma) = \begin{pmatrix} -a & \frac{\xi(\sigma^2)-a^2}{\pi^n} \\ \pi^n & a \end{pmatrix}$$

where ξ^σ is the character of G_M defined by $\xi^\sigma(g) = \xi(\sigma g \sigma^{-1})$ and $a \in \mathcal{O}_L^\times$.

Proof. We first consider the case where $\tilde{\rho}$ is irreducible over $\overline{\mathbb{Q}_p}$. In this case the representation is induced, and in the coefficient field L, the canonical basis is $\{v_1, v_2\}$, where $v_2 = \sigma(v_1)$ for σ a generator of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$. Let T be an invariant lattice for $\tilde{\rho}$. There exists a least $n \in \mathbb{Z}$ such that $w_1 = \pi^n v_1 \in T$. Rescaling T we can assume that $n = 0$ (rescaling the lattice does not affect the representation). Since $\sigma(T) \subseteq T$, $v_2 = \sigma(v_1) \in T$. Since $\sigma(v_2) = \xi(\sigma^2)v_1$, with $\xi(\sigma^2) \in \mathcal{O}_L^\times$, 0 is also the least integer such that $\pi^n v_2 \in T$, and therefore $\langle v_1, v_2\rangle_{\mathcal{O}_L} \subseteq T$. If this inclusion is an equality we are in the first case of our classification.

Otherwise, we can extend v_1 to a basis of T by adding a vector $w \in T$ such that $w \notin \langle v_1, v_2\rangle_{\mathcal{O}_L}$. We can write this element as $w = \alpha v_1 + \beta v_2$. Notice that necessarily $v_\pi(\alpha) = v_\pi(\beta) < 0$. Changing v_1 and v_2 by a unit we can assume that $w = \pi^{-n}(-av_1 + v_2)$, with $n < 0$. Using $\sigma(v_1) = v_2$ and $\sigma(v_2) = \xi(\sigma^2)v_1$ we can compute the matrix of σ in the basis v_1, w and we get

$$\tilde{\rho}(\sigma) = \begin{pmatrix} -a & \pi^{-n}(\xi(\sigma^2) - a^2) \\ \pi^n & a \end{pmatrix}.$$

The action of inertia follows from a similar computation.

On the other hand, ff $\tilde{\rho}$ is reducible over $\overline{\mathbb{Q}_p}$, we can chose an eigenvector inside our lattice, and extend it to a basis so that our representation is of the form (up to twist)

$$\tilde{\rho} \simeq \left(\begin{smallmatrix} \phi & * \\ 0 & 1 \end{smallmatrix}\right).$$

If ϕ is trivial, then $*$ is an additive character, and we are in the first case. Otherwise, if $\tilde{\rho}$ 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 $\left(\begin{smallmatrix} \chi & \mu \\ 0 & 1 \end{smallmatrix}\right)$, but an easy computation shows that such a representation is of the desired form as well. □

Remark. In the Principal Series case, if we put $n = 0$ we get $\tilde{\rho} \simeq \left(\begin{smallmatrix} \phi & \phi^{-1} \\ 0 & 1 \end{smallmatrix}\right)$, which is equivalent to $\left(\begin{smallmatrix} \phi & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we will make repeated use of this last representative for this class.

Now we want to study the possible reductions from types of $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$-equivalent representations to types of representations with coefficients in $\mathrm{GL}_2(\overline{\mathbb{F}_p})$. Although this is well known to experts, and most of the claims are in [Car89], 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 2.3. *Let $\xi : G_\ell \to \overline{\mathbb{Q}_p}^\times$ 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. Whenever an element $g \in I_\ell$ satisfies that $\xi(g) \neq 1$ and $\overline{\xi}(g) = 1$ we necessarily have $\xi(g)^{\ell-1} = 1$.

Proposition 2.4. *Let $\tilde{\rho}$ be as above, then we have the following types of reduction:*

- *If $\tilde{\rho}$ is Principal Series, then $\overline{\rho}$ is Principal Series or Steinberg, and the latter occurs only when $\ell \equiv 1 \pmod{p}$.*
- *If $\tilde{\rho}$ is Steinberg, then $\overline{\rho}$ is Steinberg or Principal Series, and the latter occurs only when $\overline{\rho}$ is unramified.*
- *If $\tilde{\rho}$ 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 $\tilde{\rho}$ 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:

- *$\tilde{\rho}$ Principal Series:* in this case $\tilde{\rho} \simeq \left(\begin{smallmatrix} \phi & \lambda(\phi-1) \\ 0 & 1 \end{smallmatrix}\right)$ 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 2.3) that $\ell \equiv 1 \pmod{p}$.

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

- $\tilde{\rho}$ *Steinberg:* in this case $\tilde{\rho} \simeq \left(\begin{smallmatrix} \chi & \lambda u \\ 0 & 1 \end{smallmatrix}\right)$ 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.
- $\tilde{\rho}$ *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.

  Now suppose that $\overline{\xi}$ does descend and, for a moment, that $\overline{\rho}$ ramifies (which implies, by assumption, that $Ad^0\overline{\rho}$ 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 $M/\mathbb{Q}_\ell$.

  Now, if $\overline{\rho}$ is Principal Series, then ϵ has to be ramified, as we are assuming that $Ad^0\overline{\rho}$ 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 $\xi : G_M \to \mathbb{Z}_p^\times$ that does not extend to $G_{\mathbb{Q}}$ then its reduction does not extend to $G_{\mathbb{Q}}$ either. Then the only possibility left to study is when $\overline{\rho}$ is Steinberg. Observe that if this is the case, looking at the semisimplifications we see that $\epsilon = \chi$, which only happens when $M/\mathbb{Q}_\ell$ is unramified and $\ell = -1 \pmod{p}$. This finishes the case where $\overline{\rho}$ is ramified.

  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 2.3, 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 $\ell \equiv -1 \pmod{p}$.

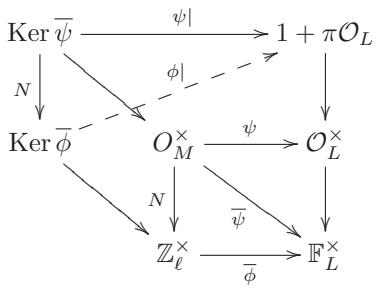
□

Lemma 2.5. *Let $M/\mathbb{Q}_\ell$ be a quadratic ramified extension and $\xi : G_M \to \overline{\mathbb{Z}_p}^\times$ 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 $\sigma \in G_\ell$ be an element not in G_M and define $\xi^\sigma(x) = \xi(\sigma x \sigma^{-1})$. We know that ξ extends to G_ℓ if and only if $\xi = \xi^\sigma$.

Via local class field theory, the character ξ corresponds to a character ψ defined over $M^\times$ and ξ^σ corresponds to $\psi^\sigma(x) = \psi(\sigma(x))$, 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 $\psi = \psi^\sigma \pmod{\pi}$ and we want to prove that $\psi = \psi^\sigma$. 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

$$\begin{array}{ccccc}
\operatorname{Ker}\overline{\psi} & \longrightarrow & \frac{\operatorname{Ker}\overline{\psi}}{\operatorname{Ker}\overline{\psi}\cap(1+\ell\mathbb{Z}_\ell)} & \xrightarrow{\psi|} & 1+\pi O_L \\
\Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle f} & \nearrow_{\phi|} & \\
\operatorname{Ker}\overline{\phi} & \longrightarrow & \frac{\operatorname{Ker}\overline{\phi}}{\operatorname{Ker}\overline{\phi}\cap(1+\ell\mathbb{Z}_\ell)} & &
\end{array}$$

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 $\sqrt{\ }:1+\pi\mathcal{O}_L\to 1+\pi\mathcal{O}_L$ 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 $\operatorname{Ker}\overline{\phi}$.

