LIFTING REDUCIBLE GALOIS REPRESENTATIONS

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Anwesh Ray

August 2020

LIFTING REDUCIBLE GALOIS REPRESENTATIONS

Anwesh Ray, Ph.D.

Cornell University 2020

Let p be an odd prime and q a power of p. By the celebrated theorem of Khare and Wintenberger (previously Serre's conjecture), an absolutely irreducible odd 2-dimensional Galois representation $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ (satisfying favorable conditions) lifts to a characteristic zero Galois representation associated to a Hecke eigencuspform. Hamblen and Ramakrishna prove the analog of (the weak form of) Serre's conjecture for residually reducible 2-dimensional Galois representations. A higher dimensional generalization of their result is proved in chapter 3. Let $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GSp}_{2n}(\mathbb{F}_q)$ be a reducible and indecomposable Galois representation which is unramified outside a finite set of primes S and whose image lies in a Borel subgroup. It is shown that if $\bar{\rho}$ satisfies some additional conditions, it lifts to characteristic zero Galois representation which is geometric in the sense of Fontaine-Mazur.

In chapter 4 we examine the problem of lifting a two dimensional Galois representation $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_q)$ to a cuspidal Hida Family which is isomorphic to the Iwasawa algebra Λ via the weight-space map. This was achieved for an odd, ordinary and absolutely irreducible $\bar{\rho}$ by Ramakrishna in [26] for a suitable choice of auxiliary local deformation conditions. We show that if $\bar{\rho}$ is reducible and indecomposable, one may indeed lift $\bar{\rho}$ to a Hida family $\mathbb{T}$ such that the image of the weight space map contains a congruence class of weights in $\operatorname{Spec}\Lambda$ modulo

p^2. This Hida family is in some sense close to $\operatorname{Spec}\Lambda$, more precisely, we show that it represents a deformation functor which is arranged to have a hull isomorphic to $\operatorname{Spec}\Lambda$ (this isomorphism is not via the weight-space map). In chapter 5 we apply results of Hamblen-Ramakrishna to construct some special Galois extensions. For every prime $p \geq 5$ for which a certain condition on the class group $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ is satisfied, we construct a p-adic analytic Galois extension of the infinite cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})$ with some special ramification properties. In greater detail, this extension is unramified at primes above p and tamely ramified above finitely many rational primes and its Galois group over $\mathbb{Q}(\mu_{p^\infty})$ is isomorphic to a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ which contains the principal congruence subgroup. For the primes $107, 139, 271$ and 379 such extensions were first constructed by Ohtani and Blondeau. The strategy for producing these special extensions at an abundant number of primes is through lifting two-dimensional reducible Galois representations which are diagonal when restricted to p.

BIOGRAPHICAL SKETCH

Anwesh Ray attended Rishi Valley School in Andhra Pradesh, India. He studied some number theory and algebraic geometry in school and was enthusiastic about pursuing a career as a mathematician. He completed a Bachelors in mathematics and computer science (2010-2013) and a masters in mathematics (2013-2015) in Chennai Mathematical Institute, Chennai, India. He started his P.h.d at Cornell in 2015 where he was presented with the opportunity of working with Ravi Ramakrishna. After receiving his degree at Cornell, he will be a postdoctoral scholar at the University of British Columbia. Besides number theory, he likes soccer, endurance running and weight-lifting. His girlfriend is a number theory graduate student and has lent a patient ear to his monologues describing his current and future research.

This document is dedicated to Shailesh Shirali and to Ravi Ramakrishna.

ACKNOWLEDGEMENTS

The author is very grateful to his advisor Ravi Ramakrishna for introducing him to the fascinating subject of Galois deformations and for proposing a number of projects they are looking forward to completing in the near future. He thanks R. Sujatha for stimulating his interest in Iwasawa theory by proposing various projects during the time he was a graduate student at Cornell. These results will not be discussed in this thesis for the sake of brevity and in the interest of keeping the thesis streamlined to a unifying topic. The thesis is a compilation of submitted papers, some of which have undergone revisions. The author appreciates the suggestions made by the anonymous referees which have led to significant improvement of the presentation of the work presented in this thesis.

The author is very thankful to Mahan Maharaj, Shailesh Shirali and B. Sury who guided his early explorations in mathematics. He considers himself unusually privileged for the extraordinary optimism from his family in supporting his mathematical pursuits. He is indebted to his parents who cheered him on as he spent a lot of his time on mathematics in high school and didn't mind that he got average grades in the other subjects. He thanks V. Balaji, R. Balasubramanian, Priyavarath Deshpande, Sukhendu Mehrohtra, Joseph Oesterle, Prem Prakash Pandey, Purusottam Rath, Shiva Shankar, Pramath Shastri and Ramaiyengar Sridharan for their support and guidence during the years he spent at the Chennai Mathematical Institute. He thanks Mahdi Asgari, Brian Hwang, Allen Knutson, Christian Maire, Jason Manning, Mike Stillman, Nicolas Templier, David Zywina and Inna Zakharevich for fruitful conversations during the time he spent at

Cornell. He has learnt a lot from fellow Cornell graduate students Philip Bonneville, Christine Mcmeekin, Andres Fernandez Herrero, Kimia Kazemian and Rakvi Shrivastava. He like to thank Alex Frederick, Gabriel Dorfman-Hopkins, Debanjana Kundu and Peter Wear for conversations/collaborations. He would like to thank his partner Mishty Ray for all the encouragement and support she has provided him and for patiently listening to all the details in this thesis straight from the horse's mouth.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Galois Representations associated to Modular forms

The absolute Galois group of the rational numbers $\mathrm{G}_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ encodes information pertaining to arithmetic and geometric objects of interest in number theory. Class field theory provides an explicit description of the abelianization of $\mathrm{G}_{\mathbb{Q}}$ and thereby, the collection of all abelian number field extensions of $\mathbb{Q}$. On the other hand, p-adic Galois representations

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$$

capture deep geometric and automorphic phenomena.

At each prime v, let $\mathrm{G}_v := \mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v)$ and fix an injection $\iota_v : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_v$. With respect to ι_v, the local Galois group G_v is identified with a decomposition group contained in $\mathrm{G}_{\mathbb{Q}}$. Let $I_v \subset \mathrm{G}_v$ denote the inertia subgroup of G_v and $\sigma_v \in \mathrm{G}_v$ a choice of Frobenius element. A Galois representation ρ is *unramified* at v if $I_v \subset \ker \rho$. At a prime v where ρ is unramified, the element $\rho(\sigma_v)$ is well-defined. At a prime v at which ρ is unramified, denote by

$$\mathrm{ch}_v(\rho, X) := \det(1 - \rho(\sigma_v)X)$$

the characteristic polynomial of ρ at a v.

The prototypical interesting examples of Galois representations are those associated to elliptic curves and certain modular forms. Let E be an elliptic curve defined over $\mathbb{Q}$ and $E[p^n] \subset E(\bar{\mathbb{Q}})$ its p^n-torsion subgroup. The p-adic Tate module of an elliptic curve E is the inverse limit

$$T_pE := \varprojlim_n E[p^n] \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$$

where the inverse limit is taken w.r.t the multiplication by p maps. The Galois group $\mathrm{G}_{\mathbb{Q}}$ acts naturally on the T_pE, which induces the p-adic Galois representation

$$\rho_{E,p} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_p}(T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Q}_p).$$

Associated to a normalized Hecke eigencuspform f is its p-adic Galois representation

$$\rho_{f,p} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p).$$

This too depends on a choice of an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. Suppose that $f = \sum_{l\geq 1} a_l q^n$ modular w.r.t $\Gamma_1(N)$ and with weight $k \geq 2$ and nebentype-character ϵ. Then for any choice of prime p, the p-adic Galois representation $\rho_{f,p}$ is unramified at all primes $l \nmid Np$ and

$$\mathrm{ch}_l(\rho_{f,p}, X) = 1 - a_l X + \epsilon(l) l^{k-1} X^2.$$

Here, the coefficients of $\mathrm{ch}_l(\rho_{f,p}, X)$ are viewed in $\bar{\mathbb{Q}}_p$ via the chosen embedding. Galois representations associated to elliptic curves and eigencuspforms satisfy certain characteristic properties, namely, they are *geometric* in the sense of Fontaine and Mazur [6], see Definition 1.1.1.

Let $c \in \mathrm{G}_{\mathbb{Q}}$ denote complex-conjugation. A Galois representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ is said to be *odd* if $\det \rho(c) = -1$ and *even* if $\det \rho(c) = 1$.

Definition 1.1.1. *A continuous and irreducible Galois representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ is said to be geometric if:*

1. *ρ is unramified at all but finitely many primes,*
2. *ρ is odd,*
3. *$\rho_{\restriction \mathrm{G}_p}$ is de-Rham.*

The third condition is a p-adic Hodge theoretic condition, see [3, chapter 6]. Geometric Galois representations are expected to arise from the étale cohomology of varieties defined over the rational numbers. Fontaine and Mazur conjectured that a 2-dimensional geometric Galois representations $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ is modular, i.e. is the p-adic Galois representation attached to a Hecke eigencuspform. Most cases of the Fontaine-Mazur conjecture for $\mathrm{GL}_{2/\mathbb{Q}}$ have been settled by Taylor [29], Skinner-Wiles [20], Kisin [14] and others.

The celebrated Modularity theorem of Wiles et al. asserts, among other things, that an elliptic curve defined over $\mathbb{Q}$ coincides with an eigencuspform. More precisely, there is an eigencuspform f of weight 2 with $\mathbb{Q}$-coefficients such that at all primes p, the p-adic Galois representations

$$\rho_{f,p} \simeq \rho_{E,p}.$$

Given a p-adic representation ρ, there is a choice of basis the underlying vector space such that $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ is the reduction $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$, referred to as the residual representation. The semi-simplification of $\bar{\rho}$ does not depend on the choice of basis. When speaking of the residual representation we shall therefore implicitly assume that $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$. The perspective introduced by Mazur and adopted by Wiles is to view a p-adic Galois representation in a p-adic family of *Galois deformations* of a fixed residual representation $\bar{\rho}$. There is a universal Galois representation

$$\rho^{\mathrm{univ}} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(R_{\bar{\rho}})$$

lifting $\bar{\rho}$ such that ρ coincides with a $\bar{\mathbb{Z}}_p$-valued point on $\mathrm{Spec}\, R_{\bar{\rho}}$. The key step in the proof of Wiles' theorem is to show that the universal deformation ring $R_{\bar{\rho}}$ is isomorphic to a certain localized Hecke algebra $\mathbb{T}_{\bar{\rho}}$. It is not hard to deduce from this that ρ arises from an eigencuspform.

1.2 Reducible Galois representations

Closely related to the Fontaine-Mazur conjecture is Serre's conjecture. The conjecture predicts when a two dimensional residual representation $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ is the residual representation of a characteristic zero representation associated to an eigencuspform. Serre's conjecture was proved by Khare and Wintenberger.

Let l be a prime and $\mathrm{G}_0 := \mathrm{G}_{\mathbb{Q}_l}$ identified with the decomposition subgroup of

$\mathrm{G}_{\mathbb{Q}}$ of the prime l. For $i > 0$, let G_i denote the i-th ramification subgroup of G_0. Let $V_{\bar{\rho}}$ denote the underlying Galois module of $\bar{\rho}$. The Artin conductor of $\bar{\rho}$ denoted $\mathrm{Art}\,\bar{\rho}$ is prescribed by

$$\mathrm{Art}\,\bar{\rho} := \prod_{l} l^{n_{\bar{\rho}}(l)}$$

where the product runs over all prime numbers l

$$n_{\bar{\rho}}(l) := \sum_{i \geq 0} \frac{1}{[\mathrm{G}_0 : \mathrm{G}_i]} \dim \left(V_{\bar{\rho}} / V_{\bar{\rho}}^{\mathrm{G}_i} \right).$$

The *Serre level* of $\bar{\rho}$ is the prime to p part of the Artin conductor of $\bar{\rho}$ and is denoted by $N_{\bar{\rho}}$.

Theorem 1.2.1. *(Khare-Wintenberger [13]) Let $p \geq 5$ be a prime number and let $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ be an odd two-dimensional continuous Galois representation. Suppose further that $\bar{\rho}$ is irreducible. Then $\bar{\rho}$ lifts to the characterisitic zero Galois representation ρ_f arising from a Hecke eigencuspform f as depicted*

$$\begin{array}{ccc} & & \mathrm{GL}_2(\bar{\mathbb{Z}}_p) \\ & \overset{\rho_f}{\nearrow} & \downarrow \\ \mathrm{G}_{\mathbb{Q}} & \xrightarrow[\bar{\rho}]{} & \mathrm{GL}_2(\bar{\mathbb{F}}_p). \end{array}$$

Furthermore, an eigenform f may be chosen so as to have level equal to the Serre level of $\bar{\rho}$.

The statement that $\bar{\rho}$ lifts to a characteristic zero Galois representation arising from an eigencuspform is/was referred to as the weak form of Serre's conjecture.

The additional requirement that the level may be optimized as well is referred to as the strong form. The key ingredient in the proof of the strong form is Ribet's Level Lowering theorem [22]. Ribet showed that if f is an eigencuspform such that $\bar{\rho} = \bar{\rho}_f$ is irreducible, then there exists an eigencuspform g of level $N_{\bar{\rho}}$ such that $\bar{\rho}_g = \bar{\rho}$. Thus it was known that the strong form of Serre's conjecture is a consequence of the weak form and Ribet's theorem.

The p-adic representation ρ_f associated to an eigencuspform f is irreducible, the residual representation $\bar{\rho}_f$ may on the other hand be reducible. This happens when the eigencuspform f exhibits a congruence with an Eisenstein series. Such congruences provide insight into the eigenspaces of the mod p class group of $\mathbb{Q}(\mu_p)$. Such considerations led Ribet to establish the converse to Herbrand's theorem [21]. It is natural to investigate analogs of Serre's conjecture to the case when $\bar{\rho}$ is reducible. More precisely, if $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ is an odd, reducible Galois representation, under what conditions can one lift $\bar{\rho}$ to a characteristic zero representation arising from an eigencuspform?

The Fontaine-Mazur conjecture for residually reducible Galois representations was established by Skinner and Wiles.

Theorem 1.2.2. *(Skinner and Wiles [20]) Suppose that $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ is a continuous Galois representation, irreducible and unramified outside a finite set of primes. Suppose also that there is a character φ such that* $\bar{\rho} \simeq \begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix}$.

Assume further that:

1. $\varphi_{\restriction \mathrm{G}_p} \neq 1$,
2. $\rho_{\restriction I_p} \simeq \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$,
3. $\det \rho = \psi \chi^{k-1}$ *where* χ *is the* p*-adic cyclotomic character,* $k \geq 2$, ψ *is a finite order character and* $\det \rho$ *is odd.*

Then ρ *comes from an eigencuspform.*

Thus, if some favorable conditions are satisfied, any geometric Galois representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ for which $\bar{\rho}$ is reducible arises from an eigencuspform. Hamblen and Ramakrishna prove the analog of the weak version of Serre's conjecture for residually reducible Galois representations $\bar{\rho}$.

Theorem 1.2.3. *(Hamblen-Ramakrishna [9]) Let* p *be an odd prime and* $\mathbb{F}$ *a finite field of characteristic* p*. Let* S *be a finite set of primes and* $\bar{\rho} = \begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_2(\bar{\mathbb{F}})$ *be a reducible and odd Galois representation. Assume that the following conditions are satisfied:*

1. $\bar{\rho}$ *is indecomposable, i.e. the extension class* $* \in H^1(\mathrm{G}_{\mathbb{Q},S}, \mathbb{F}(\varphi))$ *is nontrivial,*
2. $\varphi^2 \neq 1$,
3. $\varphi \neq \chi, \chi^{-1}$ *where* χ *is the mod* p *cyclotomic character,*
4. *the* $\mathbb{F}_p$*-span of the image of* φ *is all of* $\mathbb{F}$,

5. $\bar{\rho}_{\restriction G_p}$ *is not unramified of the form* $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Then there is a finite set of primes X disjoint from S and a characteristic zero geometric lift $\rho : G_{\mathbb{Q},S\cup X} \to GL_2(W(\mathbb{F}))$ which is ordinary at p. The Galois representation ρ arises from a p-ordinary eigencuspform.

The method of Hamblen and Ramakrishna is an adaptation of Ramakrishna's lifting strategy which had previously been applied in the residually irreducible case (cf. [23] and [25]). Via a Galois theoretic argument, it is shown that $\bar{\rho}$ lifts to a characteristic zero geometric Galois representation which satisfies the hypotheses of Theorem 1.2.2. As a result, the representation ρ indeed arises from an eigencuspform. It should be noted that in order to obtain a geometric lift of $\bar{\rho}$, the method of Hamblen-Ramakrishna necessitates adjoining a finite set of auxiliary primes X to the set at which $\bar{\rho}$ is ramified. As a result, Theorem 1.2.3 only establishes the weak version of Serre's conjecture in the residually reducible setting. Ribet's level lowering theorem stipulates that $\bar{\rho}$ be absolutely irreducible in order for the level to be optimized.

The isomorphism class of a reducible representation

$$\bar{\rho} = \begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix} : G_{\mathbb{Q},S} \to GL_2(\mathbb{F}_p)$$

coincides with the global cohomology class

$$* \in H^1(G_{\mathbb{Q},S}, \mathbb{F}_p(\varphi)).$$

Denote the mod-p class group of $\mathbb{Q}(\mu_p)$ by $\mathcal{C} := \mathrm{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p$, it decomposes into eigenspaces w.r.t the $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$-action. Letting $\bar{\chi} : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^\times$ denote the mod-p cyclotomic character,

$$\mathcal{C} = \bigoplus_{i=0}^{p-2} \mathcal{C}(\bar{\chi}^i)$$

where $\mathcal{C}(\bar{\chi}^i) = \{z \in \mathcal{C} \mid g \cdot z = \bar{\chi}^i(g)z\}$. Associated to any $\mathbb{F}_p$-quotient of $\mathcal{C}(\bar{\chi}^i)$ is a cohomology class $* \in H^1(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathbb{F}_p(\bar{\chi^i}))$ and associated Galois representation

$$\bar{\rho} = \begin{pmatrix} \bar{\chi}^i & * \\ 0 & 1 \end{pmatrix}$$

which is unramified when restricted to $\mathrm{G}_{\mathbb{Q}(\mu_p)}$. Vandiver's conjecture states that if i is even, the eigenspace $\mathcal{C}(\bar{\chi}^i) = 0$. If i is odd, the the eigenspace $\mathcal{C}(\bar{\chi}^i)$ is expected to be at most one-dimensional. There is however no known absolute bound on the dimension of the eigenspaces $\mathcal{C}(\bar{\chi}^i)$. A level lowering result in the spirit of Ribet's theorem shall shed considerable light on such questions.

The organization of this thesis is as follows. Chapter 2 reviews some notation and facts pertaining to the deformation theory of Galois representations. In chapter 3, a higher dimensional analog of Theorem 1.2.3 is presented. In chapter 4, certain p-adic families of Galois representations referred to as Hida families are constructed. It is shown that on prescribing specific local conditions on our deformations, one can construct a Hida-line of deformations of a reducible Galois representation $\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$. This construction sheds light on the question of representability the functor of Galois deformations which satisfy local conditions which are not representable. This is a feature of the deformation theory of residually reducible Galois representations. In chapter 5 we apply the results of Hamblen-Ramakrishna to construct certain special Galois extensions of $\mathbb{Q}(\mu_{p^\infty})$ which satisfy some interesting ramification conditions.

CHAPTER 2

PRELIMINARIES ON DEFORMATION THEORY

Let $\mathbb{F}_q$ be a finite field of characteristic p containing q elements. Denote by $\mathcal{O} = W(\mathbb{F}_q)$ the ring of Witt vectors of $\mathbb{F}_q$. This may be identified with the valuation ring of the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$. The uniformizer of $\mathcal{O}$ is p. Let G be a smooth group scheme over $\mathcal{O}$ such that the connected component containing the identity G^0 is a split reductive group. In this manuscript, G shall be taken to be GL_2, or more generally, GSp_{2n}. In this chapter, let S be a finite set of prime numbers containing p and $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{G}(\mathbb{F}_q)$ be a Galois representation. As notation suggests, $\bar{\rho}$ is unramified at all primes $v \notin S$. The discussion is motivated by the weak version of Serre's conjecture for $\bar{\rho}$. Namely, one is interested in showing that if $\bar{\rho}$ satisfies some favorable conditions, then it lifts to a characteristic zero geometric Galois representation in the sense of Fontaine-Mazur

$$\begin{array}{ccc} & & \mathrm{G}(\mathcal{O}) \\ & \overset{\rho}{\nearrow} & \downarrow \\ \mathrm{G}_{\mathbb{Q}} & \xrightarrow[\bar{\rho}]{} & \mathrm{G}(\mathbb{F}_q). \end{array}$$

For an introduction to the deformation theory of Galois representations the reader may refer to [15].

Let Σ be a finite set of primes containing the set of primes S. Denote by $\mathbb{Q}_\Sigma$ the maximal extension of $\mathbb{Q}$ unramified at all primes $v \notin \Sigma$. By maximality, $\mathbb{Q}_\Sigma$ is a Galois extension of $\mathbb{Q}$, set $\mathrm{G}_{\mathbb{Q},\Sigma} := \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. At each prime number v, denote by $\mathrm{G}_v := \mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v)$ and $I_v \subset \mathrm{G}_v$ be the inertia subgroup. Let $\sigma_v \in \mathrm{G}_v / I_v$ be the Frobenius element and let $\tau_v \in I_v$ be a choice of a generator for pro-p tame inertia. Let $\mathcal{C}_\mathcal{O}$ be the category of Noetherian coefficient-algebras over $\mathcal{O}$. An $\mathcal{O}$-algebra $A \in \mathcal{C}_\mathcal{O}$ is a complete Noetherian local $\mathcal{O}$-algebra equipped with an isomorphism of $\mathcal{O}$-algebras $A/\mathfrak{m}_A \xrightarrow{\sim} \mathbb{F}$.

Definition 2.0.1. *Let $A \in \mathcal{C}_\mathcal{O}$ be a coefficient ring equipped with the residual isomorphism $\lambda : A/\mathfrak{m}_A \xrightarrow{\sim} \mathbb{F}$, let $\tilde{\lambda} : \mathrm{G}(A) \to \mathrm{G}(\mathbb{F})$ be the homomorphism induced by λ.*

- *An A-lift (or lift to $\mathrm{G}(A)$) of $\bar{\rho}$ is a continuous representation $\rho : \mathrm{G}_\mathbb{Q} \to \mathrm{G}(A)$ such that $\bar{\rho} = \tilde{\lambda} \circ \rho$.*
- *Two A-lifts ρ and ρ' are strictly equivalent if there exists $c \in \ker \tilde{\lambda}$ such that and $c\rho c^{-1} = \rho'$.*
- *An A-deformation of $\bar{\rho}$ is a strict equivalence class of A-lifts of $\bar{\rho}$.*

We point out that if ρ and ρ' are strictly equivalent, then ρ is unramified (resp. tamely ramified) at a prime v if and only if ρ' is unramified (resp. tamely ramified) at v. Therefore, it makes sense to say that the deformation class of ρ is unramified (resp. tamely ramified) at v. Denote by $\mathrm{Def}_{\bar{\rho},\Sigma}(A)$ the set of A-deformations that are unramified at all primes outside Σ. The association $A \mapsto \mathrm{Def}_{\bar{\rho},\Sigma}(A)$ defines a covariant functor $\mathrm{Def}_{\bar{\rho},\Sigma} : \mathcal{C}_\mathcal{O} \to \mathrm{Sets}$.

Assume that the component group $\mathrm{G} / \mathrm{G}^0$ is finite étale with order coprime to p. Let $\mathbb{F}_q[\epsilon] := \mathbb{F}_q[X]/(X^2) \in \mathcal{C}_\mathcal{O}$ be the ring of dual-numbers, where $\epsilon := X$

$\bmod (X^2)$ satisfies $\epsilon^2 = 0$. It is equipped with the mod-ϵ map $\lambda : \mathbb{F}_q[\epsilon] \to \mathbb{F}_q$. The Lie-algebra of G^0 is denoted by $\mathfrak{g}$ has the following functor of points description:

$$\mathfrak{g} := \ker\{\mathrm{G}^0(\mathbb{F}_q[\epsilon]) \xrightarrow{\tilde{\lambda}} \mathrm{G}^0(\mathbb{F}_q)\}.$$

Let $\mathrm{Ad}\,\bar{\rho}$ be the $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q}}]$-module with underlying space $\mathfrak{g}$ equipped with the adjoint-action; if $X \in \mathfrak{g}$ and $g \in \mathrm{G}_{\mathbb{Q}}$,

$$g \cdot X := \bar{\rho}(g) X \bar{\rho}(g)^{-1}.$$

Let $\mu : \mathrm{G}_{\mathbb{Q},S} \to A$ be the map from G to its maximal abelian quotient A. Denote the kernel of μ by G_μ and $\mathfrak{g}_\mu$ the Lie-algebra of G_μ. Let $\mathrm{Ad}^0\,\bar{\rho}$ be the $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q}}]$-submodule of $\mathrm{Ad}\,\bar{\rho}$ with underlying vector space $\mathfrak{g}_\mu$. When $\mathrm{G} = \mathrm{GL}_n$, the Lie-algebra $\mathfrak{g}$ is the space of $n \times n$-matrices with entries in $\mathbb{F}_q$. A matrix A is identified with $\mathrm{Id}_n + \epsilon A \in \mathfrak{g}$. On the other hand, μ is the determinant and $\mathfrak{g}_\mu$ is identified with $n \times n$ matrices with trace-0 having entries in $\mathbb{F}_q$. Cohomology classes associated to $\mathrm{Ad}\,\bar{\rho}$ and $\mathrm{Ad}^0\,\bar{\rho}$ can be related to infinitesimal deformations of a given Galois representation. We introduce the notion of a small extension.