Now we want to prove that ψ factors through the norm map. Define $\tau(x)=\psi^\sigma\psi^{-1}$. We know that $\tau:\mathcal{O}_M^\times\to 1+\pi\mathcal{O}_L$ and that $\tau(\operatorname{Ker}\overline{\xi})=1$. So it factors through $\overline{\tau}:\mathcal{O}_M^\times/\operatorname{Ker}\overline{\psi}\to 1+\pi\mathcal{O}_L$, 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 τ must be trivial and therefore $\psi=\psi^\sigma$ when restricted to $\mathcal{O}_M^\times$. In order to deduce $\psi=\psi^\sigma$ from this, we only need to check it for the uniformizer, which is $\sqrt{\delta p}$ with $\delta=\pm1$. We have:

$$\psi^\sigma(\sqrt{\delta p})=\psi(\sigma(\sqrt{\delta p}))=\psi(-\sqrt{\delta p})=\psi(-1)\psi(\sqrt{\delta p})=\psi(\sqrt{\delta p}).$$

The last inequality follows from $\psi(-1)=\phi(N(-1))=\phi(1)=1$, because $-1\in\mathcal{O}_M^\times$. We have proved that ξ extends to G_ℓ. □

Remark. 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 2.6. *Let $\varrho:G_\ell\to\mathrm{GL}_2(W(\mathbb{F}))$ be a continuous representation.*

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

Proof. For the first case, assume that $\overline{\varrho}^{ss}$ is unramified. Then $\overline{\phi}=1$ which by the remark following Lemma 2.3 implies that $\ell\equiv 1 \pmod p$ and $\phi(\tau_\ell)$ has order a power of p. Therefore the eigenvalues of $\varrho(\tau_\ell)$ 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 one, assume that $\overline{\varrho}^{ss}$ is unramified. Then necessarily $\overline{\xi}=\overline{\xi^\sigma}$, implying that the character $\psi=\xi/\xi^\sigma$ loses all of its ramification when reduced. Again by the remark following Lemma 2.3 this implies that $\psi(\tau_\ell)$ has order a power of p implying that it generates a totally ramified extension of degree at least $p-1>2$. But $\psi(\tau_\ell)$ is the quotient between the eigenvalues of $\varrho(\tau_\ell)$, 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 $d_i=\dim \mathrm{H}^i(G_\ell,Ad^0\bar\rho)$ for $i=1,2$. The strategy in each case is as follows: we first compute d_0 and d_0^* (where $d_i^*=\dim \mathrm{H}^i(G_\ell,(Ad^0\bar\rho)^*)$). By local Tate duality $d_2=d_0^*$ and then we can derive d_1 from the local Euler-Poincare characteristic (which is zero). We do such computation in each case of the classification of mod p representations by choosing a good basis for each space.

Ramified Principal Series case: in this case we have $\overline{\rho}=\left(\begin{smallmatrix}\phi & 0\\ 0 & 1\end{smallmatrix}\right)$ with ϕ a ramified multiplicative character. It easily follows that $Ad^0\bar\rho\simeq\mathbb{F}(1)\oplus\mathbb{F}(\phi)\oplus\mathbb{F}(\phi^{-1})$. As ϕ is ramified, $\mathbb{F}(\phi)$ (resp. $\mathbb{F}(\phi^{-1})$) is not isomorphic to $\mathbb{F}(1)$ 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: in this case we need to do the computations by hand. Considering the basis $\{e_{01}, e_{10}, e_{00}+e_{11}\}$ of the space of matrices with trace zero and explicitly computing the action of $Ad^0\bar{\rho}$ on them, we derive the values of the numbers d_i, which are:

(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 [Ram02], Lemma 4)

Lemma 3.1. *Let $M/\mathbb{Q}_\ell$ a quadratic extension and $\overline{\rho} : G_\ell \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_p})$ 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 $Ad^0\bar{\rho} \simeq A_1 \oplus A_2$, with A_i an absolutely irreducible G_ℓ-module of dimension i and $\mathrm{H}^0(G_\ell, Ad^0\bar{\rho}) = 0$. Moreover $\mathrm{H}^2(G_\ell, Ad^0\bar{\rho}) = 0$ 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) $\overline{\rho}(\mathrm{Frob}_p) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
In this case $Ad^0\bar{\rho} \simeq \mathbb{F}^3$ 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) $\overline{\rho}(\mathrm{Frob}_p) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\alpha \not\equiv 1 \pmod p$.
We have that $Ad^0\bar{\rho} \simeq \mathbb{F} \oplus \mathbb{F}(\phi) \oplus \mathbb{F}(\phi^{-1})$, with $\phi \neq 1$ and $\phi = \chi$ only if $\alpha \equiv \ell \pmod p$. Again, we need to distinguish between 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 $d_1 = 1$.

(c) $\overline{\rho}(\mathrm{Frob}_p) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.
Here we do the computations by hand and establish 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 $\overline{\rho}$ (containing ρ_ℓ) and a subspace $N_\ell \subseteq \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ of dimension $d_1 - d_2$ such that $\overline{\rho}$ can be successively deformed to an element of C_ℓ by deforming from $W(\mathbb{F})/p^s$ to $W(\mathbb{F})/p^{s+1}$ with adjustments at each step made only by a multiple of an element $h \notin N_\ell$. In order to get the full statement of our theorem, we have to take the extra care of picking the set C_ℓ such that all its elements agree up to isomorphism in the inertia group with ρ_ℓ.

Notice that it is enough to do this for one representative of each of the possible types of $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$-equivalence for ρ_ℓ, as we can always pick a basis for ρ_n for which it is the reduction of one of those representatives. The only extra care we need to take is making sure that whenever we pick a set $\mathbb{C}_\ell$, the deformations that belong to it have all coefficients in $W(\mathbb{F}))$ and not in a bigger extension of $\mathbb{Q}_p$. The potential issue that this may bring is that sometimes we cannot use the representatives of $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$-equivalence classes we defined above and need to translate our calculations to $W(\mathbb{F})$.

We classify the selection of the sets C_ℓ according to the type of $\overline{\rho}$, considering for each one, all the possible types for ρ_ℓ.

Case 1: $\overline{\rho}$ is ramified Principal Series. When $\overline{\rho}$ is ramified Principal Series, we have seen that 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 $\rho_\ell \simeq \left(\begin{smallmatrix} \phi & \pi^n(\phi-1) \\ 0 & 1 \end{smallmatrix}\right)$ with $n \leq 0$ such that $\pi^n(\phi-1)$ lies in $\overline{\mathbb{Z}_p}$. Observe that if $n \neq 0$, then $\pi \mid (\phi-1)$ and therefore its reduction is not ramified Principal Series (the residual case $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ is unramified or Steinberg according to our classification). Then $\rho_\ell \simeq \begin{pmatrix} \phi & 0 \\ 0 & 1 \end{pmatrix}$ 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 $d_2 = 0$ so we must take $N_\ell = \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ the full cohomology group so there is no possible choice at each step and C_ℓ must be the full set of deformations to characteristic zero. Notice that this is the only possible choice whenever $d_2 = 0$ and $\ell \neq p$ and in this case we have to check that any lift of $\overline{\rho}$ to $W(\mathbb{F})/p^s$ is the reduction of a characteristic zero one, but this is automatic as $d_2 = 0$ so the problem is unobstructed.

In order 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 $n : G_\ell \to G_\ell/I_\ell \simeq \hat{\mathbb{Z}} \to \mathbb{Z}/p\mathbb{Z}$, then the element

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

generates $\mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ and this implies that every lift is Principal Series, as the set $\lambda h \cdot \psi_s$, where ψ is the Teichmuller 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 we need to choose a one dimensional subspace N_ℓ and a set of deformations C_ℓ to $W(\mathbb{F})$. Observe that the isomorphism between ρ_ℓ and the representative of its $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$-equivalence class may not realize over $W(\mathbb{F})$.

If the image of ψ_1 lies in $W(\mathbb{F})$, then the isomorphism does realize over $W(\mathbb{F})$. In that case, observe that the element h defined above lies inside $\mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$. Let $N_\ell = \langle h \rangle$, and $C_\ell = \left\{ \begin{pmatrix} \psi_1\gamma & 0 \\ 0 & \psi_2\gamma^{-1} \end{pmatrix} : \gamma \text{ unramified character} \right\}$.

We claim that this choice verifies the hypotheses. Clearly $\rho_\ell \in C_\ell$, and given any $h' \notin N_\ell$, the full $\mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ is generated by h and h'. Then for any mod p^s deformation $\tilde{\rho}$ of $\overline{\rho}$ there is an element $\lambda_1 h + \lambda_2 h' \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ such that $(\lambda_1 h + \lambda_2 h')\tilde{\rho}$ lies in C_ℓ. But the action of any multiple of h preserves the elements of C_ℓ, so $\lambda_2 h'\tilde{\rho}$ already lies in C_ℓ. Note that as in the previous case, 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 need to use a canonical form for ρ_ℓ over $W(\mathbb{F})$. Assume that $\psi_1(\sigma_\ell) = \alpha$ and $\psi_2(\sigma_\ell) = \beta$, 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 $\rho_\ell(\sigma_\ell) = \left(\begin{smallmatrix} 0 & -\alpha\beta \\ 1 & \alpha+\beta \end{smallmatrix}\right)$. Then we can essentially use the same sets and subspaces as in the previous case but conjugated by C.