Definition 2.0.2. *Let $f : R \to S$ be a surjective map in $\mathcal{C}_{\mathcal{O}}$, the map f is said to be a small extension if*

- *the maximal ideal $\mathfrak{m}_R$ of R is principal,*
- *the map f identifies S with R/I where I is an ideal in R and $I \cdot \mathfrak{m}_R = 0$.*

Denote by $\bar{\nu}$ the composite $\bar{\nu} := \mu \circ \bar{\rho}$ and let $\psi : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_1(\mathcal{O})$ be a choice of a Galois character lifting $\bar{\nu}$. Let v be a prime number and $\bar{\rho}_v := \bar{\rho}_{\restriction \mathrm{G}_v}$. Let $\mathrm{Def}_{\bar{\rho}_v}$ be the functor of deformations of $\bar{\rho}_v$ and $\mathrm{Def}^{\psi_v}_{\bar{\rho}_v}$ the subfunctor of deformations of $\bar{\rho}_v$ with similitude character $\psi_v := \psi_{|\,\mathrm{G}_v}$.

Definition 2.0.3. *A subfunctor $\mathcal{C}_v$ of $\mathrm{Def}_{\bar{\rho}_v}$ or $\mathrm{Def}^{\psi_v}_{\bar{\rho}_v}$ is called a deformation condition if following conditions* (1) *to* (3) *stated below are satisfied; if* (4) *is also satisfied then $\mathcal{C}_v$ is said to be a liftable deformation condition,*

1. $\mathcal{C}_v(\mathbb{F}_q, \mathrm{Id}) = \bar{\rho}_v$.
2. *Let R_1 and R_2 be in $\mathcal{C}_{\mathcal{O}}$, $\rho_1 \in \mathcal{C}_v(R_1)$ and $\rho_2 \in \mathcal{C}_v(R_2)$. Let I_1 be an ideal in R_1 and I_2 an ideal in R_2 such that there is an isomorphism $\alpha : R_1/I_1 \xrightarrow{\sim} R_2/I_2$ satisfying*
$$\alpha(\rho_1 \text{ mod } I_1) = \rho_2 \text{ mod } I_2.$$
Let R_3 be the fibred product
$$R_3 = \{(r_1, r_2) \mid \alpha(r_1 \text{ mod } I_1) = r_2 \text{ mod } I_2\}$$
and $\rho_1 \times_\alpha \rho_2$ the induced R_3-representation, then $\rho_1 \times_\alpha \rho_2 \in \mathcal{C}_v(R_3)$.
3. *Let $R \in \mathcal{C}_{\mathcal{O}}$ with maximal ideal $\mathfrak{m}_R$. If $\rho \in \mathcal{F}(R)$ and $\rho \in \mathcal{C}_v(R/\mathfrak{m}_R^n)$ for all $n > 0$ it follows that $\rho \in \mathcal{C}_v(R)$. In other words, the functor $\mathcal{C}_v$ is continuous.*
4. *For every small extension $f : R \to S$ the induced map $f_* : \mathcal{C}_v(R) \to \mathcal{C}_v(S)$ is surjective.*

The *infinitesimal deformations* $\mathrm{Def}_{\bar{\rho}_v}(\mathbb{F}_q[\epsilon])$ and $\mathrm{Def}^{\psi_v}_{\bar{\rho}_v}(\mathbb{F}[\epsilon])$ are in bijection with

$$\mathrm{Def}_{\bar{\rho}_v}(\mathbb{F}_q[\epsilon]) \xrightarrow{\sim} H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar{\rho})$$

and

$$\mathrm{Def}^{\psi_v}_{\bar\rho_v}(\mathbb{F}_q[\epsilon]) \xrightarrow{\sim} H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho)$$

respectively. Any deformation $\varrho \in \mathrm{Def}_{\bar\rho_v}(\mathbb{F}_q[\epsilon])$ coincides with a cohomology class $X \in H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar\rho)$ such that $\varrho = \bar\rho_v(\mathrm{Id} + \epsilon X)$. The character $\psi_v : \mathrm{G}_v \to \mathrm{GL}_1(\mathbb{F}_q[\epsilon]])$ factors through the map induced by the structure morphism $\mathrm{GL}_1(\mathcal{O}) \to \mathrm{GL}_1(\mathbb{F}_q[\epsilon])$. It is easy to see that ψ_v is really $\iota \circ \bar\nu_v$, where ι is the inclusion of $\mathrm{GL}_1(\mathbb{F}_q) \hookrightarrow \mathrm{GL}_1(\mathbb{F}_q[\epsilon])$ and $\bar\nu_v := \bar\nu_{\restriction \mathrm{G}_v}$. Deformations $\varrho \in \mathrm{Def}_{\bar\rho_v}(\mathbb{F}_q[\epsilon])$ are those for which

$$\mu \circ \varrho = \iota \circ \bar\nu_v. \tag{2.1}$$

Expressing $\varrho = \bar\rho(\mathrm{Id} + \epsilon X)$ for a cohomology class $X \in H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar\rho)$, it may be shown that the property 2.1 is equivalent to the requirement that $X \in H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho)$.

Let $f : R \to S$ be a small extension and t a choice of a generator of I. Associated to a deformation $\varrho_S \in \mathrm{Def}_{\bar\rho_v}(S)$ is an obstruction-class $\mathcal{O}(\varrho_S) \in H^2(\mathrm{G}_v, \mathrm{Ad}\,\bar\rho)$ associated to the problem of lifting ϱ_S to $\varrho_R \in \mathrm{Def}_{\bar\rho_v}(R)$. The class $\mathcal{O}(\varrho_S)$ is nonzero if and only if there exists a deformation ϱ_R of ϱ_S. There always exists a set theoretic lift $\tau : \mathrm{G}_{\mathbb{Q},\Sigma} \to \mathrm{G}(R)$ of ϱ_S, the obstruction class is the cohomology class represented by the 2-cocycle

$$(g_1, g_2) \mapsto \tau(g_1 g_2)\tau(g_2)^{-1}\tau(g_1)^{-1}.$$

It is obvious that this class is trivial when τ may be chosen to be a group-homomorphism. Suppose that there exists a deformation ϱ_R of ϱ_S. Then the set of such deformations is an $H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar\rho)$-torsor. Any other deformation ϱ'_R may be represented as $\varrho'_R = \varrho_R(\mathrm{Id} + tX)$, where $X \in H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar\rho)$. This discussion carries over to global deformations of $\bar\rho$. Let $\varrho_S \in \mathrm{Def}_{\bar\rho,\Sigma}(S)$, the obstruction to lifting ϱ_S to $\varrho_R \in \mathrm{Def}_{\bar\rho,\Sigma}(R)$ is a global cohomology class $\mathcal{O}(\varrho_S) \in H^2(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}\,\bar\rho)$. If the obstruction class is zero, there exists a deformation ϱ_R of ϱ_S and set of deformations ϱ_R is an $H^1(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}\,\bar\rho)$-torsor. Likewise, the obstruction to lifting $\varrho_S \in \mathrm{Def}^{\psi}_{\bar\rho,\Sigma}(S)$ to $\varrho_R \in \mathrm{Def}^{\psi}_{\bar\rho,\Sigma}(R)$ is a class $\mathcal{O}(\varrho_S) \in H^2(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar\rho)$ and the set of deformations ϱ_R is an $H^1(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar\rho)$-torsor.

Set $B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ for the Borel consisting of upper-triangular matrices and let $N \subset B$ be the unipotent subgroup of B and $\mathfrak{n}$ its Lie algebra over $\mathbb{F}$. Let ψ be a character lifting $\bar\nu$. Associated to a deformation condition $\mathcal{C}_v \subseteq \mathrm{Def}^{\psi_v}_{\bar\rho_v}$ is its tangent space $\mathcal{N}_v := \mathcal{C}_v(\mathbb{F}_q[\epsilon])$. The tangent space $\mathcal{N}_v$ is an $\mathbb{F}_q$-vector subspace of $\mathrm{Def}^{\psi_v}_{\bar\rho_v}(\mathbb{F}_q[\epsilon]) = H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho)$.

Definition 2.0.4. *A deformation condition $\mathcal{C}_v$ with tangent space $\mathcal{N}_v$ is balanced if*

$$\dim \mathcal{N}_v = \begin{cases} \dim H^0(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho) + \dim \mathfrak{n} \text{ if } v = p, \\ \dim H^0(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho) \text{ otherwise.} \end{cases}$$

Denote by $\mathcal{N}_v^{\perp}$ the annihiliator of $\mathcal{N}_v$ with respect to the local Tate pairing

$$H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho) \times H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar\rho^*) \to \mathbb{F}_q.$$

In our applications, we shall assume that there exist balanced liftable deformation conditions at each prime $v \in \Sigma$. In order to motivate this terminology we are led to a discussion on the Selmer group associated with the data $\mathcal{N} = \{\mathcal{N}_v\}_{v \in \Sigma}$.

Definition 2.0.5. *The Selmer group associated to $\mathcal{N}$ is defined by local conditions*

$$H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}) := \ker \left\{ H^1(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}) \to \bigoplus_{v\in\Sigma} H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})/\mathcal{N}_v \right\}.$$

The dual Selmer group is defined by the local conditions $\mathcal{N}^\perp$

$$H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}^*) := \ker \left\{ H^1(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}^*) \to \bigoplus_{v\in\Sigma} H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho}^*)/\mathcal{N}_v^\perp \right\}.$$

The Selmer data $\mathcal{N}$ is said to balanced if $\mathcal{N}_v$ is balanced for each $v \in \Sigma$. The dimension of the Selmer group $H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho})$ is denoted by $h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho})$. Likewise, the dimension of the dual Selmer group $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}^*)$ is denoted $h^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}^*)$. The following is a direct consequence of a formula due to Wiles (cf. [16, Theorem 8.7.9]).

Proposition 2.0.6. *If $\mathcal{N}$ is balanced,*

$$h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}) - h^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},\Sigma}, \mathrm{Ad}^0\,\bar{\rho}^*) = 0.$$

CHAPTER 3

GENERALIZATION TO HIGHER DIMENSIONS

It is natural to investigate if the 2-dimensional lifting theorem of Hamblen and Ramakrishna generalizes to higher dimensional Galois representations. The prospect of generalizing this lifting result leads us to examine higher dimensional Galois representations with image in a smooth subgroup-scheme G of GL_n. Assume that G is defined over $\mathrm{W}(\mathbb{F}_q)$ such that G^0 is a split connected reductive group. Suppose $\mathrm{B} \subset \mathrm{G}$ is a choice of a Borel containing a split torus and $\bar{\rho}$ is a homomorphism

$$\bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{G}(\mathbb{F}_q).$$

Let $\mathfrak{g}$ denote the Lie-algebra of the adjoint group G^{ad} over $\mathbb{F}_q$. The $\mathbb{F}_q$-vector space $\mathfrak{g}$ acquires an adjoint Galois action

$$\mathrm{Ad}^0 \bar{\rho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_q}(\mathfrak{g}).$$

Denote by $\mathrm{Ad}^0 \bar{\rho}$ the Galois module with underlying vector space $\mathfrak{g}$. It is imperative that $\bar{\rho}$ is *odd*. For an element $h \in \mathrm{G}(\mathbb{F}_q)$, denote by $(\mathrm{Ad}^0 \bar{\rho})^h$ the subspace of $\mathrm{Ad}^0 \bar{\rho}$ fixed by h. We observe that

$$\dim(\mathrm{Ad}^0 \bar{\rho})^h \leq \dim \mathrm{G} - \dim \mathrm{B}\,.$$

The representation $\bar{\rho}$ is *odd* if equality is achieved for the image of complex conjugation c, i.e.

$$\dim(\mathrm{Ad}^0 \bar{\rho})^{\bar{\rho(c)}} = \dim \mathrm{G} - \dim \mathrm{B}\,. \tag{3.1}$$

In particular, the group G must contain an element $h = \bar{\rho}(c)$ for which equality 3.1 is achieved. Such an element is said to induce a *split Cartan-involution*.

When $n > 2$, the general linear group $\mathrm{GL}_n(\mathbb{F}_q)$ contains no such element. Hence there are no odd representations for the group $\mathrm{GL}_n(\mathbb{F}_q)$ when $n > 2$. On the other hand, the general symplectic group $\mathrm{GSp}_{2n}(\mathbb{F}_q)$ does contain elements which induce split Cartan involutions. In [18], Patrikis generalized Ramakrishna's lifting theorem to representations with *big image* in $\mathrm{GSp}_{2n}(\mathbb{F}_q)$. Further generalizations were obtained by Fakhruddin, Khare and Patrikis in [4] and [5].

We assume that our representation has image in $\mathrm{GSp}_{2n}(\mathbb{F}_q)$ for $n \geq 2$. Associate to a commutative $\mathrm{W}(\mathbb{F}_q)$-algebra R, a non-degenerate alternating form on R^{2n} prescribed by the matrix

$$J := \begin{pmatrix} & \mathrm{Id}_n \\ -\mathrm{Id}_n & \end{pmatrix}.$$

The group of general symplectic matrices $\mathrm{GSp}_{2n}(R)$ consists of matrices X which preserve this form up to a scalar i.e. satisfy $X^t J X \in R^\times \cdot J$. The similitude character $\nu : \mathrm{GSp}_{2n}(R) \to R^\times$ is defined by the relation $X^t J X = \nu(X) \cdot J$. The space $\mathrm{Ad}^0 \bar{\rho}$ is an $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$-module with underlying space $\mathrm{sp}_{2n}(\mathbb{F}_q)$. The Galois action is prescribed by

$$g \cdot X = \bar{\rho}(g) X \bar{\rho}(g)^{-1}$$

where $g \in \mathrm{G}_{\mathbb{Q},S}$ and $X \in \mathrm{sp}_{2n}(\mathbb{F}_q)$. Let $\mathrm{B}(\mathbb{F}_q)$ be the Borel subgroup consisting of matrices

$$M = \begin{pmatrix} C & CD \\ & \xi(C^t)^{-1} \end{pmatrix}$$

where $C \in \mathrm{GL}_n(\mathbb{F}_q)$ is upper triangular, $D \in \mathrm{GL}_n(\mathbb{F}_q)$ is symmetric and $\xi \in R^\times$. Denote by $U_1 \subset \mathrm{B}$ be the unipotent subgroup.

Let $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GSp}_{2n}(\mathbb{F}_q)$ be a continuous Galois representation with image in $\mathrm{B}(\mathbb{F}_q)$. Composing $\bar{\rho}$ with the similitude-character $\bar{\nu}$ defines a Galois character denoted by $\bar{\kappa}$. Denote by $\mathcal{T} \subseteq \mathrm{GSp}_{2n}$ the diagonal torus and $e_{i,j} \in \mathrm{GL}_{2n}(\mathbb{F}_q)$ the matrix with 1 in the (i,j)-position and 0 in all other positions. Set $\mathfrak{t}$ for the $\mathbb{F}_q$-span of $H_1, \dots, H_n$, where $H_i := e_{i,i} - e_{n+i,n+i}$. Let $L_1, \dots, L_n \in \mathfrak{t}^*$ be the dual basis of $H_1, \dots, H_n$. An integer linear combination λ of $L_1, \dots, L_n$ is viewed as character on the torus $\mathcal{T}(\mathbb{F}_q)$, which is trivial on the center of $\mathrm{GSp}_{2n}(\mathbb{F}_q)$. Via the natural quotient map $\mathrm{B} \to \mathcal{T}$, a character on $\mathcal{T}$ induces a character on B. The character on B induced by λ is denoted by

$$\omega_\lambda : \mathrm{B}(\mathbb{F}_q) \to \mathbb{F}_q^\times.$$

Associated to ω_λ is the Galois character

$$\sigma_\lambda = \omega_\lambda \circ \bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathbb{F}_q^\times.$$

Let "1" be a formal symbol for the trivial linear combination of $L_1, \dots, L_n$ and set σ_1 equal to the trivial character. The roots $\Phi = \Phi(\mathrm{Ad}^0\,\bar{\rho}, \mathfrak{t})$ are specified by

$$\begin{aligned} \Phi = &\{\pm 2L_1, \dots, \pm 2L_n\} \\ &\cup \{\pm(L_i + L_j) \mid 1 \le i < j \le n\} \\ &\cup \{\pm(L_i - L_j) \mid 1 \le i < j \le n\}. \end{aligned}$$

The choice of the Borel $\mathrm{B} \subset \mathrm{GSp}_{2n}$ prescribes the following choice of simple roots $\Delta = \{\lambda_i \mid i = 1, \ldots, n\}$, with $\lambda_i := L_i - L_{i+1}$ for $i < n$ and $\lambda_n := 2L_n$. The root $2L_1 = 2\left(\sum_{i=1}^{n-1} \lambda_i\right) + \lambda_n$ is the highest root and the unique root of height $2n-1$. Denote by $\mathfrak{b}$ and $\mathfrak{n}$ the Lie subalgebras of $\mathrm{Ad}^0 \bar{\rho}$ corresponding to the Borel and unipotent subgroups respectively. Set $\bar{\chi}$ for the mod-p cyclotomic character and c for complex conjugation.

Theorem 3.0.1. *Let $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{B}(\mathbb{F}_q)$ be a Galois representation of the form:*

$$\bar{\rho} = \begin{pmatrix} \varphi_1 & * & * & \cdots & * & * & \cdots & * \\ & \varphi_2 & * & \cdots & * & * & \cdots & * \\ & & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ & & & \varphi_n & * & * & \cdots & * \\ & & & & \varphi_1^{-1}\bar{\kappa} & & & \\ & & & & * & \varphi_2^{-1}\bar{\kappa} & & \\ & & & & \vdots & \vdots & \ddots & \\ & & & & * & * & \cdots & \varphi_n^{-1}\bar{\kappa} \end{pmatrix}$$

and let S be a finite set of primes which contains p. Assume that the following conditions are satisfied:

1. $p > 2n$,
2. *$\bar{\rho}$ is odd, i.e.* $\dim(\mathrm{Ad}^0 \bar{\rho})^{\bar{\rho}(c)} = \dim \mathfrak{n}$.
3. *The image of $\bar{\rho}$ contains the unipotent subgroup $\mathrm{U}_1(\mathbb{F}_q)$.*

4. *Both the following conditions on the distinctness of the characters $\{\sigma_\lambda\}$ are satisfied:*

   (a) *For $\lambda, \lambda' \in \Phi \cup \{1\}$ such that $\lambda \neq \lambda'$, σ_λ is not a $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$-twist of $\sigma_{\lambda'}$.*

   (b) *Moreover for $\lambda, \lambda' \in \Phi \cup \{1\}$ not necessarily distinct, σ_λ is not a $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$-twist of $\bar{\chi}\sigma_{\lambda'}$.*

5. *For each of the roots $\lambda \in \Phi$, the $\mathbb{F}_p$-linear span of the image of σ_λ in $\mathbb{F}_q$ is $\mathbb{F}_q$.*

6. *At each prime $v \in S$ such that $v \neq p$, there is a liftable local deformation condition $\mathcal{C}_v$ with tangent space $\mathcal{N}_v$ of dimension*

$$\dim \mathcal{N}_v = h^0(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}).$$

7. *Tilouine's regularity conditions* (REG) *and* $(\mathrm{REG})^*$ *are satisfied, i.e.*

$$H^0(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho}/\mathfrak{b}) = 0 \text{ and } H^0(\mathrm{G}_p, (\mathrm{Ad}^0 \bar{\rho}/\mathfrak{b})(\bar{\chi})) = 0.$$

Let κ be a fixed choice of a lift of the character $\bar{\kappa}$. Then $\exists$ a finite set of auxiliary primes X disjoint from S and a lift ρ

$$\begin{array}{ccccc} & & & & \mathrm{GSp}_{2n}(W(\mathbb{F}_q)) \\ & \rho \nearrow & & & \downarrow \\ \mathrm{G}_{\mathbb{Q}, S \cup X} & \longrightarrow & \mathrm{G}_{\mathbb{Q}, S} & \xrightarrow{\bar{\rho}} & \mathrm{GSp}_{2n}(\mathbb{F}_q). \end{array}$$

for which

1. *ρ is irreducible,*

2. *ρ is p-ordinary,*

3. *$\nu \circ \rho = \kappa$,*

4. *for $v \in S \backslash \{p\}$, the restriction to the decomposition group $\rho_{\restriction \mathrm{G}_v} \in \mathcal{C}_v$.*

The lift ρ is geometric in the sense of Fontaine and Mazur. For $\lambda \in \Phi$, setting $\lambda = -\lambda'$ in condition (4), we have that $\sigma_\lambda^2 \neq 1$. Note that the conditions also imply that $\sigma_\lambda \neq \bar{\chi}, \bar{\chi}^{-1}$. This is reminiscent of the condition $\varphi^2 \neq 1$ of Hamblen-Ramakrishna. It is a consequence of Tilouine's regularity conditions that the ordinary deformations of $\bar{\rho}_{\restriction \mathrm{G}_p}$ constitute a liftable deformation condition $\mathcal{C}_p$ for which the tangent space $\mathcal{N}_p$ has dimension:

$$\dim \mathcal{N}_p = h^0(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho}) + \dim \mathfrak{n}.$$

For a discussion on the ordinary deformation condition and Tilioune's regularity conditions, the reader may refer to [19, section 4]. With reference to condition (6), the reader may consult [19, sections 4.3 and 4.4] for examples of such deformation conditions.

3.1 Notation

In this short section, we summarize some notation used in this chapter.

- For an $\mathbb{F}_q$-vector space M, set $\dim M := \dim_{\mathbb{F}_q} M$.

- At every prime v, choose an embedding $\iota_v : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_v$. The absolute Galois group $\mathrm{G}_v = \mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v)$ is identified with the decomposition group of the prime dividing v determined by ι_v.

- Let $e_{i,j}$ denote the $2n \times 2n$ square matrix with coefficients in $\mathbb{F}_q$ with 1 in the (i,j)-th position and 0 at all other positions.

- The space $\mathrm{Ad}^0 \bar{\rho}$ is an $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$-module with underlying space $\mathrm{sp}_{2n}(\mathbb{F}_q)$. The Galois action is prescribed by

$$g \cdot X = \bar{\rho}(g) X \bar{\rho}(g)^{-1}$$

where $g \in \mathrm{G}_{\mathbb{Q},S}$ and $X \in \mathrm{sp}_{2n}(\mathbb{F}_q)$.

- The space of diagonal matrices in $\mathrm{Ad}^0 \bar{\rho}$ is denoted by $\mathfrak{t}$. Let $H_1, \dots, H_n$ be the basis of $\mathfrak{t}$ defined by $H_i := e_{i,i} - e_{n+i,n+i}$. Let $L_1, \dots, L_n \in \mathfrak{t}^*$ be the dual basis.

- Let Φ be the set of roots of $\mathrm{sp}_{2n}(\mathbb{F}_q)$ and $\lambda_1, \dots, \lambda_n \in \Phi$ be the simple roots defined as follows

$$\lambda_i := \begin{cases} L_i - L_{i+1} \text{ for } i < n \\ 2L_n \text{ for } i = n. \end{cases}$$

Let Δ be the simple roots $\{\lambda_1, \dots, \lambda_n\}$. Let Φ^+ and Φ^- denote the positive and negative roots respectively.

- For $\lambda \in \Phi$, let $\mathrm{sp}_{2n}(\mathbb{F}_q)_\lambda$ be the λ root-subspace. Denote $(\mathrm{Ad}^0 \bar{\rho})_\lambda$ the subspace of $\mathrm{Ad}^0 \bar{\rho}$ corresponding to $\mathrm{sp}_{2n}(\mathbb{F}_q)_\lambda$. For $\lambda \in \Phi$, let X_λ be a choice a root vector generating the one-dimensional space $(\mathrm{Ad}^0 \bar{\rho})_\lambda$. For instance when

$n = 2$, we may choose root vectors as follows,

$$X_{2L_1} := \begin{pmatrix} 0 & & 1 & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix}, X_{2L_2} := \begin{pmatrix} 0 & & & \\ & 0 & & 1 \\ & & 0 & \\ & & & 0 \end{pmatrix},$$

$$X_{L_1+L_2} := \begin{pmatrix} 0 & & & 1 \\ & 0 & 1 & \\ & & 0 & \\ & & & 0 \end{pmatrix} \text{ and } X_{L_1-L_2} := \begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & 0 & \\ & & -1 & 0 \end{pmatrix}.$$

For $\lambda \in \Phi^-$, we may choose X_λ to be the transpose of $X_{-\lambda}$.