Let $N_\ell = \langle (\alpha-\beta) ChC^{-1} \rangle$, where h is the element defined before, and C_ℓ 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 $\gamma : G_\ell \to \overline{\mathbb{Z}_p}$ 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 $\tilde{\rho}$ is the reduction of some element in C_ℓ and $u \in N_\ell$ then $(1 + p^n u)\tilde{\rho}$ is again the reduction of an element of C_ℓ. Therefore the same reasoning as before shows that N_ℓ and C_ℓ satisfy our hypotheses.

Remark. Whenever we construct a set C_ℓ and subspace N_ℓ such that N_ℓ preserves the reductions of C_ℓ (i.e. whenever $\tilde{\rho}$ is the reduction of some element of C_ℓ and $u \in N_\ell$, $u \cdot \tilde{\rho}$ is reduction of some element of C_ℓ as well) the proof is exactly the same. In the next cases the same phenomena will occur.

Case 2: $\overline{\rho}$ is Steinberg. If $\overline{\rho}$ is of Steinberg type then Proposition 2.4 and Proposition 2.6 imply that ρ_ℓ can only be Steinberg.

(1) If $\ell \not\equiv \pm 1 \pmod{p}$, by the previous section results, $d_0 = d_1 = d_2 = 0$, implying there is only one deformation at each p^n. We take $C_\ell = \{\rho_\ell\}$.
(2) If $\ell \equiv -1 \pmod{p}$, by the previous section results, $d_1 = d_2 = 1$ and $d_0 = 0$, so $N_\ell = \{0\}$ and we have the full $\mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ available to adjust at every step. Then we take $C_\ell = \{\rho_\ell\}$.
(3) If $\ell \equiv 1 \pmod{p}$, we take the element $j \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ given by 0 at the wild inertia subgroup and by
$$j(\sigma_\ell) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ , \ j(\tau_\ell) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$
where σ_ℓ is a Frobenius element and τ_ℓ a tame inertia generator (recall these two generate G_ℓ/W_ℓ, where W_ℓ is the wild inertia, subject to the relationship $\sigma\tau\sigma^{-1} = \tau^\ell$). Let $N_\ell = \langle j \rangle$ and C_ℓ the set of lifts ρ satisfying
$$\rho(\sigma_\ell) = \begin{pmatrix} \ell & * \\ 0 & 1 \end{pmatrix} \text{ and } \rho(\tau_\ell) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$
This set contains all the extensions $\tilde{\rho_\ell}$ of ρ_ℓ to the decomposition group, 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 N_ℓ is of codimension 1 inside a space of dimension 1, hence $N_\ell = \{0\}$. We take $C_\ell = \{\rho_\ell\}$. Since we can adjust at every step by a multiple of a given element $h \notin \{0\}$, and $d_1 = 1$, we can adjust at each step by any element of $\mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ to modify ρ_n as we want.
(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. This lift must be the reduction of ρ_ℓ, so there is nothing to adjust.

Case 4: $\overline{\rho}$ is unramified. We need to define the sets C_ℓ for the primes at which ρ_n ramifies and $\overline{\rho}$ does not. By Proposition 2.6 this can only happen when ρ_ℓ is Steinberg.

We have that $\rho_\ell = \left(\begin{smallmatrix} \chi & * \\ 0 & 1 \end{smallmatrix}\right)$, with $*|_{I_\ell} \neq 0 \pmod{p^n}$. The sets C_ℓ we will pick depend on the image of σ_ℓ. Recall that the eigenvalues of $\overline{\rho}(\sigma_\ell)$ are 1 and ℓ.

(1) If $\overline{\rho}(\sigma_\ell) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, necessarily $\ell \equiv 1 \pmod{p}$ implying $d_1 = 6$ and $d_2 = 3$ and therefore we need a subspace of dimension 3, preserving a family of deformations C_ℓ. In the previous cases, we have built sets C_ℓ of deformations of ρ_n that depend on $d_2 - d_1$ parameteres, 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 cohomological trivial for the residual representation, but give isomorphic lifts modulo big powers of p, as in Section 4 of [RH08]. Let C_ℓ be the set of deformations of ρ_n satisfying:
$$\rho(\sigma_\ell) = \begin{pmatrix} \ell & * \\ 0 & 1 \end{pmatrix} \text{ and } \rho(\tau_\ell) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$
Observe that this family depends on two parameters and is clearly preserved by the elements $u_1, u_2 \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ given by
$$u_1(\sigma_\ell) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ , \ u_1(\tau_\ell) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$
and

$$u_2(\sigma_\ell) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \ , \ u_2(\tau_\ell) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

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

$$\rho_n(\sigma_\ell) = \begin{pmatrix} \ell & x \\ 0 & 1 \end{pmatrix} \text{ and } \rho_n(\tau_\ell) = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix},$$

with $y \neq 0$. There exists an element $v \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ that satisfies that whenever ρ_m is the reduction modulo p^m of some element in C_ℓ then $(1+p^{m-1}v)\rho_m$ is the same deformation as ρ_m. The element v will depend on the valuations of x, y and $\ell-1$. As we mentioned in the introduction of this Section, we only need to do this for $m \geq n+1$.

Lemma 4.1. *There exists an element $v \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ such that whenever ρ_m is the reduction modulo p^m of some element in C_ℓ, with $m \geq n+1$, then $(1+p^{m-1}v)\rho_m$ is the same deformation as ρ_m.*

Proof. The proof is divided into several cases, we first define $g_1, g_2, g_3 \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ as

$$g_1(\sigma_\ell) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \ , \ g_1(\tau_\ell) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$g_2(\sigma_\ell) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ , \ g_2(\tau_\ell) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

and

$$g_3(\sigma_\ell) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \ , \ g_3(\tau_\ell) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

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 v and a matrix C congruent to the identity modulo p such that $C^{-1}\rho_m C = (1+p^{m-1})\rho_m$. 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 left to the reader to check that $C^{-1}\rho_m C = (1+p^{m-1})\rho_m$ in each of them.

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

□

We end this case by taking C_ℓ as above and $N_\ell = \langle u_1, u_2, v\rangle$, for the element v of Lemma 4.1.

(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 $u \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ defined 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 $u \in \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ 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. If we allow ramification in the coefficient field then the cases ruled out by Proposition 2.6 may happen. Most of them correspond to cases like the first unramified case, where a trick like in [RH08] need 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 the remark after Lemma 5.8.

4.1. **The case $\ell = p$.** In this case we will pick C_p exactly as in [Ram02] (*local at p considerations*), with the observation that in the supersingular case, it follows from the work done in [Ram93] that the lifts picked have the same Hodge-Tate weights than 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

For constructing the sets Q_1 and Q_2 mentioned in the introduction we will work with primes $q \not\equiv \pm 1 \pmod{p}$ such that $\overline{\rho}$ is not ramified at q and $\overline{\rho}(q)$ has different eigenvalues of ratio q, i.e. $\bar{\rho}(\sigma_q) = \left(\begin{smallmatrix} qx & 0 \\ 0 & x \end{smallmatrix}\right)$ and $\bar{\rho}(\tau_q) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For these primes the cohomological dimensions are $\dim \mathrm{H}^0(G_q, Ad^0\bar{\rho}) = 1$, $\dim \mathrm{H}^1(G_q, Ad^0\bar{\rho}) = 2$ and $\dim \mathrm{H}^2(G_q, Ad^0\bar{\rho}) = 1$.