- Let λ be a root. There is a unique presentation of $\lambda = \sum \alpha_i \lambda_i$, where α_i are all non-negative or all non-positive. The height of λ is defined by $\mathrm{ht}(\lambda) := \sum_i \alpha_i$. For instance, the root $2L_1 = 2\left(\sum_{i=1}^{n-1} \lambda_i\right) + \lambda_n$ has height equal to $2n-1$. Every other root has height less than $2n-1$.

- For any integer k, let $(\mathrm{Ad}^0 \bar{\rho})_k$ be the $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$-submodule defined by

$$(\mathrm{Ad}^0 \bar{\rho})_k := \bigoplus_{\substack{\alpha \in \Phi \\ \mathrm{ht}\alpha \geq k}} (\mathrm{Ad}^0 \bar{\rho})_\alpha.$$

 Set $\mathfrak{b} := (\mathrm{Ad}^0 \bar{\rho})_0$ and $\mathfrak{n} := (\mathrm{Ad}^0 \bar{\rho})_1$.

- Associated with any root λ is a Galois character denoted by $\sigma_\lambda : \mathrm{G}_{\mathbb{Q},S} \to \mathbb{F}_q^\times$ obtained by composing $\bar{\rho}$ with the character induced on $\mathrm{B}(\mathbb{F}_q)$ by the root λ. Denote by σ_1 the trivial character and set $\mathrm{ht}(1) = 0$. For $\lambda \in \Phi \cup \{1\}$, we have that

$$g \cdot X_\lambda - \sigma_\lambda(g) X_\lambda \in (\mathrm{Ad}^0 \bar{\rho})_{\mathrm{ht}(\lambda)+1}.$$

- Let $Q \subseteq \mathrm{Ad}^0 \bar{\rho}$ be an $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$-submodule, the σ_{2L_1}-eigenspace of Q is the $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$-submodule defined by $Q_{\sigma_{2L_1}} := Q \cap (\mathrm{Ad}^0 \bar{\rho})_{2L_1}$. Likewise, if $P \subseteq$

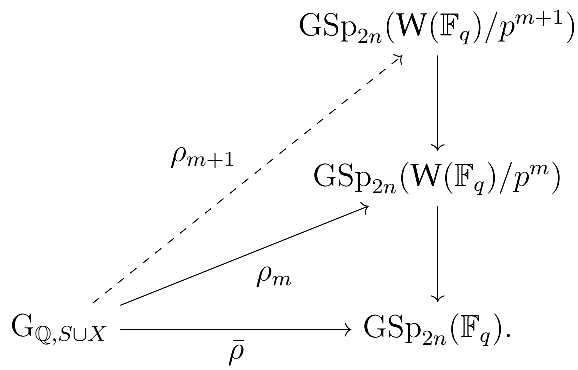
$\mathrm{Ad}^0\,\bar{\rho}^*$ is an $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$-submodule, the $\bar{\chi}\sigma_{2L_1}$-eigenspace $P_{\bar{\chi}\sigma_{2L_1}}$ is defined by

$$P_{\bar{\chi}\sigma_{2L_1}} := \{v \in P \mid v(X) = 0 \text{ for } X \in (\mathrm{Ad}^0\,\bar{\rho})_{-2n+2}\}.$$

- For $k \geq 1$, let $U_k \subset \mathrm{B}(\mathbb{F}_q)$ be the exponential subgroup generated by $\exp((\mathrm{Ad}^0\,\bar{\rho})_k)$. The group U_1 is the unipotent subgroup of $\mathrm{B}(\mathbb{F}_q)$.
- Throughout, h^i will be an abbreviation for $\dim H^i$. For instance, $h^i(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$ is an abbreviation for $\dim H^i(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$.
- Let M be an $\mathbb{F}_q[\mathrm{G}_S]$-module, let $Ш^i_S(M)$ consist of cohomology classes $f \in H^i(\mathrm{G}_{\mathbb{Q},S}, M)$ such that $f_{\restriction \mathrm{G}_v} = 0$ for all $v \in S$.

3.2 The General Lifting Strategy

Let $\bar{\varrho}$ be a Galois representation $\bar{\varrho} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ which is irreducible, odd and unramified outside finitely many primes. Ramakrishna in [23] and [25] showed that if $\bar{\varrho}$ satisfies additional conditions, it lifts to a Galois representation ϱ which is geometric in the sense of Fontaine and Mazur. In other words, ϱ is odd, unramified outside finitely many primes and $\varrho_{\restriction \mathrm{G}_p}$ is de Rham. This geometric lifting theorem provided evidence for the weak version of Serre's conjecture before it was proved by Khare and Wintenberger. The geometric lifting construction was adapted to the reducible setting in [9]. The main result of this manuscript is a higher dimensional generalization of the lifting theorem of Hamblen-Ramakrishna. The basic strategy involves successively lifting $\bar{\rho}$ to a characteristic zero irreducible geometric representation ρ by successively lifting ρ_m to ρ_{m+1}



Definition 3.2.1. *Let $\mathcal{C}$ be the category of coefficient rings over $\mathrm{W}(\mathbb{F}_q)$ with residue field $\mathbb{F}_q$. The objects of this category consist of local $\mathrm{W}(\mathbb{F}_q)$-algebras $(R, \mathfrak{m})$ for which*

- *R is complete and Noetherian,*
- *$R/\mathfrak{m}$ is isomorphic to $\mathbb{F}_q$ as a $\mathrm{W}(\mathbb{F}_q)$-algebra. The residual map*

$$\phi : R \to \mathbb{F}_q$$

  is the composite of the quotient map $R \to R/\mathfrak{m}$ with the unique isomorphism of $W(\mathbb{F}_q)$-algebras $R/\mathfrak{m} \xrightarrow{\sim} \mathbb{F}_q$.

A morphism $F : (R_1, \mathfrak{m}_1) \to (R_2, \mathfrak{m}_2)$ is a homorphism of local rings which is also a $\mathrm{W}(\mathbb{F}_q)$-algebra homorphism. Letting $\phi_i : R_i \to \mathbb{F}_q$ denote residual map to $\mathbb{F}_q$, it is further required that F be compatible with ϕ_1 and ϕ_2, i.e. $\phi_2 \circ F = \phi_1$. Recall that κ is a fixed choice of lift of $\bar{\kappa}$. Let κ_v denote the restriction of κ to G_v.

Let v be a prime and $R \in \mathcal{C}$. Denote by $\phi^* : \mathrm{GSp}_{2n}(R) \to \mathrm{GSp}_{2n}(\mathbb{F}_q)$ the group homomorphism induced by the residual homomorphism $\phi : R \to \mathbb{F}_q$. We say that $\rho_R : \mathrm{G}_v \to \mathrm{GSp}_{2n}(R)$ is an R-lift of $\bar{\rho}_{\restriction \mathrm{G}_v}$ if $\phi^* \circ \rho_R = \bar{\rho}_{\restriction \mathrm{G}_v}$, i.e. the following diagram commutes

$$\begin{array}{ccc} & & \mathrm{GSp}_{2n}(R) \\ & \overset{\rho_R}{\nearrow} & \Big\downarrow \phi^* \\ \mathrm{G}_v & \xrightarrow[\bar{\rho}_{\restriction \mathrm{G}_v}]{} & \mathrm{GSp}_{2n}(\mathbb{F}_q). \end{array}$$

Further, we shall require that the similitude character of ρ_R coincides with the composite of κ_v with the homomorphism $W(\mathbb{F}_q)^\times \to R^\times$ induced by the structure map.

Two lifts ρ_R and ρ'_R are said to strictly-equivalent if there is

$$A \in \ker\{\mathrm{GSp}_{2n}(R) \xrightarrow{\phi^*} \mathrm{GSp}_{2n}(\mathbb{F}_q)\}$$

such that $\rho_R = A\rho'_R A^{-1}$. A deformation is a strict equivalence class of lifts. Let $\mathrm{Def}_v(R)$ be the set of R-deformations of $\bar{\rho}_{\restriction \mathrm{G}_v}$. The association $R \mapsto \mathrm{Def}_v(R)$ defines a covariant functor

$$\mathrm{Def}_v : \mathcal{C} \to \mathrm{Sets}\,.$$

The tangent space $\mathrm{Def}_v(\mathbb{F}_q[\epsilon]/(\epsilon^2))$ naturally acquires the structure of an $\mathbb{F}_q$-vector space and is isomorphic to $H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$. Under this association, a cohomology class f is identified with the deformation $(\mathrm{Id} + \epsilon f)\bar{\rho}_{\restriction \mathrm{G}_v}$.

For $m \in \mathbb{Z}_{\geq 2}$, the deformations $\mathrm{Def}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$ are equipped with action of the cohomology group $H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$. For $\varrho_m \in \mathrm{Def}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$ and $f \in$

$H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$, the twist of ϱ_m by f is defined by the formula $(\mathrm{Id} + p^{m-1}f)\varrho_m$. The set of deformations ϱ_m of a fixed $\varrho_{m-1} \in \mathrm{Def}_v(\mathrm{W}(\mathbb{F}_q)/p^{m-1})$ is either empty or in bijection with $H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$.

Definition 3.2.2. *We say that a sub-functor $\mathcal{C}_v$ of Def_v is a deformation condition if (1) to (3) below are satisfied. If condition (4) is satisfied, $\mathcal{C}_v$ is said to be liftable.*

1. *First, we require that $\mathcal{C}_v(\mathbb{F}_q) = \{\bar{\rho}_{\restriction \mathrm{G}_v}\}$.*
2. *For R_1 and R_2 be $\mathcal{C}$, let $\rho_1 \in \mathcal{C}_v(R_1)$ and $\rho_2 \in \mathcal{C}_v(R_2)$. Let I_1 be an ideal in R_1 and I_2 an ideal in R_2 such that there is an isomorphism $\alpha : R_1/I_1 \xrightarrow{\sim} R_2/I_2$ satisfying*

   $$\alpha(\rho_1\ mod I_1) = \rho_2\ mod I_2.$$

   Let R_3 be the fibred product

   $$R_3 = \{(r_1, r_2) \mid \alpha(r_1 mod I_1) = r_2 mod I_2\}$$

   and ρ_3 the R_3-deformation induced from ρ_1 and ρ_2. Then ρ_3 satisfies $\mathcal{C}_v(R_3)$.
3. *Let $R \in \mathcal{C}$ with maximal ideal $\mathfrak{m}_R$. If $\rho \in \mathrm{Def}_v(R)$ is such that $\rho \mod \mathfrak{m}_R^n$ satisfies $\mathcal{C}_v$ for all $n \in \mathbb{Z}_{\geq 1}$, then ρ also satisfies $\mathcal{C}_v$.*
4. *Let $R \in \mathcal{C}$ and I an ideal such that $I.\mathfrak{m}_R = 0$. For $\rho \in \mathcal{C}_v(R/I)$, there exists $\tilde{\rho} \in \mathcal{C}_v(R)$ such that $\rho = \tilde{\rho} \mod I$.*

Let $\mathcal{C}_v$ be a local deformation condition at the prime v. By Schlessinger's theorem, there is a universal deformation

$$\rho_v^{univ} : \mathrm{G}_v \to \mathrm{GSp}_{2n}(R_v),$$

i.e., ρ_v^{univ} represents $\mathcal{C}_v$. The functor $\mathcal{C}_v$ is liftable if and only if the deformation ring R_v is smooth. The tangent space $\mathcal{N}_v := \mathcal{C}_v(\mathbb{F}_q[\epsilon]/(\epsilon^2))$ is identified with a subspace of $H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$. The action of $\mathcal{N}_v$ on $\mathrm{Def}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$ stabilizes $\mathcal{C}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$. In other words, if $\varrho_m \in \mathcal{C}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$ and $f \in \mathcal{N}_v$, then

$$(\mathrm{Id} + p^{m-1} f)\varrho_m \in \mathcal{C}_v(\mathrm{W}(\mathbb{F}_q)/p^m).$$

It is assumed that each prime $v \in S\backslash\{p\}$ is equipped with a liftable local deformation condition $\mathcal{C}_v$ such that

$$\dim \mathcal{N}_v = h^0(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho}).$$

The reader may consult [19, sections 4.3 and 4.4] for examples of such deformation conditions. The deformation condition $\mathcal{C}_p$ is the ordinary deformation condition. Since we have assumed that Tilouine's regularity conditions are satisfied (cf. [19, section 4.1]), $\mathcal{C}_p$ is liftable and the tangent space $\mathcal{N}_p$ has dimension equal to

$$\dim \mathcal{N}_p = h^0(\mathrm{G}_p, \mathrm{Ad}^0\,\bar{\rho}) + \dim \mathfrak{n},$$

see [19, Proposition 4.4]. We allow the successive lifts ρ_m to be ramified at a set of primes $S \cup X$. Each auxiliary prime $v \in X$ is equipped with a liftable subfunctor $\mathcal{C}_v$ of Def_v which is not a deformation condition in the sense of Definition 3.2.2. In fact, the deformation problem $\mathcal{C}_v$ is not representable. These auxiliary primes are referred to as trivial primes and were introduced by Hamblen and Ramakrishna in the two-dimensional setting [9, section 4]. We use a higher dimensional generalization due to Fakhruddin, Khare and Patrikis [4, Definition 3.1]. At each trivial prime v there is a subspace $\mathcal{N}_v$ of $H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$ of dimension $h^0(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$ which behaves like a versal tangent space. For $m \geq 3$, the action of $\mathcal{N}_v$ on $\mathrm{Def}(\mathrm{W}(\mathbb{F}_q)/p^m)$ stabilizes $\mathcal{C}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$. However, this is not the case for $m = 2$.

Let X be a finite set of trivial primes disjoint from S. For $v \in S \cup X$, set $\mathcal{N}_v^{\perp} \subseteq H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}^*)$ to be the orthogonal complement of $\mathcal{N}_v$ with respect to the non-degenerate Tate pairing

$$H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}) \times H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}^*) \rightarrow H^2(\mathrm{G}_v, \mathbb{F}_q(\bar{\chi})) \xrightarrow{\sim} \mathbb{F}_q.$$

Set $\mathcal{N}_\infty = 0$ and $\mathcal{N}_\infty^{\perp} = 0$. The Selmer-condition $\mathcal{N}$ is the tuple $\{\mathcal{N}_v\}_{v \in S \cup X \cup \{\infty\}}$ and the dual Selmer condition $\mathcal{N}^{\perp}$ is $\{\mathcal{N}_v^{\perp}\}_{v \in S \cup X \cup \{\infty\}}$. Attached to $\mathcal{N}$ and $\mathcal{N}^{\perp}$ are the Selmer and dual-Selmer groups:

$$H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}) = \text{ker}\left\{ H^1(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}) \xrightarrow{\mathrm{res}_{S\cup X}} \bigoplus_{v \in S \cup X} \frac{H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_v} \right\}$$

and

$$H^1_{\mathcal{N}^{\perp}}(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}^*) = \text{ker}\left\{ H^1(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}^*) \xrightarrow{\mathrm{res}'_{S\cup X}} \bigoplus_{v \in S \cup X} \frac{H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}^*)}{\mathcal{N}_v^{\perp}} \right\}$$

respectively. The following formula is due to Wiles (see [16, Theorem 8.7.9]):

$$\begin{aligned} h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}) - h^1_{\mathcal{N}^{\perp}}(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}^*) &= h^0(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}^0 \bar{\rho}) - h^0(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}^0 \bar{\rho}^*) \\ &+ \sum_{v \in S \cup X \cup \{\infty\}} \left(\dim \mathcal{N}_v - h^0(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}) \right). \end{aligned} \tag{3.2}$$

Since $\bar{\rho}$ is odd, one has that $h^0(\mathrm{G}_\infty, \mathrm{Ad}^0 \bar{\rho}) = \dim \mathfrak{n}$. It follows from the above formula that the dimensions of the Selmer group and dual Selmer group coincide, i.e.

$$h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}) = h^1_{\mathcal{N}^{\perp}}(\mathrm{G}_{\mathbb{Q}, S\cup X}, \mathrm{Ad}^0 \bar{\rho}^*).$$

The Selmer and dual Selmer groups fit into a long exact sequence called the Poitou-Tate sequence. We only point out that the cokernel of $\mathrm{res}_{S\cup X}$ injects into $H^1_{\mathcal{N}^\perp}(\mathrm{S}_{S\cup X}, \mathrm{Ad}^0\,\bar{\rho}^*)^\vee$. In particular, if the Selmer group is zero, then so is the dual Selmer group, in which case the restriction map $\mathrm{res}_{S\cup X}$ is an isomorphism. Since the spaces $\mathcal{N}_v$ at a trivial prime v stabilize lifts only past mod p^3, it becomes necessary to produce a mod p^3 lift ρ_3 of $\bar{\rho}$ before applying the general lifting-strategy. All deformations ρ_m discussed in this paper will have similitude character equal to $\kappa \mod p^m$.

The three main steps are as follows:

1. first it is shown that there is a finite set of trivial primes X_1 disjoint from S such that the representation $\bar{\rho}$ lifts to a mod p^2 representation ρ_2 which is unramified outside $S \cup X_1$.
2. On adapting the methods of Khare, Larsen and Ramakrishna from [11], it is shown that there is a finite set of trivial primes $X_2 \supset X_1$ disjoint from S and a mod p^3 lift ρ_3 of ρ_2 which satisfies the following conditions
    - ρ_3 is irreducible, i.e. does not contain a free rank one Galois stable $\mathrm{W}(\mathbb{F}_q)/p^3$-submodule.
    - It is unramified outside $S \cup X_2$.
    - The lift ρ_3 is also arranged to satisfy conditions $\mathcal{C}_v$ at each prime $v \in S \cup X_2$.
3. At this stage, all that remains to be shown is that the set of primes X_2 may

be further enlarged to a set of trivial primes X which is disjoint from S such that the Selmer group $H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho})$ is equal to zero.

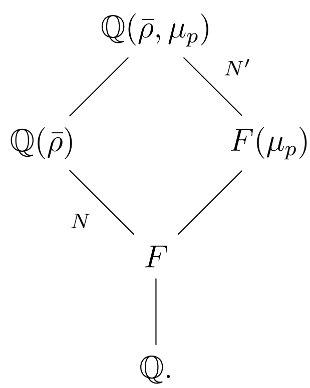
The rest of the argument warrants some explanation. Since the Selmer group is zero, the map $\mathrm{res}_{S\cup X}$ is an isomorphism. Suppose for $m \geq 3$ and ρ_m is a mod p^m lift of ρ_3 which is unramified outside $S \cup X$ and satisfies the conditions $\mathcal{C}_v$ at each prime $v \in S \cup X$. We show that ρ_m may be lifted to ρ_{m+1} which satisfies the same conditions. Since the dual Selmer group is zero, so is $Ш^1_{S\cup X}(\mathrm{Ad}^0\,\bar{\rho}^*)$, and it follows from global-duality that $Ш^2_{S\cup X}(\mathrm{Ad}^0\,\bar{\rho})$ is zero. Since local condition $\mathcal{C}_v$ is liftable, there are no local obstructions to lifting ρ_m. The cohomological obstruction to lifting ρ_m to ρ_{m+1} is a class in $Ш^2_{S\cup X}(\mathrm{Ad}^0\,\bar{\rho})$ and hence is zero. As a result, ρ_m does lift one more step to ρ_{m+1}. In order to complete the inductive argument, it is shown that ρ_{m+1} satisfies the conditions $\mathcal{C}_v$. After picking a suitable global cohomology class $z \in H^1(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho})$ and replacing ρ_{m+1} by its twist $(\mathrm{Id} + p^m z)\rho_{m+1}$, this may be arranged. At each prime $v \in S \cup X$, there is a cohomology class $z_v \in H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})$ such that the twist $(\mathrm{Id} + p^m z_v)\rho_{m+1 \restriction \mathrm{G}_v}$ satisfies $\mathcal{C}_v$. Since we assume that $m \geq 3$, we have that $\mathcal{N}_v$ stabilizes $\mathcal{C}_v$. For $v \in S \cup X$, the elements z_v are defined modulo $\mathcal{N}_v$. Since $\mathrm{res}_{S\cup X}$ is an isomorphism, the tuple

$$(z_v) \in \bigoplus_{v\in S\cup X} \frac{H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho})}{\mathcal{N}_v}$$

arises from a unique global cohomology class z which is unramified outside $S \cup X$. After replacing ρ_{m+1} by $(\mathrm{Id} + p^m z)\rho_{m+1}$, it satisfies the conditions $\mathcal{C}_v$ at each prime $v \in S \cup X$. This completes the inductive lifting argument.

3.3 Preliminaries

In this section, we prove a number of Galois theoretic results which will be applied in later sections. Let M be a finite abelian group with $\mathrm{G}_{\mathbb{Q}}$-action and E be a number field. Denote by $E(M)$ the extension of E *cut out* by M. In other words, it is the Galois extension of E which is fixed by the kernel of the action of G_E on M. Let $M_1, \dots, M_k$ be finite abelian groups on which $\mathrm{G}_{\mathbb{Q}}$ acts. Denote by $E(M_1, \dots, M_k)$ the composite of the fields $E(M_1) \cdots E(M_k)$. Let $K := \mathbb{Q}(\bar{\rho}, \mu_p)$ and $L := \mathbb{Q}(\bar{\rho})$ and set $G' := \mathrm{Gal}(K/\mathbb{Q})$ and $G := \mathrm{Gal}(L/\mathbb{Q})$. Let F be the subfield $\mathbb{Q}(\{\varphi_i\}_{1 \leq i \leq n}, \bar{\kappa})$ of L. Denote by $N' := \mathrm{Gal}(K/F(\mu_p))$ and $N := \mathrm{Gal}(\mathbb{Q}(L/F)$. The groups G, G', N and N' are depicted in the following field diagram



Condition (3) of Theorem 3.0.1 asserts that the image of $\bar{\rho}$ contains $U_1(\mathbb{F}_q)$. Therefore N may be identified with $\bar{\rho}(N) = U_1(\mathbb{F}_q)$. In particular the abelianization N^{ab} may be identified with $U_1(\mathbb{F}_q)/U_2(\mathbb{F}_q)$. Since N is a p-group and $[F(\mu_p) : F]$ is coprime to p, it follows that $\mathbb{Q}(\bar{\rho})$ and $F(\mu_p)$ are linearly disjoint over F. It follows that N is canonically isomorphic to N'. The inclusion of $\mathcal{T}$ into B is a section of the quotient map $\mathrm{B} \to \mathcal{T}$. This induces a semi-direct product decomposition $\mathrm{B} = U_1 \rtimes \mathcal{T}$. Let $\mathcal{T}'$ be the intersection of the image of $\bar{\rho}$ with $\mathcal{T}$. The group G may be identified with the image of $\bar{\rho}$. It is easy to see that G has a semi-direct product decomposition $G \simeq \bar{\rho}(G) = U_1(\mathbb{F}_q) \rtimes \mathcal{T}'$.

Lemma 3.3.1. *Suppose* $0 < |k| \leq 2n-1$, *there is an isomorphism of* $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$*-modules*

$$(\mathrm{Ad}^0 \bar{\rho})_k / (\mathrm{Ad}^0 \bar{\rho})_{k+1} \simeq \bigoplus_{ht\lambda = k} \mathbb{F}_q(\sigma_\lambda).$$

On the other hand,

$$(\mathrm{Ad}^0 \bar{\rho})_0 / (\mathrm{Ad}^0 \bar{\rho})_1 = \mathfrak{b}/\mathfrak{n} \simeq \mathfrak{t}.$$

Proof. Let λ be of height k. Let $X \in (\mathrm{Ad}^0 \bar{\rho})_\lambda$, we observe that

$$\bar{\rho}(g) \cdot X \cdot \bar{\rho}(g)^{-1} \equiv \sigma_\lambda(g) X \mod (\mathrm{Ad}^0 \bar{\rho})_{k+1}.$$

Likewise, for $X \in \mathfrak{b}$, the conjugation action on X modulo $\mathfrak{n}$ is trivial. □

For $i = 1, \ldots, n$, set $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. Likewise, for roots λ and γ, set $\delta_{\lambda,\gamma}$ to equal 1 if $\lambda = \gamma$ and 0 otherwise. Denote by X_λ^* and H_i^* the elements of $\mathrm{Ad}^0 \bar{\rho}^*$ which are defined by the following relations:

$$X_\lambda^*(X_\gamma) = \delta_{\lambda,\gamma} \text{ and } X_\lambda^*(H_i) = 0,$$

$$H_i^*(X_\lambda) = 0 \text{ and } H_i^*(H_j) = \delta_{i,j}.$$

The element $H_i^* \in \mathrm{Ad}^0 \bar{\rho}^*$ should not be confused with $L_i \in \mathfrak{t}^*$. Let $(\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}}$ be the span of $H_1^*, \ldots, H_n^*$ and $(\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_\lambda}$ the span of $X_{-\lambda}^*$. Let P be a Galois-stable subgroup of $\mathrm{Ad}^0 \bar{\rho}^*$. Associated to P are its eigenspaces for the action of $\bar{\rho}^{-1}(\mathcal{T})$.

For $\lambda \in \Phi \cup \{1\}$, set $P_{\bar{\chi}\sigma_\lambda}$ to be the intersection of P with $(\mathrm{Ad}^0\,\bar{\rho}^*)_{\bar{\chi}\sigma_\lambda}$. Likewise, associate to a Galois stable subgroup $Q \subseteq \mathrm{Ad}^0\,\bar{\rho}$, an eigenspace Q_{σ_λ}. Define Q_1 to be the intersection $Q \cap \mathfrak{t}$. For $\lambda \in \Phi$, denote by Q_{σ_λ} the intersection $Q \cap (\mathrm{Ad}^0\,\bar{\rho})_\lambda$.

The representation $\bar{\rho}$ factors through G. Let $\mathbb{T}$ be the subgroup of G' consisting of g such that $\bar{\rho}(g) \in \mathcal{T}$. For $\lambda \in \Phi \cup \{1\}$, $\mathbb{T}$ acts on $P_{\bar{\chi}\sigma_\lambda}$ by the character $\bar{\chi}\sigma_\lambda$ and on Q_{σ_λ} by the character σ_λ. Since the characters σ_λ are assumed to distinct, it is easy to see that

$$P_{\bar{\chi}\sigma_\lambda} = \{p \in P | t \cdot p = \bar{\chi}\sigma_\lambda(t)p \text{ for } t \in \mathbb{T}\}$$

$$Q_{\sigma_\lambda} = \{q \in Q | t \cdot q = \sigma_\lambda(t)q \text{ for } t \in \mathbb{T}\}.$$

The order of $\mathbb{T}$ is coprime to p, hence Maschke's theorem asserts that any finite dimensional $\mathbb{F}_p[G']$-module M decomposes into a direct sum $M = \bigoplus_\tau M_\tau$, where τ is a character of $\mathbb{T}$ and M_τ is the τ-eigenspace $M_\tau := \{m \in M | g \cdot m = \tau(g)m\}$. Thus, we have the next Lemma, which follows from the discussion above.

Lemma 3.3.2. *1. Let $P \subseteq \mathrm{Ad}^0\,\bar{\rho}^*$ be a Galois-stable subgroup. As an abelian group, P decomposes into a direct sum of subgroups $P = \bigoplus_{\lambda \in \Phi \cup \{1\}} P_{\bar{\chi}\sigma_\lambda}$.*

2. Let $Q \subseteq \mathrm{Ad}^0\,\bar{\rho}$ be a Galois-stable subgroup. Then Q decomposes into a direct sum of subgroups $Q = \bigoplus_{\lambda \in \Phi \cup \{1\}} Q_{\sigma_\lambda}$.

Set the height of the formal symbol "1" to be equal to zero. Fix a total order on $\Phi \cup \{1\}$ such that $\mathrm{ht}(\lambda) \leq \mathrm{ht}(\gamma)$ if $\lambda \leq \gamma$.

Lemma 3.3.3. *1. Let P be a non-zero Galois stable subgroup of $\mathrm{Ad}^0\,\bar{\rho}^*$. Then $P_{\bar{\chi}\sigma_{2L_1}}$ is equal to $(\mathrm{Ad}^0\,\bar{\rho}^*)_{\bar{\chi}\sigma_{2L_1}}$.*

2. *Let Q be a non-zero Galois stable subgroup of $\operatorname{Ad}^0 \bar{\rho}$. Then $Q_{\sigma_{2L_1}}$ is equal to $(\operatorname{Ad}^0 \bar{\rho})_{\sigma_{2L_1}}$.*

Proof. It follows from Lemma 3.3.2 that P decomposes into $\bigoplus_{\lambda \in \Phi \cup \{1\}} P_{\bar{\chi}\sigma_\lambda}$. By condition (5) of Theorem 3.0.1, the image of σ_{2L_1} spans $\mathbb{F}_q$. Since $\bar{\chi}$, takes values in $\mathbb{F}_p^\times$, the same is true for the image of $\bar{\chi}\sigma_{2L_1}$. Therefore, if $P_{\bar{\chi}\sigma_{2L_1}}$ is not zero, then $P_{\bar{\chi}\sigma_{2L_1}} = (\operatorname{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{2L_1}}$. Suppose by way of contradiction that $P_{\bar{\chi}\sigma_{2L_1}} = 0$. Then we may choose $\gamma \in \Phi \cup \{1\}$ such that:

- $P_{\bar{\chi}\sigma_\gamma} \neq 0$,
- $P_{\bar{\chi}\sigma_\lambda} = 0$ for all $\lambda > \gamma$.

By assumption, γ is not the maximal root $2L_1$. There exists $\gamma_1 \in \Phi$ such that the difference $\mu := \gamma_1 - \gamma$ is in Φ^+. This can be shown by considering all possibilities for γ:

1. $\gamma = 1$, then let $\mu = \gamma_1$ be any positive root,
2. $\gamma = 2L_i$ for $i > 1$, then $\mu = L_{i-1} - L_i$ and $\gamma_1 = L_{i-1} + L_i$,
3. $\gamma = -2L_i$ for $i > 1$, then $\mu = L_{i-1} + L_i$ and $\gamma_1 = L_{i-1} - L_i$,
4. $\gamma = -2L_1$, then $\mu = L_1 + L_2$ and $\gamma_1 = -L_1 + L_2$,
5. $\gamma = L_i + L_j$ for $i < j$, then $\mu = L_i - L_j$ and $\gamma_1 = 2L_i$,
6. $\gamma = -L_i - L_j$ for $i < j$, then $\mu = L_i - L_j$ and $\gamma_1 = -2L_j$,
7. $\gamma = L_i - L_j$ for $i \neq j$, then $\mu = L_i + L_j$ and $\gamma_1 = 2L_i$.

By condition (3) of Theorem 3.0.1, the root subgroup U_μ is contained in the image of $\bar{\rho}$. Let $g \in \mathrm{G}_{\mathbb{Q}}$ be such that $\bar{\rho}(g) \neq \mathrm{Id}$ and $\bar{\rho}(g) \in U_\mu$. Let $p \in P_{\bar{\chi}\sigma_\gamma}$ be a non-zero element. We show that the projection of $g \cdot p$ to $P_{\bar{\chi}\sigma_{\gamma_1}}$ is non-zero. Express $\bar{\rho}(g)$ as $e^{-X} := \sum_{i=0}^{2n-1} \frac{(-X)^i}{i!}$, where $X \in (\mathrm{Ad}^0 \bar{\rho})_\mu$. For $Y \in (\mathrm{Ad}^0 \bar{\rho})_k$, the following identity is well known (see [8, Exercise 3.9.14]):

$$\begin{aligned} g^{-1} \cdot Y =& e^X Y e^{-X} = e^{\mathrm{ad}_X}(Y) = \sum_{i=0}^{2n-1} \frac{(\mathrm{ad}_X)^i(Y)}{i!} \\ =& Y + [X, Y] + \frac{1}{2!}[X,[X,Y]] + \frac{1}{3!}[X,[X,[X,Y]]] + \dots. \end{aligned}$$

Note that μ is a positive root and hence,

$$g^{-1} \cdot Y - Y = [X, Y] \mod (\mathrm{Ad}^0 \bar{\rho})_{\mathrm{ht}(\mu)+k+1}.$$

Note that since $-\gamma_1 + \mu = -\gamma$ is a root,

$$[(\mathrm{Ad}^0 \bar{\rho})_\mu, (\mathrm{Ad}^0 \bar{\rho})_{-\gamma_1}] = (\mathrm{Ad}^0 \bar{\rho})_{-\gamma}$$

(cf. [10, p. 39]). Letting Y run through an appropriate basis of $\mathrm{Ad}^0 \bar{\rho}$, it follows from the above identity that $g \cdot p - p$ can be expressed as a sum $a + b$ where $a \neq 0$ is in $P_{\bar{\chi}\sigma_{\gamma_1}}$ and $b \in \bigoplus_{\lambda > \gamma_1} P_{\bar{\chi}\sigma_\lambda}$. In particular, this shows that the projection of $g \cdot p$ to $P_{\bar{\chi}\sigma_{\gamma_1}}$ is non-zero.

Since $\gamma_1 = \mu + \gamma$ and $\mu \in \Phi^+$, the height of γ_1 is strictly larger than the height of γ. As a result, $\gamma_1 > \gamma$. Therefore, the subgroup $P_{\bar{\chi}\sigma_{\gamma_1}} = 0$. This contradiction shows that $\gamma = 2L_1$ and $P_{\bar{\chi}\sigma_{2L_1}} \neq 0$. This concludes part (1). The proof of part (2) is similar and is left to the reader. $\square$

For $\lambda \in \Phi \cup \{1\}$, set

$$N_\lambda = \begin{cases} 1 \text{ if } \lambda \in \Delta, \\ 0 \text{ otherwise.} \end{cases}$$

Lemma 3.3.4. *Let $\lambda \in \Phi \cup \{1\}$ and σ_λ the associated character. The following assertions are satisfied:*

1. $\dim \operatorname{Hom}(N, \mathbb{F}_q(\sigma_\lambda))^{G/N} = N_\lambda$.
2. $\dim \operatorname{Hom}(N', \mathbb{F}_q(\sigma_\lambda)^*)^{G'/N'} = 0$.
3. *For $k \neq 1$,*

   $$H^1(G, (\operatorname{Ad}^0 \bar{\rho})_k / (\operatorname{Ad}^0 \bar{\rho})_{k+1}) = 0.$$

   On the other hand,

   $$h^1(G, (\operatorname{Ad}^0 \bar{\rho})_1 / (\operatorname{Ad}^0 \bar{\rho})_2) = \dim \mathfrak{t}.$$

4. *For all k, $h^1(G', ((\operatorname{Ad}^0 \bar{\rho})_k / (\operatorname{Ad}^0 \bar{\rho})_{k+1})^*) = 0$.*

Proof. By condition 3 of Theorem $3.0.1$, N may be identified with $U_1(\mathbb{F}_q)$. The abelianization N^{ab} is

$$U_1/U_2(\mathbb{F}_q) \simeq \bigoplus_{\gamma \in \Delta} \mathbb{F}_q(\sigma_\gamma).$$

By condition (5) of Theorem $3.0.1$, any G/N equivariant map $F : \mathbb{F}_q(\sigma_\gamma) \to \mathbb{F}_q(\sigma_\lambda)$ is determined by the image of any nonzero element, hence

$$\dim \operatorname{Hom}(\mathbb{F}_q(\sigma_\gamma), \mathbb{F}_q(\sigma_\lambda))^{G/N} \leq 1.$$

We have that

$$F(\sigma_\gamma(g_1)\sigma_\gamma(g_2)) = \sigma_\lambda(g_1)\sigma_\lambda(g_2)F(1) = F(\sigma_\gamma(g_1))F(\sigma_\gamma(g_2))F(1).$$

Since the image of σ_λ spans $\mathbb{F}_q$, it follows that F is a scalar multiple of an element of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. By assumption, if $\lambda \neq \gamma$, the characters σ_λ and σ_γ are not equal up to a twist of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Therefore,

$$\mathrm{Hom}(\mathbb{F}_q(\sigma_\gamma), \mathbb{F}_q(\sigma_\lambda))^{G/N} = \begin{cases} \mathbb{F}_q \text{ if } \sigma_\lambda = \sigma_\gamma, \\ 0 \text{ otherwise,} \end{cases}$$

and part (1) follows this.

Observe that N' is isomorphic to N and G'/N' is the Galois group $\mathrm{Gal}(\mathbb{Q}(\{\varphi_i\}, \bar{\kappa}, \bar{\chi})/\mathbb{Q})$. By condition (4), the characters σ_γ and $\sigma_\lambda^* = \bar{\chi}\sigma_{-\lambda}$ are not equivalent up to a twist of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Part (2) follows via the same reasoning as part (1).

The order of G/N is coprime to p. By inflation-restriction and part (1)

$$\begin{aligned}
&\dim H^1(G, (\mathrm{Ad}^0\,\bar{\rho})_k/(\mathrm{Ad}^0\,\bar{\rho})_{k+1}) \\
=&\dim \mathrm{Hom}(N, (\mathrm{Ad}^0\,\bar{\rho})_k/(\mathrm{Ad}^0\,\bar{\rho})_{k+1})^{G/N} \\
=&\sum_{\lambda\in\Phi, ht(\lambda)=k} \dim \mathrm{Hom}(N, \mathbb{F}_q(\sigma_\lambda))^{G/N} \\
=&\sum_{\lambda\in\Phi, ht(\lambda)=k} N_\lambda.
\end{aligned}$$

It follows that if $k \neq 1$,

$$H^1(G, (\mathrm{Ad}^0\,\bar{\rho})_k/(\mathrm{Ad}^0\,\bar{\rho})_{k+1}) = 0$$

and that

$$h^1(G, (\mathrm{Ad}^0\,\bar\rho)_1/(\mathrm{Ad}^0\,\bar\rho)_2) = \#\Delta = n = \dim \mathfrak{t}.$$

This concludes part (3).

The order of G'/N' is coprime to p. Therefore, by inflation-restriction,

$$\begin{aligned}&\dim H^1(G', (\mathrm{Ad}^0\,\bar\rho)_k/(\mathrm{Ad}^0\,\bar\rho)_{k+1})\\ =&\dim \mathrm{Hom}(N', (\mathrm{Ad}^0\,\bar\rho)_k/(\mathrm{Ad}^0\,\bar\rho)_{k+1})^{G'/N'}\\ =&\sum_{\lambda\in\Phi, ht(\lambda)=k} \dim \mathrm{Hom}(N', \mathbb{F}_q(\sigma_\lambda)^*)^{G'/N'}\\ =&0.\end{aligned}$$

This concludes the proof of part (4). □

Definition 3.3.5. *Let* $(\mathrm{Ad}^0\,\bar\rho)_k^\perp \subset \mathrm{Ad}^0\,\bar\rho^*$ *be the subspace of* $\mathrm{Ad}^0\,\bar\rho^*$ *consisting of* $f \in \mathrm{Ad}^0\,\bar\rho^*$ *for which* $f_{\restriction(\mathrm{Ad}^0\,\bar\rho)_k} = 0$.

Remark 3.3.6. *For* $k > -2n+1$*, the submodule* $(\mathrm{Ad}^0\,\bar\rho)_k^\perp \neq 0$ *and by Lemma* 3.3.3*,*

$$(\mathrm{Ad}^0\,\bar\rho)_{k,\bar\chi\sigma_{2L_1}}^\perp \simeq (\mathrm{Ad}^0\,\bar\rho)_{\bar\chi\sigma_{2L_1}}^*.$$

Lemma 3.3.7. *Let* k *be an integer,*

1. $H^1(G, \mathrm{Ad}^0\,\bar\rho/(\mathrm{Ad}^0\,\bar\rho)_k) = 0$ *and* $H^1(G', \mathrm{Ad}^0\,\bar\rho/(\mathrm{Ad}^0\,\bar\rho)_k) = 0$*,*
2. $H^1(G', (\mathrm{Ad}^0\,\bar\rho)_k^\perp) = 0$.

Proof. We begin with the proof of part (1). Consider the case when $k \leq 1$. By part (3) of Lemma 3.3.4, for $i \leq 1$,

$$H^1(G, (\mathrm{Ad}^0\,\bar\rho)_{i-1}/(\mathrm{Ad}^0\,\bar\rho)_i) = 0.$$

and hence there is an injection

$$H^1(G, \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_i) \hookrightarrow H^1(G, \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_{i-1}).$$

We deduce that $H^1(G, \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_k) = 0$.

Next consider the case $k > 1$. Associated to

$$0 \to (\mathrm{Ad}^0 \bar{\rho})_1/(\mathrm{Ad}^0 \bar{\rho})_k \to \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_k \to \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_1 \to 0$$

is the long exact sequence in cohomology. It follows from $3.3.3$ that any non-zero submodule of $\mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_k$ has a non-trivial σ_{2L_1} eigenspace for the $\mathbb{T}$-action. As a consequence, $H^0(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}^0 \bar{\rho}) = 0$. Further, it has been shown that $H^1(G, \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_1) = 0$. It suffices to show that

$$\dim H^0(G, \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_1) \geq \dim H^1(G, (\mathrm{Ad}^0 \bar{\rho})_1/(\mathrm{Ad}^0 \bar{\rho})_k).$$

Condition (4) of Theorem $3.0.1$ stipulates that for $\lambda \in \Phi$, σ_λ is not equal to $\sigma_1 = 1$. Therefore for $i \leq 0$,

$$H^0(G, (\mathrm{Ad}^0 \bar{\rho})_{i-1}/(\mathrm{Ad}^0 \bar{\rho})_i) = \bigoplus_{\mathrm{ht}\gamma = i-1} H^0(G, \mathbb{F}_q(\sigma_\gamma)) = 0.$$

For $i \leq 0$, we deduce that

$$H^0(G, (\mathrm{Ad}^0 \bar{\rho})_i/(\mathrm{Ad}^0 \bar{\rho})_1) \xrightarrow{\sim} H^0(G, (\mathrm{Ad}^0 \bar{\rho})_{i-1}/(\mathrm{Ad}^0 \bar{\rho})_1).$$

Composing these isomorphisms we have that

$$(\mathrm{Ad}^0 \bar{\rho})_0/(\mathrm{Ad}^0 \bar{\rho})_1 = H^0(G, (\mathrm{Ad}^0 \bar{\rho})_0/(\mathrm{Ad}^0 \bar{\rho})_1) \xrightarrow{\sim} H^0(G, \mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_1).$$

We have deduced that

$$h^0(G, \mathrm{Ad}^0\,\bar{\rho}/(\mathrm{Ad}^0\,\bar{\rho})_1) = \dim(\mathrm{Ad}^0\,\bar{\rho})_0/(\mathrm{Ad}^0\,\bar{\rho})_1 = \dim \mathfrak{t}.$$

By Lemma 3.3.4 part (3),

$$h^1(G, (\mathrm{Ad}^0\,\bar{\rho})_1/(\mathrm{Ad}^0\,\bar{\rho})_2) = \dim \mathfrak{t} = h^0(G, \mathrm{Ad}^0\,\bar{\rho}/(\mathrm{Ad}^0\,\bar{\rho})_1).$$

By Lemma 3.3.4, for $i \geq 2$, we have that

$$H^1(G, (\mathrm{Ad}^0\,\bar{\rho})_i/(\mathrm{Ad}^0\,\bar{\rho})_{i+1}) = 0.$$

and it follows that $H^1(G, (\mathrm{Ad}^0\,\bar{\rho})_2/(\mathrm{Ad}^0\,\bar{\rho})_k) = 0$. Hence it follows that

$$h^1(G, (\mathrm{Ad}^0\,\bar{\rho})_1/(\mathrm{Ad}^0\,\bar{\rho})_k) \leq h^1(G, (\mathrm{Ad}^0\,\bar{\rho})_1/(\mathrm{Ad}^0\,\bar{\rho})_2). \tag{3.3}$$

Conclude that

$$h^1(G, (\mathrm{Ad}^0\,\bar{\rho})_1/(\mathrm{Ad}^0\,\bar{\rho})_k) \leq h^0(G, \mathrm{Ad}^0\,\bar{\rho}/(\mathrm{Ad}^0\,\bar{\rho})_1).$$

Therefore we conclude that $H^1(G, \mathrm{Ad}^0\,\bar{\rho}/(\mathrm{Ad}^0\,\bar{\rho})_k) = 0$.

Since $[L : K]$ is coprime to p, from a direct application of inflation-restriction it follows that $H^1(G', \mathrm{Ad}^0\,\bar{\rho}/(\mathrm{Ad}^0\,\bar{\rho})_k) = 0$. We have proved part (1).

Consider the short exact sequence

$$0 \to (\mathrm{Ad}^0\,\bar{\rho})_{i-1}^{\perp} \to (\mathrm{Ad}^0\,\bar{\rho})_i^{\perp} \to ((\mathrm{Ad}^0\,\bar{\rho})_{i-1}/(\mathrm{Ad}^0\,\bar{\rho})_i)^* \to 0$$

and the associated sequence in cohomology. By Lemma 3.3.4,

$$H^1(G', ((\mathrm{Ad}^0\,\bar{\rho})_{i-1}/(\mathrm{Ad}^0\,\bar{\rho})_i)^*) = 0$$

from which we deduce that

$$H^1(G', (\mathrm{Ad}^0\,\bar{\rho})^{\perp}_{i-1}) \to H^1(G', (\mathrm{Ad}^0\,\bar{\rho})^{\perp}_{i})$$

is a surjection for all i. As

$$(\mathrm{Ad}^0\,\bar{\rho})^{\perp}_{-2n+1} \simeq (\mathrm{Ad}^0\,\bar{\rho}/(\mathrm{Ad}^0\,\bar{\rho})_{-2n+1})^* = 0$$

we deduce that $H^1(G', (\mathrm{Ad}^0\,\bar{\rho})^{\perp}_{k}) = 0$. □

For ψ in $H^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}^0\,\bar{\rho}^*)$, the restriction $\psi_{\restriction \mathrm{G}_K} : \mathrm{G}_K \to \mathrm{Ad}^0\,\bar{\rho}^*$ is a homomorphism since the action of G_K on $\mathrm{Ad}^0\,\bar{\rho}^*$ is trivial. Set $K_\psi \supseteq K$ be the extension *cut out* by ψ, i.e. K_ψ is the smallest extension of K which is fixed by the kernel of $\psi_{\restriction \mathrm{G}_K}$. Identify $\mathrm{Gal}(K_\psi/K)$ with $\psi(\mathrm{G}_K) \subseteq \mathrm{Ad}^0\,\bar{\rho}^*$ and let $J_\psi \subseteq K_\psi$ be the subfield for which $\mathrm{Gal}(K_\psi/J_\psi) \simeq \psi(\mathrm{G}_K)_{\bar{\chi}\sigma_{2L_1}}$. Likewise for f in $H^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}^0\,\bar{\rho})$ denote by L_f, the extension of L cut out by f. Set K_f to be the composite of L_f with K. Since $p \nmid [K : L]$, we have that $\mathrm{Gal}(K_f/K) \simeq \mathrm{Gal}(L_f/L)$.

Lemma 3.3.8. *Let $\mathcal{J} \supseteq S$ be a finite set of primes. Let $f \in H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, \mathrm{Ad}^0\,\bar{\rho})$ and $\psi \in H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, \mathrm{Ad}^0\,\bar{\rho})$ be a non-zero cohomology classes. Then the following assertions are satisfied:*

1. *$L_f \supsetneq L$ (equivalently, $K_f \supsetneq K$),*
2. *$K_\psi \supsetneq J_\psi$, in particular, $K_\psi \supsetneq K$.*

Proof. For part (2), recall that Lemma 3.3.7 asserts that $H^1(G', \mathrm{Ad}^0\,\bar{\rho}^*) = 0$. Therefore, the restriction $\psi_{\restriction \mathrm{G}_K}$ is not zero. This shows that $K_\psi \supsetneq K$. That K_ψ strictly contains J_ψ is a direct consequence of Lemma 3.3.3. Part (1) also follows from Lemma 3.3.7. □

Lemma 3.3.9. *1. Let $P \subseteq \mathrm{Ad}^0\,\bar\rho^*$ be a nonzero Galois-stable subgroup and $\iota_P : P \to \mathrm{Ad}^0\,\bar\rho^*$ denote the inclusion. We have that*

$$\mathrm{Hom}_{\mathbb{F}_p}(P, \mathrm{Ad}^0\,\bar\rho^*)^{G'} = \mathbb{F}_q \cdot \iota_P.$$

2. Let $Q \subseteq \mathrm{Ad}^0\,\bar\rho$ be a nonzero Galois-stable subgroup and $\iota_Q : Q \to \mathrm{Ad}^0\,\bar\rho$ denote the inclusion. We have that

$$\mathrm{Hom}_{\mathbb{F}_p}(Q, \mathrm{Ad}^0\,\bar\rho^*)^{G} = \mathbb{F}_q \cdot \iota_Q.$$

Proof. We prove part (1), the proof of (2) is similar. Let $\Phi' = \Phi \cup \{1\}$ and $m := \#\Phi'$. Enumerate $\Phi' = \{\gamma_1, \ldots, \gamma_m\}$, so that $\gamma_i > \gamma_j$ if $i < j$. The root γ_1 is the highest root $2L_1$ and γ_m is $-2L_1$. Let W_i be the G'-submodule of $\mathrm{Ad}^0\,\bar\rho^*$ defined by

$$W_i := \left(\bigoplus_{j \le i} (\mathrm{Ad}^0\,\bar\rho^*)_{\bar\chi\sigma_{\gamma_j}}\right).$$

Setting $P_i = P \cap W_i$, Lemma 3.3.2 asserts that

$$P = \bigoplus_{\lambda \in \Phi'} P_{\bar\chi\sigma_\lambda} \text{ and } P_i = \left(\bigoplus_{j \le i} P_{\bar\chi\sigma_{\gamma_j}}\right).$$

Let $\varphi \in \mathrm{Hom}(P, \mathrm{Ad}^0\,\bar\rho^*)^{G'}$, we show that there exists $\beta \in \mathbb{F}_q$ such that $\varphi = \beta\iota_P$.