In this case, the set C_q is formed by the deformations ω such that

$$\omega(\tau_q) = \begin{pmatrix} 1 & px \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \omega(\sigma_q) = \begin{pmatrix} q & py \\ 0 & 1 \end{pmatrix}. \tag{1}$$

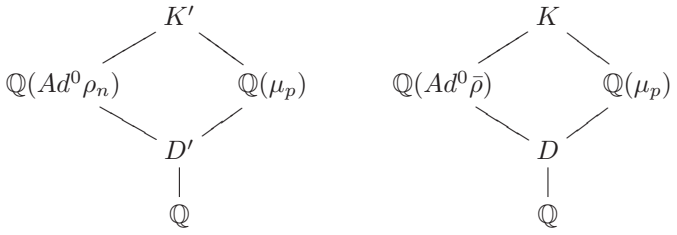
These two conditions define a tamely ramified deformation of $\overline{\rho}$. The set C_q is preserved by a subspace $N_q \subseteq \mathrm{H}^1(G_q, Ad^0\bar{\rho})$ of codimension 1 given by $j(\sigma_q) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $j(\tau_q) = \left(\begin{smallmatrix}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

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 ρ with coefficients in $W(\mathbb{F})/p^n$. Observe that, the inductive step depends only on the reduction modulo p of ρ, so we only need to check that once we set the deformation set C_q, whenever we add an auxiliary prime q together with its subspace N_q, the representation $\rho_n|_{G_q}$ is the reduction of some element in C_q, i.e. we want to prove 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 (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 [Ram02].

5.1. **Working modulo p^n.** We need to prove that there exist infinitely many auxiliary primes, that is primes q such that $q \not\equiv \pm 1 \pmod{p}$, ρ_n is unramified at q and $\rho_n(\mathrm{Frob}_q)$ has different eigenvalues of ratio q.

Following [Ram99] and [Ram02], let μ_p be a primitive p-th root of unity, $D = \mathbb{Q}(Ad^0\bar{\rho}) \cap \mathbb{Q}(\mu_p)$, $K = \mathbb{Q}(Ad^0\bar{\rho})\mathbb{Q}(\mu_p)$, $D' = \mathbb{Q}(Ad^0\rho_n) \cap \mathbb{Q}(\mu_p)$ and $K' = \mathbb{Q}(Ad^0\rho_n)\mathbb{Q}(\mu_p)$, which fit in the following diagram:



Observe that we can translate the conditions on q into the following:

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

Therefore, if we prove that there is an element $\sigma \in \mathrm{Gal}(K'/\mathbb{Q})$ such that $\sigma|_{\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})} = t \neq \pm 1$ and $\sigma|_{\mathrm{Gal}(\mathbb{Q}(Ad^0\rho_n)/\mathbb{Q})} = \overline{M}$ where M is diagonal with eigenvalues of ratio t, then we are done using Chebotarev's Theorem.

Proposition 5.1. *There is an element $c = a \times b \in \mathrm{Gal}(\mathbb{Q}(Ad^0\rho_n)/D') \times \mathrm{Gal}(\mathbb{Q}(\mu_p)/D') \simeq \mathrm{Gal}(K'/D')$ 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 is in the spirit of the arguments given in [Ram99] for finding such elements. Recall the following lemma (Lemma 3, IV-23 in [Ser89] [1])

Lemma 5.2. *Let $p \geq 5$ and $\mathbb{F}$ a finite field of characteristic p. Let $H \subseteq \mathrm{GL}_2(W(\mathbb{F}))$ a closed subgroup and $\overline{H}$ 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 $\pi : W(\mathbb{F}) \to W(\mathbb{F})/p^n$ the projection, then this follows applying the above lemma with $H = \pi^{-1}(\mathrm{Im}(\rho_n)) \subseteq W(\mathbb{F})$ which is closed as $G_{\mathbb{Q}}$ is compact . □

The following lemma gives the existence of the element c.

Lemma 5.4. *For D' the field defined above, $[D' : \mathbb{Q}] \leq 2$.*

Proof. Observe that $[\mathbb{Q}(Ad^0\rho_n) : \mathbb{Q}(Ad^0\bar{\rho})] = p^*$ which is coprime with $[\mathbb{Q}(\mu_p) : \mathbb{Q}]$. This implies that $D' = \mathbb{Q}(Ad^0\rho_n) \cap \mathbb{Q}(\mu_p) = \mathbb{Q}(Ad^0\bar{\rho}) \cap \mathbb{Q}(\mu_p)$ and $[\mathbb{Q}(Ad^0\bar{\rho}) \cap \mathbb{Q}(\mu_p) : \mathbb{Q}] = 1$ or 2 by Lemma 18 of [Ram99]

□

Proof of Proposition 5.1: Let $b \in \mathbb{F}_p^\times \subseteq \mathbb{F}^\times$ be any element such that $b^2 \neq \pm 1$. Let $\tilde{b} \in \{1, \cdots, p-1\} \subseteq W(\mathbb{F})/p^n$ be congruent to b modulo p and $M = \begin{pmatrix} \tilde{x} & 0 \\ 0 & \tilde{x}^{-1} \end{pmatrix} \in \mathrm{SL}_2(W(\mathbb{F})/p^n) \subseteq \mathrm{Im}(\rho_n)$. Then $c = (\overline{M}, b^2) \in \mathrm{Gal}(\mathbb{Q}(Ad^0\rho)/D') \times \mathrm{Gal}(\mathbb{Q}(\mu_p)/D')$ is such an element. □

Remark. The element c constructed in Proposition 5.1 is not the same as the one in [Ram99]. 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 constructed in this work 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 $Ad^0\bar{\rho}$ (as the action of our c is through this projection). To avoid confusion we denote the projection by $\tilde{c}$.

[1] Actually, Lemma 3 is stated and proved in [Ser89] for $\mathbb{F} = \mathbb{F}_p$ but the same proof holds for an arbitrary finite field of characteristic p.

Any prime q not ramified in K' such that Frob_q lies in the conjugacy class of c can be taken as an auxiliary prime. In the next subsection we are going to impose extra conditions at the auxiliary primes regarding their interaction with elements of $\mathrm{H}^1(G_{\mathbb{Q}}, Ad^0\bar{\rho})$ and $\mathrm{H}^2(G_{\mathbb{Q}}, Ad^0\bar{\rho})$.

5.2. **Properties of auxiliary primes.** We need to impose conditions to the auxiliary primes similar to the ones in Fact 16 and Lemma 14 of [Ram02]. Concretely, for non-zero elements $f \in \mathrm{H}^1(G_P, Ad^0\bar{\rho})$ and $g \in \mathrm{H}^1(G_P, (Ad^0\bar{\rho})^*)$, the auxiliary prime q should satisfy $f|_{G_q} = 0$ or $f|_{G_q} \notin N_q$ and $g|_{G_q} \neq 0$. We need to impose these conditions for many elements at the same time.

If $f \in \mathrm{H}^1(G_P, Ad^0\bar{\rho})$, then $f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(Ad^0\bar{\rho}))}$ is a morphism, so we can associate an extension $\widetilde{L_f}/\mathbb{Q}(Ad^0\bar{\rho})$ fixed by its kernel. Also let $L_f = \widetilde{L_f}K = \widetilde{L_f}(\mu_p)$. Analogously, for $g \in \mathrm{H}^1(G_P, (Ad^0\bar{\rho})^*)$ we define $M_g/\mathbb{Q}((Ad^0\bar{\rho})^*)$ as the fixed field by the kernel of $g|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}((Ad^0\bar{\rho})^*))}$. 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 $\mathrm{Gal}(M_g/\mathbb{Q})$ (as these are almost the extensions associated to the adjoint representation of $\overline{\rho}(Id + \epsilon f)$).

Let $f_1, \dots, f_{r_1}$ and $g_1, \dots, g_{r_2}$ basis for $\mathrm{H}^1(G_P, Ad^0\bar{\rho})$ and $\mathrm{H}^1(G_P, (Ad^0\bar{\rho})^*)$ 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 [Ram99].

Lemma 5.5. *Let f_i and g_j as above.*

1. *For every f_i, $\mathrm{Gal}(L_{f_i}/K) \simeq Ad^0\bar{\rho}$ as $G_{\mathbb{Q}}$-modules, and for every g_j, $\mathrm{Gal}(M_{g_j}/K) \simeq (Ad^0\bar{\rho})^*$.*
2. *$\mathrm{Gal}(L/K) \simeq \prod \mathrm{Gal}(L_{f_i}/K) \simeq (Ad^0\bar{\rho})^{r_1}$ and $\mathrm{Gal}(M/K) \simeq \prod \mathrm{Gal}(M_{g_j}/K) \simeq ((Ad^0\bar{\rho})^*)^{r_2}$. 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 [Ram99] with two remarks:

- In [Ram99] these results are proved for the representation $\widetilde{Ad}^0\bar{\rho}$, which is the descent of $Ad^0\bar{\rho}$ to its minimal field of definition. As we are assuming that $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho})$, we have that $Ad^0\bar{\rho}$ is already defined in its minimal field of definition, because of Lemma 17 of [Ram99].
- In [Ram99] these lemmas are proved for $P = S$ the set of ramification of $Ad^0\bar{\rho}$, but the same proofs work for any $P \supseteq S$.