Note that $P_1 = P_{\bar\chi\sigma_{2L_1}}$ is G'-stable. For $p \in P_1$, we have that

$$g\varphi(p) = \varphi(gp) = \bar\chi(g)\sigma_{\gamma_1}(g)\varphi(p).$$

We show that $\varphi(p) \in (\mathrm{Ad}^0\,\bar{\rho}^*)_{\bar{\chi}\sigma_{\gamma_1}} = W_1$. Assume that $\varphi(p) \neq 0$ and set $P_0 := 0$. Suppose that i is such that $\varphi(p) \in P_i$ and $\varphi(p)$ is not in P_{i-1}, we show that $i = 1$. Express $\varphi(p) = x_i + x_{i-1}$, where $x_i \in (\mathrm{Ad}^0\,\bar{\rho})_{\bar{\chi}\sigma_{\gamma_i}}$ and $x_{i-1} \in W_{i-1}$. Suppose $i \neq 1$, then there exists g be such that $\sigma_{\gamma_1}(g) \neq \sigma_{\gamma_i}(g)$. We have that

$$\begin{aligned} g\varphi(p) &= \bar{\chi}(g)\sigma_{\gamma_i}(g)x_i + g \cdot x_{i-1}, \\ \varphi(gp) &= \bar{\chi}(g)\sigma_{\gamma_1}(g)\varphi(p) = \bar{\chi}(g)\sigma_{\gamma_1}(g)x_i + \bar{\chi}(g)\sigma_{\gamma_1}(g)x_{i-1}. \end{aligned}$$

Since $g\varphi(p) = \varphi(gp)$ we deduce that

$$(\sigma_{\gamma_i}(g) - \sigma_{\gamma_1}(g))x_i = \sigma_{\gamma_1}(g)x_{i-1} - g \cdot x_{i-1} \in W_{i-1}.$$

This is a contradiction since $x_i \notin W_{i-1}$. Therefore i is equal to 1. By Lemma $3.3.3$, P_1 is equal to W_1. Note that W_1 is a one dimensional $\mathbb{F}_q$-vector space. By condition (5) of Theorem $3.0.1$, the $\mathbb{F}_p$-span of the image of σ_{2L_1} is equal to $\mathbb{F}_q$. Since the image of $\bar{\chi}$ is in $\mathbb{F}_p$, it follows that the image of $\bar{\chi}\sigma_{2L_1}$ is equal to $\mathbb{F}_q$. Therefore, the restriction of φ to $P_1 = W_1$ must be $\mathbb{F}_q$-linear. Let $\beta \in \mathbb{F}_q$ be such that $\varphi(p) = \beta p$ for all $p \in P_1$.

Next, we show that by induction on i, that φ is given by multiplication by β on P_i. Let $p \in P_{\bar{\chi}\sigma_{\gamma_i}}$ and $g \in \mathbb{T}$. We have that

$$g(p) = \bar{\chi}(g)\sigma_{\gamma_i}(g)p$$

and we deduce that

$$\varphi(gp) = \bar{\chi}(g)\sigma_{\gamma_i}(g)\varphi(p) = \bar{\chi}(g)\sigma_{\gamma_i}(g)\varphi(p).$$

Suppose by way of contradiction, $\varphi(p) \notin W_i$. Let $j > i$ be such that $\varphi(p) \in W_j$ and $\varphi(p) \notin W_{j-1}$. It follows from conditions (3) and (4) of Theorem $3.0.1$, that there exists $g \in \mathbb{T}$ such that $\sigma_{\gamma_i}(g) \neq \sigma_{\gamma_j}(g)$. Express $\varphi(p) = x_j + x_{j-1}$, where $x_j \in (\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{\gamma_j}}$ and $x_{j-1} \in W_{j-1}$. We have that

$$g\varphi(p) = \bar{\chi}(g)\sigma_{\gamma_j}(g)x_j + g \cdot x_{j-1} = \varphi(gp) = \bar{\chi}(g)\sigma_{\gamma_i}(g)(x_j + x_{j-1}).$$

We have that

$$\bar{\chi}(g)(\sigma_{\gamma_j}(g) - \sigma_{\gamma_i}(g))x_j = \bar{\chi}(g)\sigma_{\gamma_i}(g)x_{j-1} - g \cdot x_{j-1}$$

is contained in W_{j-1}. This is contradiction, we deduce that $\varphi(P_i) \subseteq W_i$. We show that $\varphi(p) = \beta p$ for $p \in P_{\bar{\chi}\sigma_{\gamma_i}}$ and this shall complete the inductive step. Write $\varphi(p) = z_i + z_{i-1}$ where $z_i \in (\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{\gamma_i}}$ and $z_{i-1} \in W_{i-1}$. Let $g \in \mathbb{T}$, we have that

$$\varphi(gp) = \varphi(\bar{\chi}(g)\sigma_{\gamma_i}(g)p) = \bar{\chi}(g)\sigma_{\gamma_i}(g)\varphi(p) = \bar{\chi}(g)\sigma_{\gamma_i}(g)z_i + \bar{\chi}(g)\sigma_{\gamma_i}(g)z_{i-1}.$$

We have that

$$g\varphi(p) = g \cdot z_i + g \cdot z_{i-1} = \bar{\chi}(g)\sigma_{\gamma_i}(g)z_i + g \cdot z_{i-1}.$$

Therefore, we deduce that

$$g \cdot z_{i-1} = \bar{\chi}(g)\sigma_{\gamma_i}(g)z_{i-1}.$$

We show that $z_{i-1} = 0$. If $z_{i-1} \neq 0$, there exists $k < i$ be such that $z_{i-1} \in W_k$ and $z_{i-1} \notin W_{k-1}$. Write $z_{i-1} = w_k + w_{k-1}$ where $w_k \in (\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{\gamma_k}}$ and $w_{k-1} \in W_{k-1}$. Let $g \in \mathbb{T}$ be such that $\sigma_{\gamma_i}(g) \neq \sigma_{\gamma_k}(g)$. Comparing $g\varphi(p)$ with $\varphi(gp)$ we deduce that w_k is contained in W_{k-1}. This implies that $z_{i-1} = 0$ and therefore, $\varphi(p) = z_i \in (\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{\gamma_i}}$. Let $h \in \mathrm{G}_{\mathbb{Q}}$, write $h \cdot p = \bar{\chi}(h)\sigma_{\gamma_i}(h)p + a$, where $a \in P_{i-1}$. By inductive hypothesis, $\varphi(a) = \beta a$. We have $h \cdot z_i = \varphi(h \cdot p) = \bar{\chi}(h)\sigma_{\gamma_i}(h)z_i + \beta a$. We deduce

$$h(z_i - \beta p) = \bar{\chi}(h)\sigma_{\gamma_i}(h)z_i + \beta a - \beta(\bar{\chi}(h)\sigma_{\gamma_i}(h)p + a) = \bar{\chi}(h)\sigma_{\gamma_i}(h)(z_i - \beta p).$$

The Galois stable module P' generated by $(z_i - \beta p)$ is contained in $P_{\bar{\chi}\sigma_{\gamma_i}}$. Since $i > 1$, we have that ${P'}_{\bar{\chi}\sigma_{2L_1}} = 0$ and therefore Lemma 3.3.3, asserts that $P' = 0$. We conclude that $\varphi(p) = z_i = \beta p$. This concludes the induction step and the proof of the result. $\square$

Corollary 3.3.10. *1. Let P_1 and P_2 be Galois-stable subgroups of $\operatorname{Ad}^0 \bar{\rho}^*$ such that there is an isomorphism $\phi : P_1 \xrightarrow{\sim} P_2$ of Galois modules. Then $P_1 = P_2$ and ϕ is multiplication by a scalar.*

2. Let Q_1 and Q_2 be Galois-stable subgroups of $\operatorname{Ad}^0 \bar{\rho}$ such that there is an isomorphism $\phi : Q_1 \xrightarrow{\sim} Q_2$ of Galois modules. Then $Q_1 = Q_2$ and ϕ is multiplication by a scalar.

Proof. We prove part (1), part (2) is identical. Let $\iota_{P_i} : P_i \hookrightarrow \operatorname{Ad}^0 \bar{\rho}^*$ be the inclusion. By Proposition 3.3.9, the two inclusions ι_{P_1} and $\iota_{P_2} \circ \phi$ are the same upto a scalar. The assertion follows. $\square$

Let Q be a G-submodule of $\operatorname{Ad}^0 \bar{\rho}$, by Lemma 3.3.2, the projection of Q to $(\operatorname{Ad}^0 \bar{\rho})_{-2L_1}$ equals $Q_{\sigma_{-2L_1}}$. For convenience of notation, let Q_{-2L_1} denote $Q_{\sigma_{-2L_1}}$.

Lemma 3.3.11. *Let Q be a Galois-stable submodule of $\operatorname{Ad}^0 \bar{\rho}$ for which $Q_{-2L_1} \neq 0$, then $Q = \operatorname{Ad}^0 \bar{\rho}$.*

Proof. Let $P := \{\gamma \in \operatorname{Ad}^0 \bar{\rho}^* \mid \gamma(x) = 0 \text{ for } x \in Q\}$. The assumption on Q implies that $P_{\bar{\chi}\sigma_{2L_1}} \neq (\operatorname{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{2L_1}}$. Since the image of $\bar{\chi}\sigma_{2L_1}$ spans $\mathbb{F}_q$, $P_{\bar{\chi}\sigma_{2L_1}} \neq (\operatorname{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{2L_1}}$ implies that $P_{\bar{\chi}\sigma_{2L_1}} = 0$ By Lemma 3.3.3, $P = 0$, and therefore, $Q = \operatorname{Ad}^0 \bar{\rho}$. $\square$

Lemma 3.3.12. *1. The fields $K = \mathbb{Q}(\bar{\rho}, \mu_p)$ and $\mathbb{Q}(\mu_{p^2})$ are linearly disjoint over $\mathbb{Q}(\mu_p)$.*

2. Let $\mathcal{J} \supseteq S$ be a finite set of prime numbers, $\psi_1, \dots, \psi_t \in H^1(\mathrm{G}_{\mathbb{Q},Z}, \mathrm{Ad}^0 \bar{\rho}^*)$ and set $K_j := K_{\psi_j}$ for $j = 1, \dots, t$. Then the composite $K_1 \cdots K_t$ and $\mathbb{Q}(\mu_{p^2})$ are linearly disjoint over $\mathbb{Q}(\mu_p)$.

Proof. Suppose by way of contradiction that $\mathbb{Q}(\mu_{p^2}) \subseteq K$. Set $V := \mathrm{Gal}(K/F(\mu_{p^2}))$ and $\mathcal{A} := G'/N' = \mathrm{Gal}(F(\mu_p)/\mathbb{Q})$. For $n \in N'^{ab}$ and $g \in \mathcal{A}$, let $\tilde{n}$ and $\tilde{g}$ be lifts of n and g to N' and G' respectively. The action of $\mathcal{A}$ on N'^{ab} is induced by conjugation, defined by $g \cdot n := \tilde{g}\tilde{n}\tilde{g}^{-1} \mod [N', N']$. The groups N and N' are isomorphic and the image of $\bar{\rho}$ is assumed to contain $U_1(\mathbb{F}_q)$ (condition 3 of Theorem $3.0.1$). The quotient $N'/V = \mathrm{Gal}(F(\mu_{p^2})/F(\mu_p)) \simeq \mathbb{F}_p$. Since E is an abelian extension of $\mathbb{Q}$, the action of $\mathcal{A}$ on the quotient N'/V is trivial. Let $\pi : G' \to \mathbb{F}_p$ denote the quotient map. The restriction of π to N' factors through an $\mathcal{A}$-equivariant map $\pi' : N'^{ab} \to \mathbb{F}_p$. As an $\mathcal{A}$-module, $N'^{ab} \simeq \bigoplus_{\lambda \in \Delta} \mathbb{F}_q(\sigma_\lambda)$. It follows from condition 4 of Theorem $3.0.1$ that $\sigma_\lambda \neq \bar{\chi}^{-1}$ for $\lambda \in \Phi$. As a result, the restriction of π to N' must be trivial. Hence π factors as a map $\mathcal{A} = G'/N' \to \mathbb{F}_p$. Therefore π must be zero since the order of $\mathcal{A}$ is prime to p. This is a contradiction since the quotient map π is surjective. Therefore, $\mathbb{Q}(\mu_{p^2})$ is not contained in K. This concludes the proof of part (1).

Set $\mathcal{K}_j$ to be $K_1 \dots K_j$ and $\mathcal{K}_0 := K$. Setting $E := \mathbb{Q}(\mu_{p^2})$, it suffices to show that $\mathcal{K}_j \cap E = \mathcal{K}_{j-1} \cap E$. We begin with the case $j = 1$. For $\psi \in H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, \mathrm{Ad}^0 \bar{\rho}^*)$, regard $\mathrm{Gal}(K_\psi/K)$ as an $\mathbb{F}_q[G']$-module, where the Galois action is induced via conjugation. The G'-module $P_1 := \mathrm{Gal}(K_1/K)$ is identified with $\psi_1(\mathrm{G}_K)$. Let $Q_1 \subseteq P_1$ be the G'-stable subgroup defined by $Q_1 := \mathrm{Gal}(K_1/(K_1 \cap E) \cdot K)$. The action of G' on $P_1/Q_1 = \mathrm{Gal}((K_1 \cap E) \cdot K/K)$ is trivial. By Lemma 3.3.2, the quotient P_1/Q_1 decomposes into subgroups

$$P_1/Q_1 = \bigoplus_{\lambda \in \Phi \cup \{1\}} (P_1)_{\bar{\chi}\sigma_\lambda}/(Q_1)_{\bar{\chi}\sigma_\lambda}.$$

The characters $\sigma_\lambda \neq \bar{\chi}^{-1}$ and hence $P_1 = Q_1$. We have thus shown that $K_1 \cap E = K \cap E$.

Let P_j be defined by $P_j := \mathrm{Gal}(\mathcal{K}_j/\mathcal{K}_{j-1})$. The G'-module P_j is isomorphic to

$$\mathrm{Gal}(K_j/K_j \cap \mathcal{K}_{j-1}) \subseteq \psi_j(\mathrm{G}_K) \subseteq \mathrm{Ad}^0 \bar{\rho}^*.$$

Let Q_j be the G'-stable subgroup $\mathrm{Gal}(\mathcal{K}_j/(\mathcal{K}_j \cap E) \cdot \mathcal{K}_{j-1})$ and note that the G' action on P_j/Q_j is trivial. Invoking the same argument as in the case when $j = 1$, we have that $P_j = Q_j$ and hence $\mathcal{K}_j \cap E = \mathcal{K}_{j-1} \cap E$. This completes the proof. □

Definition 3.3.13. *1. Let M_1 and M_2 be $\mathbb{F}_p[G']$-modules. We say that M_1 is unrelated to M_2 if for every $\mathbb{F}_p[G']$-submodule N of M_1,*

$$\mathrm{Hom}(N, M_2)^{G'} = 0.$$

2. Let L be a finite extension of K such that L is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(L/K)$ is an $\mathbb{F}_p$-vector space. Let M be an $\mathbb{F}_p[G']$-module. We say that L is unrelated to M if $\mathrm{Gal}(L/K)$ is G'-unrelated to M. Here, the G'-action on $\mathrm{Gal}(L/K)$ is induced via conjugation (let $x \in \mathrm{Gal}(L/K)$ and $g \in G'$, pick a lift $\tilde{g}$ of g, set $g \cdot x := \tilde{g}x\tilde{g}^{-1}$).

Proposition 3.3.14. *Let $\mathcal{J} \supseteq S$ be a finite set of prime numbers and*

$$\psi_0, \ldots, \psi_t \in H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, \mathrm{Ad}^0\, \bar{\rho}^*)$$

be linearly independent over $\mathbb{F}_q$. Set $K_i := K_{\psi_i}$ and let $L_1, \ldots, L_k$ be a (possibly empty) set of Galois extensions of $\mathbb{Q}$. Assume that L_i contains K and $\mathrm{Gal}(L_i/K)$ is an $\mathbb{F}_p$-vector space for $i = 1, \ldots, k$. Suppose that L_i is unrelated to $\mathrm{Ad}^0\, \bar{\rho}^*$ for $i = 1, \ldots, k$. Denote by $\mathcal{L}$ the composite $L_1 \cdots L_k$. If the set $\{L_1, \ldots, L_k\}$ is empty, set $\mathcal{L} = K$. The field K_0 is not contained in the composite of the fields $K_1 \cdots K_t \cdot \mathcal{L}$.

Proof. Let $\mathcal{K}$ denote the composite of the fields $K_1, \ldots, K_t$. If K_0 is contained in $\mathcal{K} \cdot \mathcal{L}$, then $\psi_0, \ldots, \psi_t \in H^1(\mathrm{Gal}(\mathcal{K} \cdot \mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0\, \bar{\rho}^*)$ and hence

$$h^1(\mathrm{Gal}(\mathcal{K} \cdot \mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0\, \bar{\rho}^*) \geq t + 1.$$

Hence it suffices to show that

$$h^1(\mathrm{Gal}(\mathcal{K} \cdot \mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0\, \bar{\rho}^*) \leq t.$$

First we show that

$$h^1(\mathrm{Gal}(\mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0\, \bar{\rho}^*) = 0.$$

Denote by $\mathcal{L}_i$ the composite of the fields $L_1 \cdots L_i$ and set $\mathcal{L}_0 := K$. Note that $\mathrm{Gal}(\mathcal{L}_i/\mathcal{L}_{i-1})$ is isomorphic to $\mathrm{Gal}(L_i/L_i \cap \mathcal{L}_{i-1})$, which is an $\mathbb{F}_p[G']$-submodule of $\mathrm{Gal}(L_i/K)$. Since L_i is unrelated to $\mathrm{Ad}^0\, \bar{\rho}^*$,

$$\mathrm{Hom}(\mathrm{Gal}(\mathcal{L}_i/\mathcal{L}_{i-1}), \mathrm{Ad}^0\, \bar{\rho}^*)^{G'} = 0.$$

Hence the inflation map

$$H^1(\mathrm{Gal}(\mathcal{L}_{i-1}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) \xrightarrow{\text{inf}} H^1(\mathrm{Gal}(\mathcal{L}_i/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*)$$

is an isomorphism. We deduce that $H^1(\mathrm{Gal}(\mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*)$ is isomorphic to $H^1(G', \mathrm{Ad}^0 \bar{\rho}^*)$ and hence, is zero.

Let $\mathcal{K}_i$ denote the composite $K_1 \cdots K_i$ and $\mathcal{K}_0$ denote K. Note that $\mathrm{Gal}(\mathcal{K}_i \cdot \mathcal{L}/\mathcal{K}_{i-1} \cdot \mathcal{L})$ is an $\mathbb{F}_p[G']$-submodule of $\mathrm{Gal}(K_i/K)$, and hence, of $\mathrm{Ad}^0 \bar{\rho}^*$. Lemma 3.3.9 asserts that

$$\dim \mathrm{Hom}(\mathrm{Gal}(\mathcal{K}_i \cdot \mathcal{L}/\mathcal{K}_{i-1} \cdot \mathcal{L}), \mathrm{Ad}^0 \bar{\rho}^*)^{G'} \leq 1.$$

Therefore, by inflation-restriction,

$$h^1(\mathrm{Gal}(\mathcal{K}_i \cdot \mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) \leq h^1(\mathrm{Gal}(\mathcal{K}_{i-1} \cdot \mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) + 1.$$

Consequently, we deduce that $h^1(\mathrm{Gal}(\mathcal{K} \cdot \mathcal{L}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) \leq t$ and the proof is complete. □

Lemma 3.3.15. *Let $\mathcal{J} \supseteq S$ be a finite set of primes.*

1. *Let $f \in H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, \mathrm{Ad}^0 \bar{\rho})$, then the extension K_f is unrelated to $\mathrm{Ad}^0 \bar{\rho}^*$.*
2. *Let M be a nontrivial quotient of $\mathrm{Ad}^0 \bar{\rho}^*$ and $\eta \in H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, M)$ be non-zero. Let K_η be the field extension of K cut out by η. The field K_η is G'-unrelated to $\mathrm{Ad}^0 \bar{\rho}^*$.*

Proof. Let Q be a G'-submodule of $\mathrm{Ad}^0 \bar{\rho}$, Lemma 3.3.2 asserts that $Q = \bigoplus_{\lambda \in \Phi \cup \{1\}} Q_{\sigma_\lambda}$. On the other hand, $\mathrm{Ad}^0 \bar{\rho}^* = \bigoplus_{\gamma \in \Phi \cup \{1\}} (\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_\lambda}$. It follows from condition (4) of Theorem 3.0.1 that

$$\mathrm{Hom}(Q_{\sigma_\lambda}, (\mathrm{Ad}^0\,\bar{\rho}^*)_{\bar{\chi}\sigma_\gamma})^{\mathbb{T}} = 0.$$

As a result, $\mathrm{Hom}(Q, \mathrm{Ad}^0\,\bar{\rho}^*)^{G'} = 0$ and hence part (1) follows.

For part (2), it suffices to show that M is unrelated to $\mathrm{Ad}^0\,\bar{\rho}^*$. Since M is a non-trivial quotient of $\mathrm{Ad}^0\,\bar{\rho}^*$, it follows from Lemma 3.3.3 that the $\bar{\chi}\sigma_{2L_1}$-eigenspace of M is zero. Let $N \subseteq M$ be a G'-submodule and $f : N \to \mathrm{Ad}^0\,\bar{\rho}^*$ be a homomorphism. The $\bar{\chi}\sigma_{2L_1}$-eigenspace of $f(N)$ is zero, hence by Lemma 3.3.3, the map $f = 0$. ☐

Lemma 3.3.16. *Let $L_1, \ldots, L_k$ and $K_1, \ldots, K_l$ be Galois extensions of $\mathbb{Q}$ which contain K. Assume that:*

- *$\mathrm{Gal}(L_i/K)$ and $\mathrm{Gal}(K_i/K)$ are finite dimensional $\mathbb{F}_p$-vector spaces.*
- *As a G'-module, $\mathrm{Gal}(L_i/K)$ is isomorphic to a subquotient of $\mathrm{Ad}^0\,\bar{\rho}$ for $i = 1, \ldots, k$.*
- *As a G'-module, $\mathrm{Gal}(K_i/K)$ is isomorphic to a subquotient of $\mathrm{Ad}^0\,\bar{\rho}^*$ for $i = 1, \ldots, l$.*

Then the composite $L_1 \cdots L_k$ is linearly disjoint from $K_1, \ldots, K_l$.

Proof. The order of $\mathbb{T}$ is coprime to p, hence Maschke's theorem asserts that any finite dimensional $\mathbb{F}_p[G']$-module M decomposes into a direct sum

$$M = \oplus_\tau M_\tau.$$

Here, τ is a character of $\mathbb{T}$ and M_τ is the τ-eigenspace

$$M_\tau := \{m \in M | g \cdot m = \tau(g)m\}.$$

The action of G' on $\mathrm{Gal}(L_i/K)$ and $\mathrm{Gal}(K_i/K)$ is induced by conjugation. By assumption, $\mathrm{Gal}(L_i/K)$ is isomorphic to a subquotient of $\mathrm{Ad}^0\,\bar{\rho}$, i.e. there exist G'-submodules $Q_1 \subseteq Q_2$ of $\mathrm{Ad}^0\,\bar{\rho}$ such that $\mathrm{Gal}(L_i/K) \simeq Q_2/Q_1$. By Lemma 3.3.2, the module Q_i decomposes into $\mathbb{T}$-eigenspaces

$$Q_i = \bigoplus_{\lambda \in \Phi \cup \{1\}} (Q_i)_{\sigma_\lambda}$$

for $i = 1, 2$. Therefore, the quotient $\mathrm{Gal}(L_i/K)$ decomposes into

$$\mathrm{Gal}(L_i/K) = \bigoplus_{\lambda \in \Phi \cup \{1\}} (\mathrm{Gal}(L_i/K))_{\sigma_\lambda}$$

where $(\mathrm{Gal}(L_i/K))_{\sigma_\lambda} := (Q_2)_{\sigma_\lambda}/(Q_1)_{\sigma_\lambda}$ is the σ_λ-eigenspace for the action of $\mathbb{T}$ on $\mathrm{Gal}(L_i/K)$. Likewise, $\mathrm{Gal}(K_i/K)$ decomposes into

$$\mathrm{Gal}(K_i/K) = \bigoplus_{\lambda \in \Phi \cup \{1\}} (\mathrm{Gal}(K_i/K))_{\bar{\chi}\sigma_\lambda}.$$

Let $\mathcal{L}$ be the composite $L_1 \cdots L_k$ and $\mathcal{K}$ be the composite $K_1 \cdots K_l$. Letting $\mathcal{L}_i$ be the composite $L_1 \cdots L_i$, filter $\mathcal{L}$ by

$$\mathcal{L} \supseteq \mathcal{L}_{k-1} \cdots \supseteq \mathcal{L}_1 \supseteq K.$$

The Galois group

$$\mathrm{Gal}(\mathcal{L}_i/\mathcal{L}_{i-1}) \simeq \mathrm{Gal}(L_i/L_i \cap \mathcal{L}_{i-1})$$

is a G'-submodule of $\mathrm{Gal}(L_i/K)$. Hence the characters for the action of $\mathbb{T}$ on $\mathrm{Gal}(\mathcal{L}_i/\mathcal{L}_{i-1})$ are each of the form σ_λ. Similar reasoning shows that the characters for the action of $\mathbb{T}$ on $\mathrm{Gal}(\mathcal{K}/K)$ are each of the form $\bar{\chi}\sigma_\lambda$. Set $E = \mathcal{K} \cap \mathcal{L}$ and $M = \mathrm{Gal}(E/K)$. Being a quotient of $\mathrm{Gal}(\mathcal{L}/K)$, M decomposes into eigenspaces for the action of the torus

$$M = \bigoplus_{\lambda \in \Phi \cup \{1\}} M_{\sigma_\lambda}.$$

Since M is a quotient of $\mathrm{Gal}(\mathcal{K}/K)$,

$$M = \bigoplus_{\gamma \in \Phi \cup \{1\}} M_{\bar{\chi}\sigma_\gamma}.$$

It is assumed that the image of σ_λ spans $\mathbb{F}_q$ and that σ_λ is not a $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ twist of $\bar{\chi}\sigma_\gamma$. Hence, it follows that

$$\mathrm{Hom}(\mathbb{F}_q(\sigma_\lambda), \mathbb{F}_q(\bar{\chi}\sigma_\gamma))^{\mathbb{T}} = 0.$$

Therefore, $\mathrm{Hom}(M, M)^{G'} = 0$ and in particular, the identity map is zero. This implies that $\mathcal{K} \cap \mathcal{L} = K$. □

3.4 Deformation conditions at Auxiliary Primes

We introduce the auxiliary primes v and the liftable deformation problem $\mathcal{C}_v$ at v.

Definition 3.4.1. *A prime number v is a trivial prime if the following splitting conditions are satisfied:*

- $\mathrm{G}_v \subseteq \ker \bar{\rho}$,

- $v \equiv 1 \mod p$ *and* $v \not\equiv 1 \mod p^2$.

In other words, a prime number v is trivial if it splits in $\mathbb{Q}(\bar{\rho}, \mu_p)$ and does not split in $\mathbb{Q}(\mu_{p^2})$. By Lemma 3.3.12, $\mathbb{Q}(\bar{\rho}, \mu_p)$ does not contain $\mathbb{Q}(\mu_{p^2})$. This is a Chebotarev condition, i.e. defined by a finite union of sets that are defined by applying the Chebotarev density theorem. Therefore, the set of trivial primes has positive Dirichlet density, in particular, it is infinite.

Let v be a trivial prime. The deformations of the trivial representation $\bar{\rho}_{\restriction \mathrm{G}_v}$ are tamely ramified. The Galois group of the maximal pro-p extension of $\mathbb{Q}_v$ is generated by a Frobenius σ_v and a generator of tame pro-p inertia τ_v. These satisfy the relation $\sigma_v \tau_v \sigma_v^{-1} = \tau_l^v$. We define the deformation functor $\mathcal{C}_v$. The functor $\mathcal{C}_v$ will be liftable, however, it will not be a deformation condition. Let α be a root which shall be specified later. The root-subgroup $\mathrm{U}_\alpha \subset \mathrm{GSp}_{2n}$ is the subgroup generated by the image of the root-subspace $(\mathrm{sp}_{2n})_\alpha$ under the exponential map. We let $\mathrm{Z}(\mathrm{U}_\alpha)$ be the subgroup of GSp_{2n} consisting of elements which commute with U_α.

Definition 3.4.2. *[4, Definition 3.1] Let $\mathcal{D}_v^\alpha$ consist of the deformation classes of lifts ϱ such that*

1. $\varrho(\sigma_v) \in \mathcal{T} \cdot Z(U_\alpha)$ *and* $\varrho(\tau_v) \in U_\alpha$*,*
2. *under the composite*

$$\mathcal{T} \cdot Z(U_\alpha) \to \mathcal{T}/(\mathcal{T} \cap Z(U_\alpha)) \xrightarrow{\alpha} GL_1$$

$\varrho(\sigma_v)$ maps to v.

Remark 3.4.3. *When $n = 1$ and α is the positive root of sl_2, the deformation functor $\mathcal{D}_v^\alpha$ consists of ϱ such that there exists x and y such that*

$$\varrho(\sigma_v) = c \begin{pmatrix} v & x \\ 0 & 1 \end{pmatrix} \text{ and } \varrho(\tau_v) = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}.$$

Here c is equal to $(\psi(\sigma_v)/v)^{\frac{1}{2}}$.

We shall denote by the kernel of α restricted to $\mathfrak{t}$ by $\mathfrak{t}_\alpha$. Since the action of G_v on $\mathrm{Ad}^0 \bar{\rho}$ is trivial,

$$H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}) = \mathrm{Hom}(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}).$$

Let $\mathcal{P}_v^\alpha$ be the subspace of $H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho})$ consisting of ϕ such that

$$\phi(\sigma_v) \in \mathfrak{t}_\alpha + \mathrm{Cent}((\mathrm{Ad}^0 \bar{\rho})_\alpha)$$

$$\phi(\tau_v) \in (\mathrm{Ad}^0 \bar{\rho})_\alpha.$$

Let Φ^α denote the subset of roots β such that $[(\mathrm{Ad}^0 \bar{\rho})_\alpha, (\mathrm{Ad}^0 \bar{\rho})_\beta] \neq 0$ and let $\mathcal{S}_v^\alpha$ consist of ϕ such that $\phi(\sigma_v) \in \bigoplus_{\beta \in \Phi^\alpha} (\mathrm{Ad}^0 \bar{\rho})_\beta$ and $\phi(\tau_v) = 0$. Recall that X_α is a choice of root vector for α.

Definition 3.4.4. 1. *Let v be a trivial prime which is unramified mod p^2 in our lifting argument. Set $\alpha = 2L_1$ and $\mathcal{C}_v = \mathcal{C}_v^{nr}$ consist of deformations*

$$\varrho' = (\mathrm{Id} + X_{-\alpha})\varrho(\mathrm{Id} + X_{-\alpha})^{-1}$$

where $\varrho \in \mathcal{D}_v^\alpha$. Associated to $\mathcal{C}_v$ is the space

$$\mathcal{N}_v = \mathcal{N}_v^{nr} := (\mathrm{Id} + X_{-\alpha})(\mathcal{P}_v^\alpha + \mathcal{S}_v^\alpha)(\mathrm{Id} + X_{-\alpha})^{-1}.$$

2. *Let v be a trivial prime which will be ramified mod p^2 in our lifting argument. Let $\alpha = -2L_1$ and $\mathcal{C}_v = \mathcal{C}_v^{ram} = \mathcal{D}_v^{\alpha}$ is the space $\mathcal{N}_v = \mathcal{N}_v^{ram}$ defined by*

$$\mathcal{N}_v := \mathcal{P}_v^{\alpha} + \mathcal{S}_v^{\alpha}.$$

Lemma 3.4.5. *Let v be a trivial prime and $\mathcal{C}_v = \mathcal{C}_v^{nr}$. Let $f \in \mathcal{N}_v$, express $f(\sigma_v) = \sum_{\lambda\in\Phi} a_\lambda X_\lambda + \sum_{i=1}^{n} a_i H_i$. Write $X_{-2L_1} = ce_{n+1,1}$ and $X_{2L_1} = de_{1,n+1}$. We have that $a_{2L_1} \neq -(cd)^{-1}a_1$.*

Proof. Set $g := (\mathrm{Id} + X_{-2L_1})^{-1} f (\mathrm{Id} + X_{-2L_1})$ and express $g(\sigma_v) = \sum_{\lambda\in\Phi} b_\lambda X_\lambda + \sum_{i=1}^{n} b_i H_i$. Observe that $b_1 = 0$ since $g \in \mathcal{P}_v^{2L_1} + \mathcal{S}_v^{2L_1}$. We have that

$$g(\sigma_v) = (\mathrm{Id} - X_{-2L_1}) f(\sigma_v)(\mathrm{Id} + X_{-2L_1}) = f(\sigma_v) + c[f(\sigma_v), e_{n+1,1}] - a_{2L_1} cd X_{-2L_1}$$

and hence it follows that $b_1 = a_1 + cda_{2L_1}$. Thus we have shown that $a_1 \neq -cda_{2L_1}$.

□

Lemma 3.4.6. *[4, Lemma 3.2, 3.6] Let v be a trivial prime (for which either $\mathcal{C}_v = \mathcal{C}_v^{ram}$ or $\mathcal{C}_v^{nr}$ is the chosen deformation condition) and $X \in \mathcal{N}_v$,*

1. $\dim \mathcal{N}_v = \dim \mathrm{Ad}^0 \bar{\rho} = h^0(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho})$.

2. *Let $m \geq 3$ and $\rho_m \in \mathcal{C}_v(\mathrm{W}(\mathbb{F}_q)/p^m)$, then*

$$(\mathrm{Id} + p^{n-1} X)\rho_m \in \mathcal{C}_v(\mathrm{W}(\mathbb{F}_q)/p^m).$$

3. *The deformation functor $\mathcal{C}_v$ is liftable.*

Prior to lifting $\bar{\rho}$ to characteristic zero, we show that $\bar{\rho}$ lifts to ρ_2 after increasing the set of ramification from S to $S \cup X_1$. One may choose a set theoretic τ of $\bar{\rho}$ as depicted

$$\begin{array}{ccc} & & \mathrm{GSp}_{2n}(\mathrm{W}(\mathbb{F}_q)/p^2) \\ & \overset{\tau}{\nearrow} & \downarrow \\ \mathrm{G}_{\mathbb{Q},S\cup X_1} & \xrightarrow[\bar{\rho}]{} & \mathrm{GSp}_{2n}(\mathbb{F}_q) \end{array}$$

such that the composite $\nu \circ \tau = \psi \mod p^2$. The obstruction class

$$\mathcal{O}(\bar{\rho})_{\restriction S\cup X_1} \in H^1(\mathrm{G}_{S\cup X_1}, \mathrm{Ad}^0 \bar{\rho})$$

is represented by the 2-cocycle

$$(g_1, g_2) \mapsto \tau(g_1 g_2)\tau(g_2)^{-1}\tau(g_1)^{-1}.$$

The residual representation $\bar{\rho}$ lifts to a representation ρ_2 ramified only at primes in $S \cup X_1$ if and only if this obstruction is zero. For $v \in S$, the local representation $\bar{\rho}_{\restriction \mathrm{G}_v}$ satisfies $\mathcal{C}_v$ which is a liftable deformation condition (by assumption) and thus lifts to mod p^2. The residual representation $\bar{\rho}$ is unramified at each prime $v \in X_1$ and thus it is easy to see that $\bar{\rho}_{\restriction \mathrm{G}_v}$ lifts to mod p^2 for $v \in X_1$. As a consequence, $\mathcal{O}(\bar{\rho})_{\restriction S\cup X_1}$ is contained in $Ш^2_{S\cup X_1}(\mathrm{Ad}^0 \bar{\rho})$. We will show that a set of finitely many trivial primes X_1 can be chosen so that

$$Ш^2_{S\cup X_1}(\mathrm{Ad}^0 \bar{\rho}) = 0.$$

For such a choice of X_1, there is a deformation ρ_2

$$\begin{array}{ccc} & & \mathrm{GSp}_{2n}(\mathrm{W}(\mathbb{F}_q)/p^2) \\ & \overset{\rho_2}{\nearrow} & \downarrow \\ \mathrm{G}_{\mathbb{Q},S\cup X_1} & \xrightarrow[\bar{\rho}]{} & \mathrm{GSp}_{2n}(\mathbb{F}_q). \end{array}$$

Proposition 3.4.7. *Let $\mathcal{M}$ denote the finite set of $\mathrm{G}_{\mathbb{Q}}$-modules defined by*

$$\begin{aligned} \mathcal{M} :=& \{(\mathrm{Ad}^0 \bar{\rho})/(\mathrm{Ad}^0 \bar{\rho})_k, \mid -2n+1 \leq k \leq 2n-1\} \\ & \cup \{(\mathrm{Ad}^0 \bar{\rho})_k^{\perp}, \mid -2n+1 \leq k \leq 2n-1\}. \end{aligned}$$

There is a finite set $T \supset S$ such that T/S consists of only trivial primes such that for all $M \in \mathcal{M}$,

$$\ker\{H^1(\mathrm{G}_{\mathbb{Q},T}, M) \to \bigoplus_{w \in T \setminus S} H^1(\mathrm{G}_w, M)\} = 0 \tag{3.4}$$

and so in particular,

$$Ш^1_T(M) = 0.$$

Proof. We show that T can be chosen for which

$$Ш^1_T(\mathrm{Ad}^0 \bar{\rho}^*) = 0,$$

the argument for any $M \in \mathcal{M}$ is identical. For $0 \neq \psi \in H^1(\mathrm{G}_{\mathbb{Q},S}, \mathrm{Ad}^0 \bar{\rho}^*)$, let $K_\psi \supset \mathbb{Q}(\mathrm{Ad}^0 \bar{\rho}^*)$ be the field extension cut out by ψ. By Lemma 3.3.8, the extension K_ψ is not equal to $\mathbb{Q}(\mathrm{Ad}^0 \bar{\rho}^*)$. The extension $K(\mu_{p^2})$ is linearly disjoint with K_ψ over K. By Lemma 3.3.12, $K(\mu_{p^2})$ is not contained in K and $K(\mu_{p^2}) \cap K_\psi = K$. As a result, there is a nonempty Chebotarev class of primes which split in K and are non-split in K_ψ and $K(\mu_{p^2})$. If v is such a prime, it must be a trivial prime since it splits in K and is non-split in $\mathbb{Q}(\mu_{p^2})$. On the other hand, since v is non-split in K_ψ, deduce that $\psi_{\restriction \mathrm{G}_v} \neq 0$. We may therefore choose a finite set of primes T such that

- T is finite,
- $T \backslash S$ consists of only trivial primes,
- $\ker\{H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0 \bar{\rho}^*) \to \bigoplus_{w \in T \backslash S} H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho}^*)\} = 0.$

□

The set of trivial primes $X_1 := T \backslash S$.

3.5 Lifting to mod p^3

By Proposition 3.4.7, there is a finite set of primes T containing S such that $T \backslash S$ consists of trivial primes and $Ш^1_T(\mathrm{Ad}^0 \bar{\rho}^*) = 0$. Let X_1 be the set of trivial primes $T \backslash S$. At each prime $v \in X_1$, set $\mathcal{C}_v$ be the liftable deformation problem $\mathcal{C}_v^{nr}$. By Global-duality, $Ш^2_T(\mathrm{Ad}^0 \bar{\rho}) = 0$ and thus the cohomological obstruction to lifting

$\bar\rho$ to a representation ζ_2

$$\begin{array}{ccc} & & \mathrm{GSp}_{2n}(\mathrm{W}(\mathbb{F}_q)/p^2) \\ & \overset{\zeta_2}{\nearrow} & \downarrow \\ \mathrm{G}_{\mathbb{Q},T} & \xrightarrow[\bar\rho]{} & \mathrm{GSp}_{2n}(\mathbb{F}_q) \end{array} \tag{3.5}$$

vanishes. Let $v \in T$, recall that the set of $W(\mathbb{F}_q)/p^2$ lifts of $\bar\rho_{\restriction \mathrm{G}_v}$ is an $H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar\rho)$-torsor. Therefore there exists $z_v \in H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar\rho)$ such that the twist $(\mathrm{Id} + z_v p)\zeta_{2 \restriction \mathrm{G}_v}$ satisfies $\mathcal{C}_v$. Further, for $v \in X_1$, the class z_v may is chosen so that this twist is unramified. We show that there is a set W of at most two trivial primes such that on increasing the set T to $Z = T \cup W$ there exists a global cohomology class $h \in H^1(\mathrm{G}_{\mathbb{Q},Z}, \mathrm{Ad}^0 \bar\rho)$ such that

- $h_{\restriction \mathrm{G}_v} = z_v$ for $v \in T$,
- $h_{\restriction \mathrm{G}_v} \in \mathcal{C}_v^{ram}$ for $v \in W$.

Further, letting ρ_2 be the twist $\rho_2 = (\mathrm{Id} + hp)\zeta_2$, each local representation $\rho_{2 \restriction \mathrm{G}_v}$ satisfies $\mathcal{C}_v$ for $v \in Z$. As a consequence, the obstruction class $\mathcal{O}(\rho_2)$ is in $\text{Ш}^2_Z(\mathrm{Ad}^0 \bar\rho)$. Since Z contains T, the group $\text{Ш}^2_Z(\mathrm{Ad}^0 \bar\rho)$ is zero. As a result, ρ_2 must lift to a $W(\mathbb{F})/p^3$. Assume that there is no such class h for a set W such that $\#W \leq 1$. It is shown that there is a pair of trivial primes $v_1, v_2 \notin T$ such that W can be chosen to be equal to $\{v_1, v_2\}$. The set of trivial primes X_2 is then chosen to be $Z \backslash S$. For $v \in W$, choose $\mathcal{C}_v$ to be equal to $\mathcal{C}_v^{ram}$.

Proposition 3.5.1. *Let T be as in Proposition 3.4.7 and ψ be a nonzero element in $H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0\,\bar{\rho}^*)$ and let $W \subset H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0\,\bar{\rho}^*)$ be a subspace not containing ψ. Then, there exists a trivial prime v such that*

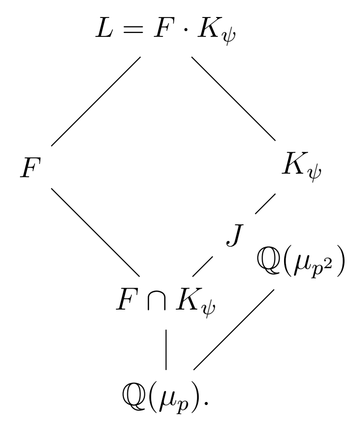
$$\psi_{\restriction \mathrm{G}_v} \neq 0$$

$$\beta_{\restriction \mathrm{G}_v} = 0 \text{ for all } \beta \in W.$$

Moreover we may choose v so that v does not split completely in the $\bar{\chi}\sigma_{2L_1}$-eigenspace of $\mathrm{Gal}(K_\psi/K)$ when viewed as a Galois submodule of $\mathrm{Ad}^0\,\bar{\rho}^*$.

Proof. Let $\{\psi_1, \ldots, \psi_r\}$ be a basis of W and denote by the composite $F := K_{\psi_1} \cdots K_{\psi_r}$. Set $P = \mathrm{Gal}(K_\psi/K)$ and let $J \subset K_\psi$ be the field fixed by $P_{\bar{\chi}\sigma_{2L_1}}$. Since $\psi \neq 0$ by Lemma 3.3.7 it follows that $P \neq 0$. As a consequence of Lemma 3.3.3 of Theorem 3.0.1 we deduce that $P_{\bar{\chi}\sigma_{2L_1}} \neq 0$ and in particular, $J \subsetneq K_\psi$. We will show that $F \cap K_\psi \subseteq J$. First we show how the result follows from this.

Set $L = F \cdot K_\psi = K_{\psi_1} \cdots K_{\psi_r} \cdot K_\psi$. We consider the following field diagram,



By Lemma 3.3.12, the intersection $\mathbb{Q}(\mu_{p^2}) \cap K = \mathbb{Q}(\mu_p)$. In fact, Lemma 3.3.12 asserts that $F \cap \mathbb{Q}(\mu_{p^2}) = \mathbb{Q}(\mu_p)$. Therefore there is a prime v which is

1. split in $\mathrm{Gal}(F/\mathbb{Q})$,
2. nonsplit in $\mathrm{Gal}(\mathbb{Q}(\mu_{p^2})/\mathbb{Q}(\mu_p))$,
3. nonsplit in $\mathrm{Gal}(K_\psi/J)$.

Since $K = \mathbb{Q}(\bar{\rho}, \mu_p)$ is contained in F, the prime v is a trivial prime. Since v splits in $\mathrm{Gal}(F/\mathbb{Q})$, we have that $\psi_{i\restriction \mathrm{G}_v} = 0$ for $i = 1, \ldots, r$. Since v does not split in $\mathrm{Gal}(K_\psi/K)$, we have that $\psi_{\restriction \mathrm{G}_v} \neq 0$.

We begin by showing that K_ψ is not contained in F. This is equivalent to the assertion that $F \cdot K_\psi \neq F$. By inflation-restriction,

$$h^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) = h^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0 \bar{\rho}^*) \geq r + 1.$$

It suffices to show that $h^1(\mathrm{Gal}(F/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) \leq r$. We show by induction on i that

$$h^1(\mathrm{Gal}(K_{\psi_1} \cdots K_{\psi_i}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) \leq i.$$

Lemma $3.3.7$ asserts that $H^1(G' \, \mathrm{Ad}^0 \bar{\rho}^*) = 0$ and hence by inflation-restriction,

$$H^1(\mathrm{Gal}(K_{\psi_1}/\mathbb{Q}), \mathrm{Ad}^0 \bar{\rho}^*) \simeq \mathrm{Hom}(P_1, \mathrm{Ad}^0 \bar{\rho}^*)^{G'}.$$

Lemma $3.3.9$ asserts that

$$\dim \mathrm{Hom}(P_1, \mathrm{Ad}^0 \bar{\rho}^*)^{G'} \leq 1$$

and hence the case $i = 1$ follows.

For the induction step, set $F_i = K_{\psi_1} \cdots K_{\psi_i}$ and

$$P_i := \mathrm{Gal}(F_i/F_{i-1}) \simeq \mathrm{Gal}(K_{\psi_i}/K_{\psi_i} \cap F_{i-1}).$$

Lemma 3.3.9 asserts that

$$\dim \operatorname{Hom}(P_i, \operatorname{Ad}^0 \bar{\rho}^*)^{G'} \leq 1$$

from which we see from inflation-restriction

$$h^1(\operatorname{Gal}(F_i/\mathbb{Q}), \operatorname{Ad}^0 \bar{\rho}^*) \leq h^1(\operatorname{Gal}(F_{i-1}/\mathbb{Q}), \operatorname{Ad}^0 \bar{\rho}^*) + 1.$$

We conclude that $L \neq F$ and thus we have deduced that $K_\psi \cap F \neq K_\psi$. Set $Q := \operatorname{Gal}(K_\psi/K_\psi \cap F)$, by Lemma 3.3.3,

$$Q_{\bar{\chi}\sigma_{2L_1}} \simeq (\operatorname{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{2L_1}} \simeq P_{\bar{\chi}\sigma_{2L_1}}.$$

We deduce that $K_\psi \cap F$ is contained in J. This completes the proof. □

Definition 3.5.2. *Let $\mathcal{J}$ be a set of trivial primes that contains the set S and $v \notin \mathcal{J}$ be a trivial prime. Denote by $\Psi_{\mathcal{J}}$ and $\Psi^k_{\mathcal{J},v}$ the maps defined by*

$$\Psi^k_{\mathcal{J}} : H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}}, (\operatorname{Ad}^0 \bar{\rho})_k) \xrightarrow{res_{\mathcal{J}}} \bigoplus_{w \in \mathcal{J}} H^1(\mathrm{G}_w, (\operatorname{Ad}^0 \bar{\rho})_k)$$

and

$$\Psi^k_{\mathcal{J},v} : H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}\cup\{v\}}, (\operatorname{Ad}^0 \bar{\rho})_k) \xrightarrow{res_{\mathcal{J}}} \bigoplus_{w \in \mathcal{J}} H^1(\mathrm{G}_w, (\operatorname{Ad}^0 \bar{\rho})_k).$$

Let τ_v be a generator of the maximal pro-p quotient of the tame inertia at v, denote by

$$\pi^k_{\mathcal{J},v} : H^1(\mathrm{G}_{\mathbb{Q},\mathcal{J}\cup\{v\}}, (\operatorname{Ad}^0 \bar{\rho})_k) \to (\operatorname{Ad}^0 \bar{\rho})_k$$

be the evaluation map defined by

$$\pi^k_{\mathcal{J},v}(f) := f(\tau_v).$$

Lemma 3.5.3. *Let T be a set of trivial primes as in Proposition 3.4.7 that contains the set S and k an integer. Suppose $v \notin T$ is a trivial prime with the property that for all $\beta \in H^1(\mathrm{G}_T, (\mathrm{Ad}^0\,\bar{\rho})^*_k)$, the restriction $\beta_{\restriction \mathrm{G}_v} = 0$. The following are exact:*

$$0 \to \ker \Psi^k_T \xrightarrow{inf} \ker \Psi^k_{T,v} \xrightarrow{\pi^k_v} (\mathrm{Ad}^0\,\bar{\rho})_k \to 0, \tag{3.6}$$

$$0 \to H^1(\mathrm{G}_T, (\mathrm{Ad}^0\,\bar{\rho})_k) \xrightarrow{inf} H^1(\mathrm{G}_{T\cup\{v\}}, (\mathrm{Ad}^0\,\bar{\rho})_k) \xrightarrow{\pi^k_v} (\mathrm{Ad}^0\,\bar{\rho})_k \to 0. \tag{3.7}$$

Further, the image of Ψ_T is equal to the image of $\Psi_{T,v}$.