□

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

Proposition 5.6. *Let $q \in \mathbb{Q}$ be a prime, $f \in \mathrm{H}^1(G_P, Ad^0\bar{\rho})$ and $g \in \mathrm{H}^1(G_P, (Ad^0\bar{\rho})^*)$.*

1. *If Frob_q lies in the conjugacy class of $1 \rtimes \tilde{c} \in \mathrm{Gal}(L_f/\mathbb{Q})$ then $f|_{G_q} = 0$. The same holds for g and $\mathrm{Gal}(M_g/\mathbb{Q})$.*
2. *There are nontrivial elements $\alpha \in Ad^0\bar{\rho}$ 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 $\beta \in (Ad^0\bar{\rho})^*$ 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 [Ram99], noting that in our setting $Ad^0\bar{\rho} = \widetilde{Ad}^0\bar{\rho}$, so the proof of the existence of α and β is almost trivial. □

Corollary 5.7. *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

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

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 want the same to hold for ρ_n, i.e. to find primes q satisfying the same conditions plus $\rho_n(\mathrm{Frob}_q)$ to have different eigenvalues of ratio q. As we mentioned before, any q such that $\mathrm{Frob}_q \in \mathrm{Gal}(K'/\mathbb{Q})$ 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 $\mathrm{Gal}(K'F/\mathbb{Q})$. In order to prove this, we need the following lemma.

Lemma 5.8. *$K' \cap F = K$.*

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 on the classes of matrices in $\mathrm{Im}(\rho_n)$ which are trivial in $\mathrm{PGL}_2(\mathbb{F})$, i.e. $\mathcal{H} = \mathrm{Im}(Ad^0\rho_n) \cap \mathrm{Ker}(\pi_1)$. Recall that our hypotheses imply $\mathrm{PSL}_2(W(\mathbb{F})/p^n) \subseteq \mathrm{Im}(Ad^0\rho_n) \subseteq \mathrm{PGL}_2(W(\mathbb{F})/p^n)$, 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 $\mathrm{Gal}(F/K) \simeq (Ad^0\bar{\rho})^r \times (Ad^0\bar{\rho}^*)^s$ as $\mathbb{Z}[G_\mathbb{Q}]$-module and by Lemma 7 of [Ram99], this is its decomposition as $\mathbb{Z}[G_\mathbb{Q}]$ simple modules. This implies that if $K' \cap F \neq K$ then $Ad^0\bar{\rho}$ or $(Ad^0\bar{\rho})^*$ appear as a quotient of $\mathrm{Gal}(K'/K)$.

Assume that $K' \cap F \neq K$ and that there is a surjective morphism $\varpi : \mathcal{H} \to Ad^0\bar{\rho}$. Let $\pi_2 : \mathrm{PGL}_2(W(\mathbb{F})/p^n) \to \mathrm{PGL}_2(W(\mathbb{F})/p^2)$ and let $\mathcal{N} = \ker(\pi_2) \subset \mathcal{H}$. We claim that $\varpi(\mathcal{N}) = 0$. For this, observe that 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

$$\varpi(Id + p^2M) = \varpi((Id + pN)^p) = p\varpi(Id + pN) = 0.$$

This implies that ϖ factors through $\mathrm{Gal}(\mathbb{Q}(Ad^0\rho_2)/K)$, where $Ad^0\rho_2$ is the reduction mod p^2 of $Ad^0\rho_n$. Since $\#\mathrm{Gal}(\mathbb{Q}(Ad^0\rho_2)/K) = \#(\mathrm{Im}(Ad^0\rho_2) \cap \mathrm{Ker}(\pi_1)) \leq (\#\mathbb{F})^3$ and $\#Ad^0\bar{\rho} = (\#\mathbb{F})^3$ we necessarily have $\mathrm{Gal}(\mathbb{Q}(Ad^0\rho_2)/\mathbb{Q}) = \mathrm{Gal}(L_f/\mathbb{Q})$ for some $f \in \mathrm{H}^1(G_\mathbb{Q}, Ad^0\bar{\rho})$. But this cannot happen since it would imply that the image of $Ad^0\rho_2$ 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 $\pi : \mathcal{H} \to (Ad^0\bar{\rho})^*$ works the same. □

Remark. As we mentioned before, this global argument does not adapt to the cases when the coefficient field is ramified. Specifically, Lemma 5.8 above in no longer true if we allow the coefficients to ramify, as the extension corresponding to $Ad^0\rho_2$ corresponds to an element of $\mathrm{H}^1(G_\mathbb{Q}, Ad^0\bar{\rho})$. Then we cannot apply Chebotarev's Theorem to find auxiliary primes which are nontrivial in the element of the cohomology corresponding to $Ad^0\rho_2$, so we do not get an isomorphism between local and global deformations.

Proposition 5.9. *For any $\tau \in \mathrm{Gal}(L/K)$ as above we have that*

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

is a surjection.

Proof. This is essentially Proposition 10 of [Ram02], up to the fact that we ask a condition on $\mathrm{Gal}(K'/\mathbb{Q})$ rather than $\mathrm{Gal}(K/\mathbb{Q})$. Nevertheless, the same proof applies as the main argument is that for any $g \in \mathrm{H}^1(G_{P\cup T_\tau}, (Ad^0\bar{\rho})^*)$ there are primes $q \in T_\tau$ such that $g|_{G_q} \neq 0$ and this is Proposition 5.6. □

6. Proof of main theorems

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

- *The image is big, i.e. $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{Im}(\overline{\rho_n})$.*
- *ρ_n is odd.*
- *The restriction $\overline{\rho_n}|_{G_p}$ is not twist equivalent to the trivial representation nor the indecomposable unramified representation given by $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$.*

Let P be a finite set of primes containing S, and for every $\ell \in P$, $\ell \neq p$, fix a deformation $\rho_\ell : G_\ell \to W(\mathbb{F})$ of $\rho_n|_{G_\ell}$. At the prime p, let ρ_p be a deformation 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 $\ell \in P$,*
- *$\rho|_{G_q}$ is a ramified representation of Steinberg type for every $q \in Q$.*

Proof. Once we have all the ingredients, the proof mimics that of Theorem 1 of [Ram02]. Let $r = \dim_{\mathbb{F}} Ш^2_P(Ad^0\bar{\rho}) = \dim_{\mathbb{F}} Ш^1_P((Ad^0\bar{\rho})^*)$, and let $\{g_1, \dots, g_r\}$ be a basis of $Ш^1_P((Ad^0\bar{\rho})^*)$. Let $\{f_1, \dots, f_r\}$ be a linearly independent set in $\mathrm{H}^1(G_P, Ad^0\bar{\rho})$. For each $i = 1, \dots, r$ let q_i be such that:

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

Such primes exists in virtue of Corollary 5.7 and Lemma 5.8. Let $Q_1 = \{q_1, \dots, q_r\}$ so that $Ш^2_{P\cup Q_1}(Ad^0\bar{\rho}) = 0 = Ш^1_{P\cup Q_1}((Ad^0\bar{\rho})^*)$. With this choice, the inflation map $\mathrm{H}^1(G_P, Ad^0\bar{\rho}) \to \mathrm{H}^1(G_{P\cup Q_1}, Ad^0\bar{\rho})$ is an isomorphism by the same dimension counting as in the proof of Fact 16 ([Ram02]). As mentioned in the introduction, we need to pick the set of primes Q_2 such that the map

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

is an isomorphism. Recall that once we achieved $Ш^2_{P\cup Q_1} = 0$, no set of extra primes we consider adds new global obstructions.