Proof. Clearly the composite of the maps is zero and (3.6) is exact in the middle. Denote by res_v the restriction map:

$$\mathrm{res}_v : H^1(\mathrm{G}_{T\cup\{v\}}, (\mathrm{Ad}^0\,\bar{\rho})^*_k) \to H^1(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})^*_k).$$

By assumption, $H^1(\mathrm{G}_T, (\mathrm{Ad}^0\,\bar{\rho})^*_k)$ and $\ker \mathrm{res}_v$ are equal. By the local Euler characteristic formula and local duality,

$$h^1(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})_k) - h^0(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})_k)$$

$$= h^2(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})_k) = h^0(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})^*_k) = \dim \mathrm{Ad}^0\,\bar{\rho}.$$

By Wiles' Formula (3.2),

$$\begin{aligned}\dim \ker \Psi^k_{T,v} &= \dim \ker \Psi^k_T + \dim \ker \mathrm{res}_v - h^1(\mathrm{G}_T, (\mathrm{Ad}^0\,\bar{\rho})^*_k) \\ &\quad + h^1(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})^*_k) - h^0(\mathrm{G}_v, (\mathrm{Ad}^0\,\bar{\rho})^*_k) \\ &= \dim \ker \Psi^k_T + \dim (\mathrm{Ad}^0\,\bar{\rho})_k\end{aligned}$$

and the exactness of (3.6) follows. The exactness of (3.7) follows by the same arguments. Therefore,

$$\begin{aligned}\dim \operatorname{im} \Psi_{T,v} =& h^1(\mathrm{G}_{T\cup\{v\}}, (\mathrm{Ad}^0 \bar{\rho})_k) - \dim \ker \Psi_{T,v} \\ =& h^1(\mathrm{G}_T, (\mathrm{Ad}^0 \bar{\rho})_k) - \dim \ker \Psi_T = \dim \operatorname{im} \Psi_T.\end{aligned}$$

□

Let M be an $\mathbb{F}_q[\mathrm{G}_v]$-module which is a finite dimensional $\mathbb{F}_q$-vector space. The cup product induces the map

$$H^1(\mathrm{G}_v, M) \times H^1(\mathrm{G}_v, M^*) \to H^2(\mathrm{G}_v, \mathbb{F}_q(\bar{\chi})) \xrightarrow{\sim} \mathbb{F}_q$$

taking $f_1 \in H^1(\mathrm{G}_w, M)$ and $f_2 \in H^1(\mathrm{G}_w, M^*)$ to $\mathrm{inv}_w(f_1 \cup f_2) \in \mathbb{F}_q$. Define the non-degenerate pairing

$$\left(\bigoplus_{w\in T} H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho})\right) \times \left(\bigoplus_{w\in T} H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho}^*)\right) \to \mathbb{F}_q$$

defined by $a \cup b = \sum_{w\in T} \mathrm{inv}_w(a_w \cup b_w)$. Denote by $\mathrm{Ann}((z_w)_{w\in T})$ the annihilator of the tuple $(z_w)_{w\in T}$. If the tuple $(z_w)_{w\in T}$ is not zero, then $\mathrm{Ann}((z_w)_{w\in T})$ is codimension one. Recall that we assume that $(z_w)_{w\in T}$ does not arise from a global class unramified outside T. This implies that ${\Psi_T^*}^{-1}(\mathrm{Ann}(z_w)_{w\in T})$ has codimension one in $H^1(\mathrm{G}_T, \mathrm{Ad}^0 \bar{\rho}^*)$. Set $(\mathrm{Ad}^0 \bar{\rho})_{-2L_1}$ for the $\mathbb{F}_q$ span of the root vector X_{-2L_1}.

Proposition 3.5.4. *Let T be as in Proposition 3.4.7. There exists a Chebotarev class $\mathfrak{l}$ of trivial primes v such that*

1. $\beta_{\restriction \mathrm{G}_v} = 0$ *for all* $\beta \in H^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0 \bar{\rho})^*_d)$ *for* $d \geq -2n+2$,

2. *there exists an* $\mathbb{F}_q$ *basis* $\{\psi, \psi_1, \dots, \psi_r\}$ *of* $H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0 \bar{\rho}^*)$ *such that*

   - $\{\psi_1, \dots, \psi_r\}$ *is a basis of* $\Psi_T^{*\,-1}(Ann(z_w)_{w \in T})$
   - $\psi_{\restriction \mathrm{G}_v} \neq 0$ *and* $\psi_{j\,\restriction \mathrm{G}_v} = 0$ *for all* $j \geq 1$.

Furthermore, there is, for each $v \in \mathfrak{l}$*, an element* $h^{(v)} \in H^1(\mathrm{G}_{T \cup \{v\}}, \mathrm{Ad}^0 \bar{\rho})$ *such that*

$$h^{(v)}|_{\mathrm{G}_w} = z_w$$

for all $w \in T$ *and*

$$h^{(v)}(\tau_v) \in (\mathrm{Ad}^0 \bar{\rho})_{-2L_1} \backslash \{0\}. \tag{3.8}$$

Proof. First, we analyze condition (1). By Lemma 3.3.3, we have that $(\mathrm{Ad}^0 \bar{\rho})^*_d$ is the direct sum of subgroups $(\mathrm{Ad}^0 \bar{\rho})^*_{d,\bar{\chi}\sigma_\lambda}$ for $\lambda \in \Phi \cup \{1\}$ with $ht(\lambda) \geq d$. By condition 4 of Theorem 3.0.1, the characters $\sigma_\lambda \neq \bar{\chi}^{-1}$. Let Q be Galois stable submodule of $\mathrm{Ad}^0 \bar{\rho}^*$. It follows from Lemma 3.3.2 that

$$(\mathrm{Ad}^0 \bar{\rho}^*)_d / Q = \bigoplus_{\Phi \cup \{1\}} (\mathrm{Ad}^0 \bar{\rho}^*)_{d,\bar{\chi}\sigma_\lambda} / Q_{\bar{\chi}\sigma_\lambda}.$$

Hence there is no proper Galois stable submodule Q of $(\mathrm{Ad}^0 \bar{\rho})^*_d$ for which the Galois action on $(\mathrm{Ad}^0 \bar{\rho})^*_d / Q$ is trivial. Hence the splitting conditions imposed by condition (1) are independent of the non-splitting condition in $\mathbb{Q}(\mu_{p^2})$ imposed by the fact that trivial primes are not $1 \mod p^2$.

Analyze the non-splitting condition of v in K_ψ imposed by condition (2). By Lemma 3.3.8, we have that $K_\psi \neq K$. Identify $P := \mathrm{Gal}(K_\psi/K)$ with $\psi(G_K) \subset \mathrm{Ad}^0 \bar{\rho}^*$ and by Lemma 3.3.3, the $P_{\bar{\chi}\sigma_{2L_1}} \simeq (\mathrm{Ad}^0 \bar{\rho}^*)_{\bar{\chi}\sigma_{2L_1}}$. On invoking Proposition

3.5.1 we deduce that these conditions are satisfied by a Chebotarev class of trivial primes v.

Therefore, conditions (1) and (2) are satisfied independently by Chebotarev classes. They may be simultaneously satisfied by a Chebotarev class. To show this, note that the splitting conditions in $(\mathrm{Ad}^0\,\bar{\rho}^*)_d = \bigoplus_{\mathrm{ht}(\lambda)\geq d}(\mathrm{Ad}^0\,\bar{\rho}^*)_{d,\bar{\chi}\sigma_\lambda}$ are independent of the non-splitting condition of v in $P_{\bar{\chi}\sigma_{2L_1}}$. This follows since the characters σ_λ are all distinct by assumption.

We show that $h^{(v)}$ exists as specified. Let $d > -2n+1$, a trivial prime v for which condition (1) is satisfied, by Lemma 3.5.3, the image of

$$\Psi_T^d : H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0\,\bar{\rho})_d) \to \bigoplus_{w\in T} H^1(\mathrm{G}_w, (\mathrm{Ad}^0\,\bar{\rho})_d)$$

is the same as the image of

$$\Psi_{T,v}^d : H^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0\,\bar{\rho})_d) \to \bigoplus_{w\in T} H^1(\mathrm{G}_w, (\mathrm{Ad}^0\,\bar{\rho})_d).$$

For a trivial prime v for which condition (2) is satisfied, it follows from an application of Wiles' formula (3.2) that the image of the map

$$\Psi_{T,v} : H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, \mathrm{Ad}^0\,\bar{\rho}) \to \bigoplus_{w\in T} H^1(\mathrm{G}_w, \mathrm{Ad}^0\,\bar{\rho})$$

is greater than that of the map

$$\Psi_T : H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0\,\bar{\rho}) \to \bigoplus_{w\in T} H^1(\mathrm{G}_w, \mathrm{Ad}^0\,\bar{\rho}).$$

We deduce the existence of $h^{(v)} \in H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, \mathrm{Ad}^0\,\bar{\rho})$ satisfying the specified properties. Since the image of $\Psi_{T,v}$ is greater than the image of Ψ_T, there is a class g in $H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, \mathrm{Ad}^0\,\bar\rho)$ such that $\Psi_{T,v}(g) \notin$ Image(Ψ_T). Let

$$W_1 := \text{Image}(\Psi_T) + \mathbb{F}_q \cdot \Psi_{T,v}(g)$$

and

$$W_2 := \text{Image}(\Psi_T) + \mathbb{F}_q \cdot (z_w)_{w\in T}.$$

The argument in [9, Proposition 34] applies verbatim to imply that $W_1 = W_2$ and so we deduce the existence of $h^{(v)} \in H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, \mathrm{Ad}^0\,\bar\rho)$ for which

$$h^{(v)}_{\restriction \mathrm{G}_w} = z_{w\restriction \mathrm{G}_w}$$

for all $w \in T$. As we have observed,

$$\text{Image}(\Psi_T^{-2n+2}) = \text{Image}(\Psi_{T,v}^{-2n+2})$$

since $h^{(v)} \notin$ Image(Ψ_T) it follows that $h^{(v)}(\tau_v)$ is not contained in $(\mathrm{Ad}^0\,\bar\rho)_{-2n+2}$. Invoking Lemma $3.5.3$, we deduce that on adding a suitable linear combination of elements to $h^{(v)}$ from $\ker \Psi_{T,v}^d$ for $d > -2n+1$, we modify the class $h^{(v)}$ so that

$$h^{(v)}(\tau_v) \in (\mathrm{Ad}^0\,\bar\rho)_{-2L_1} \backslash \{0\}$$

as required. □

Lemma 3.5.5. *Let* $\mathfrak{l}$ *be the Chebotarev class of trivial primes in the Proposition* $3.5.4$ *and* $\zeta \in \mathbb{F}_q(\bar\chi)$ *be a nontrivial element. There exists an* $\mathbb{F}_q$*-independent set*

$$\{\eta_\lambda^{(v)} \mid \lambda \in \Phi\} \cup \{\, \eta_1^{(v)}, \dots, \eta_n^{(v)}\}$$

contained in $H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, \mathrm{Ad}^0\,\bar\rho^*)$*, satisfying the following properties:*

1. $\eta_\lambda^{(v)} \in H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0 \bar{\rho})_{h+1}^{\perp})$ *where* $h = \mathrm{ht}(\lambda)$,
2. $\eta_i^{(v)} \in H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0 \bar{\rho})_1^{\perp})$,
3. $\eta_\lambda^{(v)}(\tau_v) = \zeta X_\lambda^*$,
4. $\eta_i^{(v)}(\tau_v) = \zeta H_i^*$,
5. *the images of the elements* $\eta_\lambda^{(v)}$ *are a basis for the cokernel of the map*

$$H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0 \bar{\rho}^*) \to H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}^*).$$

Proof. As T is chosen such that $\text{Ш}_T^1((\mathrm{Ad}^0 \bar{\rho})_k^{\perp *}) = 0$ for all $k \in \mathbb{Z}$, Wiles' formula (3.2) asserts that

$$\begin{aligned}
&h^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp}) - \dim \text{Ш}_{T\cup\{v\}}^1((\mathrm{Ad}^0 \bar{\rho})_k^{\perp *}) \\
=&h^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp}) - \dim \text{Ш}_T^1((\mathrm{Ad}^0 \bar{\rho})_k^{\perp *}) \\
+&h^1(\mathrm{G}_v, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp}) - h^0(\mathrm{G}_v, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp}).
\end{aligned}$$

The dual to $(\mathrm{Ad}^0 \bar{\rho})_k^{\perp}$ is $\mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_k$. Proposition 3.4.7 asserts that $\text{Ш}_T^1(\mathrm{Ad}^0 \bar{\rho}/(\mathrm{Ad}^0 \bar{\rho})_k) = 0$. On applying the local Euler characteristic formula and Tate duality we have that

$$h^1(\mathrm{G}_v, (\mathrm{Ad}^0 \bar{\rho})_k)^{\perp} - h^0(\mathrm{G}_v, (\mathrm{Ad}^0 \bar{\rho})_k)^{\perp}) = h^0(\mathrm{G}_v, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp *}) = \dim(\mathrm{Ad}^0 \bar{\rho})_k^{\perp}.$$

For the last equality, note that $\bar{\chi}_{\restriction \mathrm{G}_v} = 1$ since $v \equiv 1 \mod p$ and that the action on $(\mathrm{Ad}^0 \bar{\rho})_k)^{\perp}$ is trivial. It follows that

$$h^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp}) = h^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0 \bar{\rho})_k^{\perp}) + \dim(\mathrm{Ad}^0 \bar{\rho})_k^{\perp}$$

and the evaluation map at τ_v

$$H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0\,\bar{\rho})_k^\perp) \to (\mathrm{Ad}^0\,\bar{\rho})_k^\perp$$

induces a short exact sequence

$$0 \to H^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0\,\bar{\rho})_k^\perp) \to H^1(\mathrm{G}_{\mathbb{Q},T\cup\{v\}}, (\mathrm{Ad}^0\,\bar{\rho})_k^\perp) \to (\mathrm{Ad}^0\,\bar{\rho})_k^\perp \to 0.$$

The assertion of the Lemma follows. □

Let v a trivial prime in the Chebotarev class $\mathfrak{l}$ of Proposition 3.5.4. For $\lambda \in \Phi$, denote by $K_\lambda^{(v)} := K_{\eta_\lambda^{(v)}}$ and for $i = 1, \dots, n$, set $K_i^{(v)} := K_{\eta_i^{(v)}}$. When there no cause for confusion, set $K_\lambda = K_\lambda^{(v)}$ and $K_i = K_i^{(v)}$. Let $J_i \subsetneq K_i$ and $J_\lambda \subsetneq K_\lambda$ denote $J_{\eta_i^{(v)}}$ and $J_{\eta_\lambda^{(v)}}$ respectively. If $E = K_i$ (resp. K_λ), denote by J_E the sub-extension J_i (resp. J_λ). Set $\mathcal{F}^{(v)}$ to denote the collection of fields consisting of $K_i^{(v)}$ for $i = 1, \dots, n$ and $K_\lambda^{(v)}$ for $\lambda \in \Phi$. Let $\mathcal{F}_\mathfrak{l}$ be the collection of fields:

- K_{ψ_i} from Proposition 3.5.4 on which Chebotarev conditions define $\mathfrak{l}$,
- K_β as β runs through all cohomology classes $H^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0\,\bar{\rho}^*)_l)$, where $l > -2n+1$,
- $K(\mu_{p^2})$.

Associate to a set of trivial primes $A = \{v_1, \dots, v_k\}$ in $\mathfrak{l}$,

$$\mathcal{F}_A := \cup_{i=1}^k \mathcal{F}^{(v_i)}, \text{ and } \mathcal{L}_A := \{L_{h^{(v_1)}}, \dots, L_{h^{(v_k)}}\}.$$

Lemma 3.5.6. *Let* $A = \{v_1, \dots, v_k\} \subset \mathfrak{l}$.

1. *Let $F_1 \in \mathcal{F}_A$ and F_2 be the composite of all the other fields in $\mathcal{L}_A \cup \mathcal{F}_A \cup \mathcal{F}_{\mathfrak{l}}$. Then F_1 is not contained in F_2. Moreover, the intersection $F_1 \cap F_2$ is contained in J_{F_1}.*
2. *Let $L_1 \in \mathcal{L}_A$ and L_2 the composite of all the other fields in $\mathcal{F}_A \cup \mathcal{L}_A \cup \mathcal{F}_{\mathfrak{l}}$. The intersection $L_1 \cap L_2 = L$.*

Proof. For part (1), set $\psi_1, \dots, \psi_m$ to be a basis of $H^1(\mathrm{G}_{\mathbb{Q},T}, \mathrm{Ad}^0 \bar{\rho}^*)$ as in Proposition 3.5.4. The classes $\eta_j^{(v_i)}$ and $\eta_\lambda^{(v_i)}$ for $i = 1, \dots, k$, $j = 1, \dots, n$ and $\lambda \in \Phi \cup \{1\}$ are linearly independent. Enumerate these classes by $\eta_1, \dots, \eta_d$ so that $F_1 = K_{\eta_1}$. The other fields in $\mathcal{F}_A \cup \mathcal{F}_{\mathfrak{l}}$ are $K_{\eta_2}, \cdots, K_{\eta_d}$ and the fields K_β, as β runs through all cohomology classes $H^1(\mathrm{G}_{\mathbb{Q},T}, (\mathrm{Ad}^0 \bar{\rho}^*)_l)$ for $l > -2n+1$. By Lemma 3.3.15, the fields K_β are unrelated to $\mathrm{Ad}^0 \bar{\rho}^*$. Since the G' action on $\mathrm{Gal}(K(\mu_{p^2})/K)$ is trivial, $K(\mu_{p^2})$ is also unrelated to $\mathrm{Ad}^0 \bar{\rho}^*$. By Proposition 3.3.14, F_1 is not contained in F_2 and it follows from Lemma 3.3.3 that $F_1 \cap F_2 \subseteq J_{F_1}$.

Assume WLOG that $L_1 = L_{h^{(v_1)}}$. The prime v_1 is ramified in the σ_{-2L_1}-eigenspace of $\mathrm{Gal}(L_1/L)$ and unramified in the σ_{-2L_1}-eigenspace of $\mathrm{Gal}(L_2/L)$. Therefore, $L_1 \nsubseteq L_2$. Identify $Q := \mathrm{Gal}(L_1/L_1 \cap L_2)$ with a subgroup of $h^{(v_1)}(\mathrm{G}_L) \subseteq \mathrm{Ad}^0 \bar{\rho}$. By Lemma 3.3.11 it suffices to show that $Q_{-2L_1} \neq 0$. Since v_1 is unramified in L_2, the image of τ_{v_1} in $\mathrm{Gal}(L_1/L)$ lies in $\mathrm{Gal}(L_1/L_1 \cap L_2)$. From the fact that $h^{(v_1)}(\tau_{v_1})$ is in $(\mathrm{Ad}^0 \bar{\rho})_{-2L_1} \backslash \{0\}$ we deduce that $Q_{-2L_1} \neq 0$. The assertion (2) follows. □

Lemma 3.5.7. *Let $v \in \mathfrak{l}$ and $h^{(v)}$ be as in Proposition 3.5.4. Then the $\mathrm{Gal}(L_{h^{(v)}}/L) \simeq \mathrm{Ad}^0 \bar{\rho}$.*

Proof. Let $Q := \mathrm{Gal}(L_{h^{(v)}}/L) \subseteq \mathrm{Ad}^0 \bar{\rho}$. Since $Q_{-2L_1} \neq 0$, the assertion follows from Lemma 3.3.11. $\square$

Proposition 3.5.8. *For a pair (v_1, v_2) of trivial primes in $\mathfrak{l}$ in Proposition 3.5.4 set $h = -h^{(v_1)} + 2h^{(v_2)}$ and $\rho_2 := (I + ph)\zeta_2$. There is a pair (v_1, v_2) such that $\rho_{2\restriction \mathrm{G}_w} \in \mathcal{C}_w$ for all $w \in T$ and $\rho_{2\restriction \mathrm{G}_{v_i}} \in \mathcal{C}_{v_i}^{ram}$ for $i = 1, 2$.*

Proof. For $i = 1, 2$, we set $\mathcal{C}_{v_i} := \mathcal{C}_{v_i}^{ram}$. Note that $h_{\restriction \mathrm{G}_w} = z_w$ for all $w \in T$ and hence $\rho_{2\restriction \mathrm{G}_w} \in \mathcal{C}_w$ for all $w \in T$. For each $v \in \mathfrak{l}$ choose z_v such that $(I + pz_v)\zeta_2 \in \mathcal{C}_v^{ram}$. We show that v_1 and v_2 may be chosen so that $h_{\restriction \mathrm{G}_{v_i}} = z_{v_i}$ for $i = 1, 2$. Consider for $v \in \mathfrak{l}$ the elements $h^{(v)}(\sigma_v)$ and let A be the matrix that occurs most frequently, that is, with maximal upper density. The choice of A is not necessarily unique. Let $\mathfrak{l}_1 = \{v \in \mathfrak{l} \mid h^{(v)}(\sigma_v) = A\}$. Since there are finitely many choices for A, the set of primes $\mathfrak{l}_1$ has positive upper-density. Since $h(\tau_{v_i}) \in (\mathrm{Ad}^0 \bar{\rho})_{-2L_1}$ and ζ_2 is unramified at v_i, we have that $(\mathrm{Id} + ph(\tau_{v_i}))\zeta_2(\tau_{v_i}) \in \mathrm{U}_{-2L_1}$. Therefore, there are (not necessarily unique) matrices C_i such that if $h(\sigma_{v_i}) = C_i$, we will have $(\mathrm{Id} + ph)\zeta_{2\restriction \mathrm{G}_{v_i}} \in \mathcal{C}_{v_i}$ for $i = 1, 2$. The values $h^{(v_i)}(\sigma_{v_j})$ are represented in the table below:

	σ_{v_1}	σ_{v_2}
$h^{(v_1)}$	A	R
$h^{(v_2)}$	E	$A.$

We need $E = (A + C_1)/2$ and $R = 2A - C_2$. For $v \in \mathfrak{l}_1$, let $\delta^{(v)} \in H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}^*)$ be the cohomology class given by $\delta^{(v)}(\sigma_v) = X^*_{-2L_1}$ and $\delta^{(v)}(\tau_v) = 0$. Let x be the element that occurs most frequently among the elements $\mathrm{inv}_v(\delta^{(v)} \cup h^{(v)})$ among primes v of $\mathfrak{l}_1$. Set

$$\mathfrak{l}_2 = \{v \in \mathfrak{l}_1 \mid \mathrm{inv}_v(\delta^{(v)} \cup h^{(v)}) = x\},$$

$\mathfrak{l}_2$ has positive upper density. Suppose we first choose $v_1 \in \mathfrak{l}_2$. Recall that $h^{(v_1)}(\tau_{v_1}) \in (\mathrm{Ad}^0 \bar{\rho})_{-2L_1}$. By Lemma 3.3.11, the class $h^{(v_1)}$ has full rank, i.e. $h^{(v_1)}(\mathrm{G}_K) = \mathrm{Ad}^0 \bar{\rho}$. In particular, $2A - C_2$ is contained in $h^{(v_1)}(\mathrm{G}_K)$. Choosing v_2 such that $h^{(v_1)}(\sigma_{v_2}) = 2A - C_2$ is a Chebotarev condition on the splitting of v_2 in $L_{h^{(v_1)}}$. We show that $h^{(v_2)}(\sigma_{v_1})$ is determined by how v_2 splits in the $\bar{\chi}\sigma_{2L_1}$-eigenspace each of the fields in $\mathcal{F}^{(v_1)}$. Since $h^{(v_2)}$ is unramified at v_1, the values $\eta_\lambda^{(v_1)}(\tau_{v_1})$ and $h^{(v_2)}(\sigma_{v_1})$ determine $(\eta_\lambda^{(v_1)} \cup h^{(v_2)})_{\restriction \mathrm{G}_{v_1}}$. Express $h^{(v_2)}(\sigma_{v_1}) = \sum_\lambda a_\lambda X_\lambda + \sum_{i=1}^n a_i H_i$. As $\eta_\lambda^{(v_1)}(\tau_{v_1}) = \zeta X_\lambda^*$, we see that $\mathrm{inv}_{v_1}(\eta_\lambda^{(v_1)} \cup h^{(v_2)})$ determines a_λ. Likewise, $\mathrm{inv}_{v_1}(\eta_i^{(v_1)} \cup h^{(v_2)})$ determines a_i. For $v \in \mathfrak{l}$ and $\lambda \in \Phi$, set $z_\lambda^{(v)}$ to be equal to $\mathrm{inv}_v(\eta_\lambda^{(v)} \cup h^{(v)})$. The global reciprocity law asserts that

$$\sum_{w \in T \cup \{v_1, v_2\}} \mathrm{inv}_w(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) = 0, \text{ and } \sum_{w \in T \cup \{v_1\}} \mathrm{inv}_w(\eta_\lambda^{(v_1)} \cup h^{(v_1)}) = 0.$$

Since $h^{(v_2)}_{\restriction \mathrm{G}_w} = z_w = h^{(v_1)}_{\restriction \mathrm{G}_w}$ for $w \in T$, we deduce that

$$\begin{aligned}
\mathrm{inv}_{v_1}(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) &= -\sum_{w \in T} \mathrm{inv}_w(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) - \mathrm{inv}_{v_2}(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) \\
&= -\sum_{w \in T} \mathrm{inv}_w(\eta_\lambda^{(v_1)} \cup h^{(v_1)}) - \mathrm{inv}_{v_2}(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) \\
&= \mathrm{inv}_{v_1}(\eta_\lambda^{(v_1)} \cup h^{(v_1)}) - \mathrm{inv}_{v_2}(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) \\
&= z_\lambda^{(v_1)} - \mathrm{inv}_{v_2}(\eta_\lambda^{(v_1)} \cup h^{(v_2)}).
\end{aligned}$$

Since $z_\lambda^{(v_1)}$ depends on v_1 which is fixed, the variance of the right hand side of the equation comes from the term $\mathrm{inv}_{v_2}(\eta_\lambda^{(v_1)} \cup h^{(v_2)})$. The specification of $h^{(v_2)}(\sigma_{v_1})$

amounts to the specification of $\mathrm{inv}_{v_1}(\eta_\lambda^{(v_1)} \cup h^{(v_2)})$ for $\lambda \in \Phi$ and $\mathrm{inv}_{v_1}(\eta_i^{(v_1)} \cup h^{(v_2)})$ for $i = 1, \ldots, n$. Set u_λ to be $\eta_\lambda^{(v_1)}(\sigma_{v_2})(X_{-2L_1})$ for $\lambda \in \Phi$ and set u_i to be $\eta_\lambda^{(v_1)}(\sigma_{v_2})(X_{-2L_1})$ for $i = 1, \ldots, n$. Since $h^{(v_2)}(\tau_{v_2})$ is a multiple of X_{-2L_1}, we see that

$$\mathrm{inv}_{v_2}(\eta_\lambda^{(v_1)} \cup h^{(v_2)}) = \mathrm{inv}_{v_2}(u_\lambda \delta^{(v_2)} \cup h^{(v_2)})$$
$$\mathrm{inv}_{v_2}(\eta_i^{(v_1)} \cup h^{(v_2)}) = \mathrm{inv}_{v_2}(u_i \delta^{(v_2)} \cup h^{(v_2)}).$$

Since the pairing is not zero, we can choose u_λ such that $\mathrm{inv}_{v_2}(u_\lambda \delta^{(v_2)} \cup h^{(v_2)})$ takes on any value. As a result, we may choose $\{u_\lambda\}_{\lambda \in \Phi}$ and $\{u_i\}_{i=1,\ldots,n}$ so that $h^{(v_2)}(\sigma_{v_1}) = (A + C_1)/2$. The choices of $\{u_\lambda\}_{\lambda \in \Phi}$ and $\{u_i\}_{i=1,\ldots,n}$ are determined by Chebotarev conditions on the splitting of v_2 in the $\bar{\chi}\sigma_{2L_1}$-eigenspaces of the fields in $\mathcal{F}^{(v_1)}$.