The way to construct such set is as follows: take a basis $\{f_1, \dots, f_d\}$ of the preimage under the restriction map $\mathrm{H}^1(G_P, Ad^0\bar{\rho}) \to \oplus_{l\in P} \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ of the set $\oplus_{\ell\in P} N_\ell$. By Lemma 12 ([Ram02]), $r \geq d$. For $r+1 \leq i \leq d$, 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. By Proposition 5.9, the map $\mathrm{H}^1(G_{S\cup Q_1\cup T_i}, Ad^0\bar{\rho}) \to \oplus_{\ell\in P} \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})$ is surjective. By Lemma 14 ([Ram02]), we can pick a prime ideal $\mathfrak{p}_i \in T_i$ such that if $T = \{\mathfrak{p}_{r+1}, \dots, \mathfrak{p}_d\}$, then the map

$$\mathrm{H}^1(G_{P\cup Q_1\cup Q_2}, Ad^0\bar{\rho}) \to \oplus_{\ell\in P} \mathrm{H}^1(G_\ell, Ad^0\bar{\rho})/N_\ell,$$

is surjective. The same proofs of Lemma 15 and 16 ([Ram02]) show that this set Q_2 satisfies the required properties. This proves the existence of the lift, the condition on the restriction to inertia is automatic by the choice of the sets C_ℓ.

To prove that ρ is modular, we know it has big residual image hence it is residually modular (by Serre's conjectures). The modularity is covered by the following two modularity lifting theorems: for the ordinary case modularity follows as a consequence of Theorem 5.2 of [SW01] (we are in a situation covered by the theorem stated in the introduction); for the supersingular case we apply Theorem 3.6 of [DFG04]. Observe that ρ is crystalline by definition and meets the shortness

condition because it preserves the Hodge-Tate weights of $\rho_{f,p}$, which satisfy $2 \leq k \leq p-1$. The irreducibility condition holds because of the big image hypothesis.

□

Let us recall the hypothesis of our second result: let $f \in S_k(\Gamma_0(N), \epsilon)$ be a newform, 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

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

the reduction modulo $\mathfrak{p}^n$ of its p-adic Galois representation.

Theorem B. *In the above hypothesis, let n be a positive integer and $p > k$ be a prime such that:*

- *$p \nmid N$ or f is ordinary at p,*
- *$\mathrm{SL}_2(\mathcal{O}_\mathfrak{p}/\mathfrak{p}) \subseteq \mathrm{Im}(\overline{\rho_{f,p}})$,*
- *p does not ramify in K_f.*

Let R be the set of ramified primes of ρ_n. If $N' = \prod_{p \in R} p^{v_p(N)}$, 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 $N' q_1 \ldots q_r$ 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.

Proof. We want to apply Theorem A to the representation ρ_n, with the local deformation $\rho_{f,p}|_{I_\ell}$ at the primes dividing N'. Note that f being a modular form implies that the representation is odd, and the hypothesis $p > k$ implies that $\rho_{f,p}|_{I_p}$ satisfies the third hypothesis of such theorem. Finally, the condition $p \nmid N$ or f being ordinary at p implies that $\rho_{f,p}|_{I_p}$ can be taken as a deformation at p.

Theorem A then gives a modular representation ρ which is congruent to $\rho_{f,p}$ modulo p^n, and of conductor dividing $N' q_1 \ldots q_r$. 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.

Note that when ρ_f does not lose ramification when reduced modulo p^n and $r = 0$, the newform g that Theorem A produces could 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).

□

7. Example

We want to apply the main result to some particular example. More concretely, we want to add some Steinberg primes to a modular form, modulo powers of a prime. For that purpose we pick the smallest prime in the hypothesis, $p = 5$, and start with a representation coming from an elliptic curve E of prime level $\mathfrak{q}$ (in order to deal with small cohomological dimensions) with full image modulo 5, i.e. $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_5)$. Its adjoint representation is then isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5)$ which is isomorphic to S_5, the symmetric group in 5 elements. For $S = \{5, \mathfrak{q}\}$, we need to compute $\mathrm{H}^1(G_S, Ad^0\bar{\rho})$ and $\mathrm{H}^2(G_S, Ad^0\bar{\rho})$. Recall the following dimension computations:

- If $\ell \not\equiv \pm 1 \pmod{p}$ then $\mathrm{H}^2(G_\ell, Ad^0\bar{\rho}) = 0$ (see Section 3, or [Ram99] Proposition 2).
- Suppose that at p inertia acts via fundamental characters of level two. Then $\mathrm{H}^2(G_p, Ad^0\bar{\rho}) = 0$ ([Ram99] Lemma 5).
- Suppose that $\bar{\rho}$ is flat, and $\bar{\rho}|_{G_p}$ is indecomposable. Then $\mathrm{H}^2(G_p, Ad^0\bar{\rho}) = 0$ ([Ram93]).

Also, if we denote by $r = \dim Ш^1_S((Ad^0\bar{\rho})^*)$, and s the number of primes with $H^2(G_\ell, Ad^0\bar{\rho}) \neq 0$, then (see [Ram02] Lemma, page 139):

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

7.1. **Some group theory.** Recall from Lemma 9 (of [Ram99]) that the elements in $\mathrm{H}^1(G_s, Ad^0\bar{\rho})$ (resp. in $\mathrm{H}^1(G_s, Ad^0\bar{\rho}^*)$) correspond to extensions M of $\mathbb{Q}(Ad^0\bar{\rho})$ (resp. $\mathbb{Q}(Ad^0\bar{\rho}^*)$) whose Galois group is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5) \ltimes M_2^0(\mathbb{F}_5)$ (the 2×2 matrices with zero trace), so we need to compute all such extensions. The problem is that $\mathrm{PGL}_2(\mathbb{F}_5)$ has order 120, and we cannot do Class Field Theory in such a huge extension, so we will reduce the problem to compute some abelian extension over a small degree extension of $\mathbb{Q}$ where we actually can compute Class Field Theory.

The action of S_5 in $M_2^0(\mathbb{F}_5)$ is faithful, so we need to restrict the action to smaller subgroups to find the desired extension.

Lemma 7.1. *Let H be a subgroup of S_5, and suppose that the restriction of the action of S_5 in $M_2^0(\mathbb{F}_5)$ to H decomposes as the direct sum of two subspaces $V_1 \oplus V_2$. Then $H \ltimes V_i$ is a subgroup of $S_5 \ltimes M_2^0(\mathbb{F}_5)$. Furthermore, if V_1 is one dimensional, then $H \ltimes V_2$ is a normal subgroup of $H \ltimes M_2^0(\mathbb{F}_5)$ if and only if V_1 is the trivial representation.*

Proof. The first claim is clear from the definition of a semi-direct product. For the second claim, let $\{v_1, v_2, v_3\}$ be a basis of $M_2^0(\mathbb{F}_5)$ such that $V_1 = \langle v_1 \rangle$ and $V_2 = \langle v_2, v_3 \rangle$. Then it is clear that $H \ltimes V_2$ is invariant under elements of the form (h, v_i) with $i = 2, 3$ (since it is a subgroup), and since it is enough to check invariance on generators it is enough to check invariance under elements of the form (h, v_1). But a direct computation shows that

$$(h, v_1)(g, w)(h, v_1)^{-1} = (hgh^{-1}, v_1 + h \cdot w - (hgh^{-1}) \cdot v_1),$$

which lies in V_2 if and only if $g \cdot v_1 = v_1$ for all $g \in H$. □

Then we need a subgroup of S_5 whose order is prime to 5 (for the representation to be semisimple), whose restriction contains the trivial representation and such that the intersection of its conjugates is trivial (for the Galois closure of the fixed field to be the whole extension). The subgroups of S_5 of order prime to 5 are: $\{1\}$, C_2, $C_2 \times C_2$, C_4, D_8, C_3, C_6, S_3, $S_3 \times C_2$, A_4, S_4 (where C_n means a cyclic group of order n, and D_n the dihedral group with n elements). The largest one (in terms of cardinality) for which the actions splits is $S_3 \times C_2$, for which $M_2^0(\mathbb{F}_5)$ splits as a direct sum

$$< (3, 1, 0), (3, 0, 1) > \oplus \langle (4, 1, 1) \rangle,$$

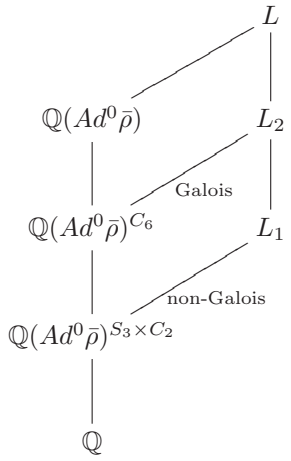
via the identification $S_3 \times C_2 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 4 & 2 \\ 1 & 1 \end{smallmatrix}\right) \rangle \times \langle \left(\begin{smallmatrix} 3 & 2 \\ 2 & 2 \end{smallmatrix}\right) \rangle$ in $\mathrm{PGL}_2(\mathbb{F}_5)$ and in the basis of $M_2^0(\mathbb{F}_5)$ $\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\}$. The action in the 1-dimensional subspace is non-trivial, nevertheless the restriction to its cyclic subgroup of order 6 is trivial as can be seen via a direct computation (and actually 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 7.2. $(C_3 \times C_2) \ltimes V_2 \lhd (S_3 \times C_2) \ltimes M_2^0(\mathbb{F}_5)$.

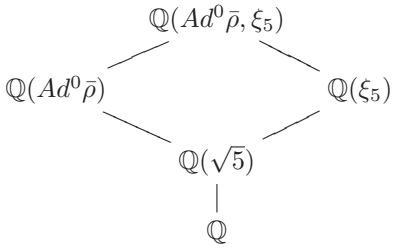
Proof. The previous Lemma implies that $(C_3 \times C_2) \ltimes V_2 \lhd (C_3 \times C_2) \ltimes M_2^0(\mathbb{F}_5)$ but since $C_3 \lhd S_3$, the same proof gives the statement. □

Then we first search for the S_5 extension corresponding to the adjoint representation (which might be given as the Galois closure of a degree 5 extension) and then we search for the fixed field of $(C_3 \times C_2) \ltimes M_2^0(\mathbb{F}_5)$, which is a degree 20 extension of $\mathbb{Q}$. By Lemma 7.2, the field fixed of $(C_3 \times C_2) \ltimes V_2$ is a degree 5 abelian extension L_2 of it, so we can compute it using class field theory. Note that since $(S_3 \times C_2) \ltimes V_2$ is a subgroup, the degree five extension we are looking for actually is a non-Galois degree 5 extension L_1 of the degree 10 extension over $\mathbb{Q}$ fixed by $(S_3 \times C_2) \ltimes M_2^0(\mathbb{F}_5)$.

We illustrate this phenomena in the following diagram:



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



The Galois group $\mathrm{Gal}(\mathbb{Q}(Ad^0\bar{\rho}^*)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(Ad^0\bar{\rho},\xi_5)/\mathbb{Q}) \simeq C_4 \ltimes A_5$, 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 $\mathrm{Ш}^1(G_S, Ad^0\bar{\rho}^*)$, 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.

7.2. **Particular example.** Consider the elliptic curve

$$E_{17a1} : y^2 + xy + y = x^3 - x^2 - x - 14.$$

The representation obtained by looking at the 5-torsion points has full image (using [S$^+$13]), so is isomorphic to $\mathrm{GL}_2(\mathbb{F}_5)$. Then its 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 only ramified at 5 and 17. We can search for such extensions (they are the Galois closure of a degree 5 extension) in Roberts-Jones tables (see [JR13]), and get 12 such extensions, given by the polynomials:

$$\begin{array}{ccc} x^5+x^3-2x^2-2x-3, & x^5-5x^2+5, & x^5-85x-153, \\ x^5-15x^3-75x^2-110x-89, & x^5-50x^2+100x-65, & x^5-10x^3-20x^2-15x+421, \\ x^5+35x^3-15x^2+185x-1102, & x^5-85x^2-85x-51, & x^5+15x^3-45x^2+60x-239, \\ x^5+25x^3-125x^2+250x-420, & x^5-50x^2-25x-230, & x^5+2125x-8075. \end{array}$$

To know which one corresponds to our elliptic curve, we just compute the characteristic polynomial of the Frobenius at 3, which is given by x^2-3, which means that it has order 2 in $\mathrm{PGL}_2(\mathbb{F}_5)$. If we compute the inertial degree of 3 in the above extensions, we see that there exists a prime above 3 with inertial degree greater than 2 in all the field extensions but $x^5-85x-153$, which must be the extension we are looking for.

To search for the 2-dimensional space $\mathrm{H}^1(G_S, Ad^0\bar{\rho})$, we search for a degree 20 extension M of $\mathbb{Q}$ fixed by the C_6 subgroup (using the Pari script subfieldgen written by Bill Allomber). It is given by the polynomial

$$\begin{aligned}P(x) = x^{20} - 5x^{19} + 5x^{18} + 5x^{17} + 105x^{16} - 591x^{15} + 1545x^{14} - 1125x^{13} - 5975x^{12} + 28195x^{11} - \\ - 57199x^{10} + 44405x^9 + 188910x^8 - 778890x^7 + 1946100x^6 - 3335796x^5 + \\ + 4553305x^4 - 4695185x^3 + 3627665x^2 - 1817365x + 443586\end{aligned}$$

Its degree 10 subextension N is given by

$$x^{10} - 5x^9 + 5x^8 + 10x^7 - 15x^6 + 40x^5 - 155x^4 + 350x^3 - 430x^2 + 1525x - 2670.$$

Lemma 7.3. *In the previous hypothesis,* $\dim \mathrm{H}^2(G_S, Ad^0\bar{\rho}) = 0$ *and* $\dim \mathrm{H}^1(G_S, Ad^0\bar{\rho}) = 2$.

Proof. By Lemma 9 in [Ram99] $\dim \mathrm{H}^2(G_S, Ad^0\bar{\rho}) = r + s$ and $\dim \mathrm{H}^1(G_S, Ad^0\bar{\rho}) = r + s + 2$, where $r = \dim Ш^1_S((Ad^0\bar{\rho})^*)$ and s is the number of primes $v \in S$ such that $\dim \mathrm{H}^2(G_s, Ad^0\bar{\rho}) \neq 0$.

Since $17 \not\equiv \pm 1 \pmod 5$, Proposition 2 of [Ram93] implies $\mathrm{H}^2(G_{17}, Ad^0\bar{\rho}) = 0$. Also, since the prime 5 is totally ramified in the extension $\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}$, $\bar{\rho}|_{G_5}$ is indecomposable (it is not abelian), and also $\mathrm{H}^2(G_5, Ad^0\bar{\rho}) = 0$ (the numbers in Table 3 on [Ram99] apply), so $s = 0$.

On the other hand, the elements of $Ш^1_S((Ad^0\bar{\rho})^*)$ correspond to extensions of $\mathbb{Q}((Ad^0\bar{\rho})^*)$ unramified outside S at which the primes above 5 and 17 split completely. In particular, they are unramified extensions of M. Since the class group of such extension is not divisible by 5, we deduce that it is trivial, so $r = 0$, and the result follows. □

Remark. The local $\mathrm{H}^1(G_5, Ad^0\bar{\rho})$ has dimension 3, and the subspace N_5 is that of finite flat group schemes, which are indecomposable (see Remark7.2), which has dimension 1 (see Table 3 on [Ram99]).

We have to compute all degree 5 Galois extensions of M which are unramified outside 5 and 17. We use Class Field Theory, where a bound for the exponent of the modulus $e(\mathfrak{p})$ is given by the following result.

Proposition 7.4. *Let L/K be an abelian extension of prime degree 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 [Coh00] Proposition 3.3.21 and Proposition 3.3.22. □

We need a degree 5 extension, and since the primes 5 and 17 ramify completely in L_2, the modulus is $\mathfrak{p}_5^{26}\mathfrak{p}_{17}$. We compute such class group using Pari/GP ([PAR13]), and get that such class group is isomorphic to

$$C_{240} \times C_{40} \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5.$$

It should be pointed out that one can chose a basis of the characters such that only one of them ramifies at $\mathfrak{p}_{17}$.

Recall that the extensions we are looking for come from degree 5 extensions of N, but are not Galois over it. If we apply CFT to N, the class group is isomorphic to

$$C_{80} \times C_{20} \times C_5 \times C_5 \times C_5,$$

and no extension is ramified over the prime 17.

Lemma 7.5. *If a rational prime p is unramified in $\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}$ and has a prime over it with inertial degree 5, then all primes dividing it have inertial degree 5 and split completely in $L_2/\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}$.*

Proof. The maximal cyclic subgroup of S_5 of order divisible by 5 is of order 5, hence for any prime in $\mathbb{Q}(Ad^0\bar{\rho})$ the decomposition group is cyclic of order 5. Since it does not intersect $S_3 \times C_2$, the first assertion follows and any prime over it in $\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}$ splits completely in $\mathbb{Q}(Ad^0\bar{\rho})/\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}$. But a cyclic group cannot be written as a semidirect product of groups whose order is divisible by 5, hence it must split completely in $L/\mathbb{Q}(Ad^0\bar{\rho})$ as well. □

We search for $\mathrm{H}^1(G_S, Ad^0\bar{\rho})$ computing all the elements in the class group of $\mathbb{Q}(Ad^0\bar{\rho})^{C_6}$ that split completely for primes with inertial degree 5 in $\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}/\mathbb{Q}$. With the first such primes, we get a degree 5 subspace, which contains a degree 3 subspace coming from the class group of $\mathbb{Q}(Ad^0\bar{\rho})^{S_3\times C_2}$, so we get the 2-dimensional subspace corresponding to the $\mathrm{H}^2(G_S, Ad^0\bar{\rho})$. Also, an important fact is that all the characters in this 5-dimensional space are unramified at 17.

Remark. To determine the number of auxiliary primes we need to add, we have to determine which elements in $\mathrm{H}^1(G_S, Ad^0\bar{\rho})$ are trivial while restricting to G_5. Since the flat subspace is one dimensional (and the representations coming from our elliptic curve is in there), we are just led to prove which extensions give the same field extension of $\mathbb{Q}_5$. Note that since $\mathbb{Q}(Ad^0\bar{\rho})^{C_6}$ is totally ramified, and there are no solvable subgroups of S_5 whose order is divisible by 20 and have order greater than 20, the prime $\mathfrak{p}$ splits completely in $\mathbb{Q}(Ad^0\bar{\rho})/\mathbb{Q}(Ad^0\bar{\rho})^{C_6}$. Then if we restrict our representation to G_5, the representation we get has degree 20 and is that of the completion of M at $\mathfrak{p}_5$.

We can check the local behavior of our representations just by looking at the 5-adic part of our character, and since our characters are only ramified at 5, if two linearly independent ones have the same 5-adic component, then the quotient would give a non-trivial unramified character of order 5, but there are no such characters. Then one goes to zero (in $\mathrm{H}^1(G_5, Ad^0\bar{\rho})/N_5$) and the other does not. In particular just one extra prime is enough.

We search for a prime $q \not\equiv \pm 1 \pmod 5$ and such that $a_q \equiv \pm(q+1) \pmod{25}$, and $q = 113$ is such a prime, since $a_{113} = -14 \equiv -(113+1) \pmod{25}$.

Lemma 7.6. *There exists a weight* 2 *modular form of level* $17 \cdot 113$ *which is congruent modulo* 5^2 *to the modular form attached to* E_{17a1}.

Proof. In view of the previous discussion, we just need to check that 113 is the right choice for the map

$$\mathrm{H}^1(G_{\{5,113\}}, Ad^0\bar{\rho}) \mapsto \mathrm{H}^1(G_5, Ad^0\bar{\rho})/N_5 \times \mathrm{H}^1(G_{113}, Ad^0\bar{\rho})/N_{113},$$

to be an isomorphism. We already know that the space $\mathrm{H}^1(G_{\{5\}}, Ad^0\bar{\rho})$ is two dimensional, and that its image in $\mathrm{H}^1(G_5, Ad^0\bar{\rho})/N_5$ has dimension 1 (the deformation f_E corresponding to our elliptic curve maps to 0), so we need to check that the extra element is linearly independent with the non-zero element in such cohomological group and that $f_E|_{G_{113}} \notin N_{113}$, which is equivalent to say that the Frobenius element at 113 modulo 5 and modulo 25 have different orders. Since $a_{113} = -14$, the characteristic polynomial is given by $x^2 + 14x + 113 \equiv (x-12)(x-24) \pmod{25}$, so the Frobenius element has order 4 modulo 5 and order 20 modulo 25.

We do the same computation as before, but adding this extra prime to the ramification, and check that the cohomological dimension of $\mathrm{H}^1(G_{S\cup\{113\}}, Ad^0\bar{\rho})$ increases by 1 (the whole $\mathbb{F}_5$ vector space computed using CFT has dimension 17, but using Lemma 7.5 we get a 7-dimensional subspace, and the ones coming from N satisfying the same property have dimension 4). We just need to check that the 5-adic characters corresponding to these 3-dimensional subspace generate a 3-dimensional space. Note that we can chose a basis such that there is a 2-dimensional part $\langle v_1, v_2\rangle$ unramified at 113, and a one dimensional part $\langle v_3\rangle$ ramified also at 113. If the 5-adic character of v_3 is in the vector space spanned by $\langle v_1, v_2\rangle$, then we can multiply v_3 by the inverse of the 5-adic part of the character (which exists globally) to get an extension in our subspace (which does not come from N) only ramified at 113. But using CFT, it is easy to check that the only subspace satisfying Lemma 7.5 comes from an abelian extension of N. □

Remark. In this particular case, one can search for the form in the right space. We did such computation using Magma ([BCP97]) and computed the space of newforms of level $17 \cdot 113$. Such

space contains (up to conjugation) 5 newforms. Our curve is isomorphic modulo 25 to an eigenform whose coefficient field has degree 43 over $\mathbb{Q}$, given by the polynomial

$$x^{43} - 6x^{42} - 52x^{41} + 373x^{40} + 1125x^{39} - 10604x^{38} - 11821x^{37} + 182630x^{36} + 26405x^{35} - 2127738x^{34} + 979653x^{33} + 17730287x^{32} - 15815881x^{31} - 108925194x^{30} + 134740636x^{29} + 500970519x^{28} - 774455464x^{27} - 1732542039x^{26} + 3221093358x^{25} + 4479749953x^{24} - 9965892052x^{23} - 8501952587x^{22} + 23170021972x^{21} + 11368626528x^{20} - 40486609059x^{19} - 9675455698x^{18} + 52796933022x^{17} + 3349112852x^{16} - 50684587408x^{15} + 2843708080x^{14} + 35061372555x^{13} - 4639214583x^{12} - 16918972986x^{11} + 2949253955x^{10} + 5411942205x^{9} - 1031364938x^{8} - 1053178460x^{7} + 201802209x^{6} + 106332326x^{5} - 20249486x^{4} - 3919101x^{3} + 714966x^{2} + 1842x - 263.$$

References

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

[BD] Christophe Breuil and Fred Diamond. Formes modulaires de hilbert modulo p et valeurs d'extensions entre caractÃ¨res galoisiens. *Ann. Scient. de l'E.N.S., to appear*.

[Car89] Henri Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem*. Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[DFG04] Fred Diamond, Matthias Flach, and Li Guo. The Tamagawa number conjecture of adjoint motives of modular forms. *Ann. Sci. École Norm. Sup. (4)*, 37(5):663–727, 2004.

[Dum05] Neil Dummigan. Level-lowering for higher congruences of modular forms. 2005. `http://www.neil-dummigan.staff.shef.ac.uk/levell4.dvi`.

[JR13] John W. Jones and David P. Roberts. A database of number fields. `http://hobbes.la.asu.edu/NFDB`, 2013.

[PAR13] *PARI/GP, version* `2.5.5`. Bordeaux, 2013. available from `http://pari.math.u-bordeaux.fr/`.

[Ram93] Ravi Ramakrishna. On a variation of Mazur's deformation functor. *Compositio Math.*, 87(3):269–286, 1993.

[Ram99] Ravi Ramakrishna. Lifting Galois representations. *Invent. Math.*, 138(3):537–562, 1999.

[Ram02] Ravi Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. *Ann. of Math. (2)*, 156(1):115–154, 2002.

[RH08] Ravi Ramakrishna and Spencer Hamblen. Deformation of certain reducible galois representations, ii. *American Journal of Mathematics*, 130, 2008.

[Rib85] Kenneth A. Ribet. On l-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[S+13] W. A. Stein et al. *Sage Mathematics Software (Version 5.8)*. The Sage Development Team, 2013. `http://www.sagemath.org`.

[Ser89] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*. The advanced book program. Addison-Wesley publishing company, 1989.

[SW01] C. Skinner and A. Wiles. Nearly ordinary deformations of irreducible residual representations. *Annales de la faculte des sciences de Toulouse*, 10(1):185–215, 2001.

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires

E-mail address: `maxicampo@gmail.com`

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires and IMAS, CONICET, Argentina

E-mail address: `apacetti@dm.uba.ar`