Suppose that for the choice of $v_1 \in \mathfrak{l}_2$, there is a $v_2 \in \mathfrak{l}_2$ for which the required conditions are satisfied:

1. the condition on the splitting of v_2 in $L_{h^{(v_1)}}$ which amounts to specifying $h^{(v_1)}(\sigma_{v_2})$,
2. the condition on the splitting of v_2 in the fields $\mathcal{F}^{(v_1)}$ which amounts to specifying $h^{(v_2)}(\sigma_{v_1})$.

Then we are done. Hence consider the case when there is no choice of $v_2 \in \mathfrak{l}_2$ for which the above conditions are satisfied. Let $\mathfrak{l}_{v_1}$ be the subset of $\mathfrak{l}$ for which $(R, E) \neq (2A - C_2, \frac{(A+C_1)}{2})$ for the choice of v_1. We have thus assumed that $\mathfrak{l}_2 \subseteq \mathfrak{l}_{v_1}$, it follows that the upper density $\delta(\mathfrak{l}_2)$ is less than or equal to the upper density $\delta(\mathfrak{l}_{v_1})$.

Set $\mathcal{E}^{(v_1)}$ to be the composite of the field $L_{h^{(v_1)}}$ with the fields in $\mathcal{F}^{(v_1)}$ and let $\mathfrak{F}_\mathfrak{l}$ be the composite of fields in $\mathcal{F}_\mathfrak{l}$. We show that there is an element $x \in \mathrm{Gal}(\mathcal{E}^{(v_1)} \cdot \mathfrak{F}_\mathfrak{l}/K)$ such that if v_2 is trivial prime such that the Frobenius at v_2 maps to x, then $v_2 \in \mathfrak{l}$ and the conditions on v_2 are satisfied. Said differently, if $\sigma_{v_2} = x$, then $v_2 \in \mathfrak{l}\backslash\mathfrak{l}_{v_1}$. If F_1 is any of the fields in $\mathcal{F}^{(v_1)}$ and F_2 is the composite of the other fields in $\mathcal{F}^{(v_1)} \cup \mathcal{F}_\mathfrak{l}$, Lemma 3.5.6 asserts that $F_1 \cap F_2 \subseteq J_{F_1}$. Lemma 3.5.6 asserts that $L_{h^{(v_1)}}$ is linearly disjoint over L from the composite of all fields in $\mathcal{F}^{(v_1)} \cup \mathcal{F}_\mathfrak{l}$. To construct such an element x, enumerate the fields in $\mathcal{F}^{(v_1)} = \{E_1, \ldots, E_{k-1}\}$ and set $E_k := F_{h^{(v_1)}}$. Set $E_0 := \mathfrak{F}_\mathfrak{l}$ and let $\mathcal{E}_j$ be the composite $E_0 \cdots E_j$, note that $\mathcal{E}_k = \mathcal{E}^{(v_1)} \cdot \mathfrak{F}_\mathfrak{l}$. Consider the filtration

$$\mathcal{E}_k \supset \mathcal{E}_{k-1} \supset \cdots \supset \mathcal{E}_1 \supset \mathcal{E}_0 \supset K.$$

Let $x_0 \in \mathrm{Gal}(\mathcal{E}_0/K)$ be an element defining $\mathfrak{l}$. Note that $\mathrm{Gal}(\mathcal{E}_1/\mathcal{E}_0) \simeq \mathrm{Gal}(E_1/E_1 \cap \mathcal{E}_0)$ and the intersection $E_1 \cap \mathcal{E}_0$ is contained in J_{E_1}. The condition on E_1/K is on the $\bar{\chi}\sigma_{2L_1}$-eigenspace $\mathrm{Gal}(E_1/J_{E_1})$. Hence x_0 lifts to a suitable $x_1 \in \mathrm{Gal}(\mathcal{E}_1/K)$. Repeating the process, we see that x_1 lifts to $x_{k-1} \in \mathrm{Gal}(\mathcal{E}_{k-1}/K)$ such that if $\sigma_{v_2} = x_{k-1}$, then $v_2 \in \mathfrak{l}$ and $h^{(v_2)}(\sigma_{v_1}) = (A + C_1)/2$. Since $E_k \cap \mathcal{E}_{k-1} = K$, it follows that x_{k-1} can be lifted to $x_k \in \mathrm{Gal}(\mathcal{E}_{k-1}/K)$ such that if $\sigma_{v_2} = x$, then all conditions on v_2 are satisfied.

As a result, $\delta(\mathfrak{l}\backslash\mathfrak{l}_{v_1}) \geq \frac{1}{[\mathcal{E}^{(v_1)}\cdot\mathfrak{F}_{\mathfrak{l}}:K]}$, and hence,

$$\delta(\mathfrak{l}_{v_1}) \leq \left(1 - \frac{1}{[\mathcal{E}^{(v_1)}\cdot\mathfrak{F}_{\mathfrak{l}}:K]}\right).$$

For $F \in \mathcal{F}^{(v_1)}$, the Galois group $\mathrm{Gal}(F/K)$ may be identified with a Galois submodule of $\mathrm{Ad}^0\bar{\rho}^*$. Hence $[F:K] \leq q^{\dim(\mathrm{Ad}^0\bar{\rho})}$ for $F \in \mathcal{F}^{(v_1)}$ is a uniform bound independent of v_1. Similar reasoning shows that $[L^{h^{(v_1)}}:L] \leq q^{\dim(\mathrm{Ad}^0\bar{\rho})}$. Setting $N := (\#\Phi + n + 1)\cdot\dim\mathrm{Ad}^0\bar{\rho}$, deduce that

$$\delta(\mathfrak{l}_{v_1}) \leq 1 - q^{-N}[\mathfrak{F}_{\mathfrak{l}}:K]^{-1}.$$

Suppose that there is a sequence of m primes $v_1^{(1)},\dots,v_1^{(m)} \in \mathfrak{l}_2$, such that it is not possible to find a second prime v_2 for any of the primes $v_1^{(j)}$. In other words, $\mathfrak{l}_2 \subseteq \cap_{j=1}^m \mathfrak{l}_{v_1^{(j)}}$. We show that the density of $\cap_{j=1}^m \mathfrak{l}_{v_1^{(j)}}$ approaches zero as m approaches infinity. Since the upper density of $\mathfrak{l}_2$ is positive, we will eventually find a pair (v_1, v_2). For convenience of notation, set $w_j := v_1^{(j)}$ and set $A = \{w_1,\dots,w_m\}$. Fix $1 \leq j \leq m$ and enumerate the fields $\mathcal{F}^{(w_j)} = \{E_1,\dots,E_{k-1}\}$ and set $E_k = F_{h^{(w_j)}}$. Denote by $\mathfrak{E}_j := \mathfrak{F}_{\mathfrak{l}}\cdot\mathcal{E}^{(w_1)}\cdots\mathcal{E}^{(w_j)}$ and let C_j be the subset of $\mathrm{Gal}(\mathfrak{E}_j/K)$ defining the set $\cap_{i=1}^j \mathfrak{l}_{w_i}$. This means that $v_2 \in \cap_{i=1}^j \mathfrak{l}_{w_i}$ if and only if $\sigma_{v_2} \in C_j$. We show that any element $y \in \mathrm{Gal}(\mathfrak{E}_{j-1}/K)$ lifts to an element $\tilde{y} \in \mathrm{Gal}(\mathcal{E}_j/K)$ which is not in C_j. This is shown by filtering $\mathfrak{E}_j/\mathfrak{E}_{j-1}$ by

$$\mathfrak{E}_k = \mathcal{E}_k \supset \mathcal{E}_{k-1} \supset \cdots \mathcal{E}_1 \supset \mathcal{E}_0 = \mathfrak{E}_{j-1},$$

where $\mathcal{E}_j := \mathfrak{E}_{j-1}E_1\cdots E_j$. The argument is identical to that provided before.

As a result,

$$\#C_j \leq ([\mathfrak{E}_j:\mathfrak{E}_{j-1}] - 1)\#C_{j-1}.$$

Therefore,

$$\begin{aligned}\delta(\cap_{i=1}^{j}\mathfrak{l}_{w_i}) = \frac{\#C_j}{[\mathfrak{E}_j : K]} \leq & \left(1 - \frac{1}{[\mathfrak{E}_j : \mathfrak{E}_{j-1}]}\right)\frac{\#C_{j-1}}{[\mathfrak{E}_{j-1} : K]}, \\ \leq & \left(1 - \frac{1}{[\mathcal{E}^{(w_j)} : K]}\right)\frac{\#C_{j-1}}{[\mathfrak{E}_{j-1} : K]}, \\ \leq & (1 - q^{-N})\delta(\cap_{i=1}^{j-1}\mathfrak{l}_{w_i}).\end{aligned}$$

Therefore, $\delta(\cap_{i=1}^{m}\mathfrak{l}_{w_i}) \leq (1 - q^{-N})^{m-1}(1 - q^{-N}[\mathfrak{F}_{\mathfrak{l}} : K]^{-1})$. Since $\mathfrak{l}_2$ has positive upper density there is a large value of m such that $\mathfrak{l}_2$ is not contained in $\cap_{i=1}^{m}\mathfrak{l}_{w_i}$. This shows that a pair (v_1, v_2) satisfying the required conditions does exist. □

Proposition 3.5.9. *For ρ_2 has as in Proposition 3.5.8. Identify $\mathrm{Gal}(K(\rho_2)/K)$ with a subset of $\mathrm{Ad}^0\,\bar{\rho}$. The class z_{v_1} may be chosen so that the $-2L_1$-component of $\rho_2(\sigma_{v_1}) - \mathrm{Id} \in \mathrm{Ad}^0\,\bar{\rho}$ is non-zero. For such a choice of z_{v_1}, $\mathrm{Gal}(K(\rho_2)/K) = \mathrm{Ad}^0\,\bar{\rho}$.*

Proof. Recall that since v is a trivial prime, $\bar{\rho}(\sigma_v) = \mathrm{Id}$. Replacing z_{v_1} by $z_{v_1} + a$ for some class $a \in \mathcal{N}_{v_1}$ if necessary, one produces an element for which $\rho_2(\sigma_v) - \mathrm{Id}$ has non-zero $-2L_1$-component. From Lemma 3.3.11, it may deduced that $\mathrm{Gal}(K(\rho_2)/K) = \mathrm{Ad}^0\,\bar{\rho}$. □

3.6 Annihiliating the dual-Selmer Group

Let $\rho_3 : \mathrm{G}_{\mathbb{Q},T\cup\{v_1,v_2\}} \to \mathrm{GSp}_{2n}(\mathrm{W}(\mathbb{F}_q)/p^3)$ be the lift of $\bar{\rho}$ obtained from the application of Propositions 3.5.8 and 3.5.9. Recall that the Galois group $\mathrm{Gal}(K(\rho_2)/K)$ is identified with $\mathrm{Ad}^0\,\bar{\rho}$. As a result, once it is shown that ρ_3 lifts to a characteristic zero representation ρ, it shall follow that ρ is irreducible. In showing that ρ_3 can be lifted to characteristic zero, we enlarge the set of primes $Z = T \cup \{v_1, v_2\}$ to a finite set of primes Y such that $X := Y \backslash S$ consists only of trivial primes. For $i = 1, 2$ set $\mathcal{C}_{v_i} = \mathcal{C}_{v_i}^{ram}$ and for primes $v \in X \backslash \{v_1, v_2\}$, set $\mathcal{C}_v = \mathcal{C}_v^{nr}$. We show that the dual-Selmer group $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*)$ vanishes for a suitably chosen set of primes Y. For convenience of notation, denote by $\mathcal{W}$ the Galois submodule $(\mathrm{Ad}^0 \bar{\rho})_{-2n+2}$ of $\mathrm{Ad}^0 \bar{\rho}$ spanned by root spaces $(\mathrm{Ad}^0 \bar{\rho})_\beta$ for $\beta \neq -2L_1$.

Proposition 3.6.1. *Let $\rho_3 : \mathrm{G}_{\mathbb{Q},T\cup\{v_1,v_2\}} \to \mathrm{GSp}_{2n}(W(\mathbb{F}_q)/p^3)$ be the lift of $\bar{\rho}$ obtained from the application of Propositions 3.5.8 and 3.5.9. Let Y be a finite set of primes which contains $Z = T \cup \{v_1, v_2\}$ such that $Y \backslash S$ consists of trivial primes. Suppose $f \in H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho})$ and $\psi \in H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*)$ are nonzero classes. Then there exists a prime $v \notin Y$ such that*

1. *v is a trivial prime,*
2. $(\mathrm{Id} + X_{-2L_1})^{-1} \rho_2(\sigma_v)(\mathrm{Id} + X_{-2L_1}) \in \mathcal{T} \cdot Z(\mathrm{U}_{2L_1})$.
3. *$f \notin \mathcal{N}_v$.*
4. *$\beta_{\restriction \mathrm{G}_v} = 0$ for all $\beta \in H^1(\mathrm{G}_{\mathbb{Q},Y}, \mathcal{W}^*)$.*
5. *$\psi_{\restriction \mathrm{G}_v} \neq 0$ and one can extend $\{\psi\}$ to a basis $\psi_1 = \psi, \psi_2, \ldots, \psi_k$ of $H^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*)$ such that $\psi_{i \restriction \mathrm{G}_v} = 0$ for $i > 1$.*

Proof. Each condition is a union of Chebotarev conditions on a number of finite extensions J of K. Each of the extensions J are Galois over $\mathbb{Q}$ with $\mathrm{Gal}(J/K)$ an $\mathbb{F}_p$-vector space. Let $g \in G'$ and $x \in \mathrm{Gal}(J/K)$, define, $g \cdot x := \tilde{g} x \tilde{g}^{-1}$ where $\tilde{g}$ is a lift of g to $\mathrm{Gal}(J/\mathbb{Q})$. This gives $\mathrm{Gal}(J/K)$ the structure of an $\mathbb{F}_p[G']$-module. For each condition, we list the choices for J below as well as characters for the $\mathbb{T}$-action on $\mathrm{Gal}(J/K)$:

Condition	J	Eigenspaces of $\mathrm{Gal}(J/K)$
(1)	$K(\mu_{p^2})$	1
(2)	$K(\rho_2)$	$1, \{\sigma_\lambda\}_{\lambda\in\Phi}$
(3)	K_f	$1, \{\sigma_\lambda\}_{\lambda\in\Phi}$
(4)	K_β for $\beta \in H^1(\mathrm{G}_{\mathbb{Q},Y}, \mathcal{W}^*)$	$\bar{\chi}, \{\bar{\chi}\sigma_\lambda^{-1} \mid \lambda \neq -2L_1\}$
(5)	K_{ψ_i}	$\bar{\chi}, \{\bar{\chi}\sigma_\lambda^{-1}\}$.

We show that these conditions may be simultaneously satisfied. First, we show that each of the conditions are nonempty Chebotarev conditions (or a union of finitely many Chebotarev conditions). It is clear that conditions (1) and (2) are Chebotarev conditions. Condition (3) is the complement of a Chebotarev condition and hence a union of finitely many Chebotarev conditions. Condition (4) requires that the prime splits in the composite of the fields K_β. That condition (5) is a nonempty Chebotarev condition follows from Proposition 3.5.4.

Next we examine the independence of these conditions. It follows from Lemma 3.3.16 that the composite of the fields defining the first three conditions is linearly disjoint over K from the composite of the fields defining the last two conditions. As a result, the conditions may be treated separately from the last two. It follows from Proposition 3.5.4 that the conditions (4) and (5) are compatible with each other. Therefore, it remains to show that (1),(2) and (3) may be simultaneously satisfied. We begin with the independence of (1) and (2). Proposition 3.5.9 asserts that $\mathrm{Gal}(K(\rho_2)/K) = \mathrm{Ad}^0\,\bar{\rho}$. Suppose that Q is a proper G'-stable subgroup of $\mathrm{Ad}^0\,\bar{\rho}$. Lemma 3.3.2 asserts that Q decomposes into $\mathbb{T}$-eigenspaces $Q = \bigoplus_{\lambda\in\Phi\cup\{1\}} Q_{\sigma_\lambda}$ and Lemma 3.3.11 asserts that the eigenspace $Q_{-2L_1} := Q_{\sigma_{-2L_1}}$ must be trivial. Hence the quotient $\mathrm{Ad}^0\,\bar{\rho}/Q$ must have a non-zero σ_{-2L_1}-eigenspace. It follows that there is no proper Galois stable subgroup Q of $\mathrm{Ad}^0\,\bar{\rho}$ such that $\mathrm{Ad}^0\,\bar{\rho}/Q$ is has trivial Galois action. Since G' acts trivially on $\mathrm{Gal}(K(\mu_{p^2})/K)$ it follows that $K(\rho_2)\cap K(\mu_{p^2}) = K$. Thus conditions (1) and (2) are independent.

We show that the first three conditions may be simultaneously satisfied by considering the cases $K(\rho_2) \supseteq K_f$ and $K(\rho_2) \not\supseteq K_f$ separately. First consider the case when $K(\rho_2) \supseteq K_f$. Let $r := \dim_{\mathbb{F}_p} f(\mathrm{G}_K)$. Since $\mathrm{Gal}(K(\rho_2)/K) \simeq \mathrm{Ad}^0\,\bar{\rho}$, if $r < \dim_{\mathbb{F}_p} \mathrm{Ad}^0\,\bar{\rho}$ the containment $K(\rho_2) \supset K_f$ is proper. Since f is non-zero, Lemma 3.3.8 asserts that $K_f \neq K$. Let $Q \subset \mathrm{Gal}(K(\rho_2)/K)$ be the proper subgroup such that $\mathrm{Gal}(K(\rho_2)/K)/Q \simeq \mathrm{Gal}(K_f/K)$. Lemma 3.3.2 asserts that Q decomposes into $\mathbb{T}$-eigenspaces $Q = \bigoplus_{\lambda\in\Phi\cup\{1\}} Q_{\sigma_\lambda}$ and Lemma 3.3.11 asserts that the eigenspace $Q_{-2L_1} := Q_{\sigma_{-2L_1}}$ must be trivial. Hence the quotient $\mathrm{Gal}(K_f/K)$ must have a non-zero σ_{-2L_1}-eigenspace. Identify $\mathrm{Gal}(K_f/K)$ with $f(\mathrm{G}_K) \subset \mathrm{Ad}^0\,\bar{\rho}$. Since $r < \dim_{\mathbb{F}_p} \mathrm{Ad}^0\,\bar{\rho}$, Lemma 3.3.11 asserts that $f(\mathrm{G}_K)_{-2L_1} = 0$, a contradiction. Hence, $K(\rho_2) \supseteq K_f$ forces equality $K(\rho_2) = K_f$. Let

$$\alpha_1 := f_{\restriction \mathrm{G}_K} : \mathrm{Gal}(K_f/K) \xrightarrow{\sim} \mathrm{Ad}^0\,\bar{\rho}$$

and

$$\alpha_2 := \rho_{2\restriction \mathrm{G}_K} : \mathrm{Gal}(K_f/K) \xrightarrow{\sim} \mathrm{Ad}^0\,\bar{\rho}.$$

The composite $\alpha_1\alpha_2^{-1}$ is a G'-automorphism of $\mathrm{Ad}^0\,\bar{\rho}$. It follows from Corollary 3.3.10 that $\alpha_1\alpha_2^{-1}$ is a scalar $a \in \mathbb{F}_q^\times$ and hence $\alpha_1 - a\alpha_2 = 0$. Note that it need not be the case that $\mathrm{Gal}(K_f/K)$ is an $\mathbb{F}_q[G']$-module, it is only asserted that there exists $a \in \mathbb{F}_q^\times$ such that $\alpha_1\alpha_2^{-1} = a$. Let v satisfy (1), (2), (4) and (5) such that

$$(\mathrm{Id} + X_{-2L_1})^{-1}\rho_2(\sigma_v)(\mathrm{Id} + X_{-2L_1}) \in \mathcal{T}$$

has non-trivial H_1 component. Since v is a trivial prime, σ_v lies in G_K. Identifying $\ker\{\mathrm{GSp}(\mathrm{W}(\mathbb{F}_q)/p^2) \to \mathrm{GSp}(\mathbb{F}_q)\}$ with $\mathrm{Ad}^0\,\bar{\rho}$, we view $\rho_2(\sigma_v)$ as an element in $\mathrm{Ad}^0\,\bar{\rho}$. Since $f(\sigma_v) = a\rho_2(\sigma_v)$, we see that $(\mathrm{Id} + X_{-2L_1})^{-1}f(\sigma_v)(\mathrm{Id} + X_{-2L_1})$ has non-zero H_1 component and hence is not contained in $\mathfrak{t}_{2L_1} + \mathrm{Cent}((\mathrm{Ad}^0\,\bar{\rho})_{2L_1})$. As a result, f is not in $(\mathrm{Id} + X_{-2L_1})\mathcal{P}_v^{2L_1}(\mathrm{Id} + X_{-2L_1})^{-1}$. It is easy to see that f is not in $\mathcal{N}_v$ and hence (3) is also satisfied.

We consider the case when $K_f \not\subseteq K(\rho_2)$. Since

$$[K(\rho_2) : K] = \#\,\mathrm{Ad}^0\,\bar{\rho} \geq [K_f : K],$$

$K(\rho_2)$ is not contained in K_f. It follows that $K(\rho_2) \supsetneq K(\rho_2) \cap K_f$ and $K_f \supsetneq K(\rho_2) \cap K_f$ and thus by Lemma 3.3.3, the images of

$$\mathrm{Gal}(K(\rho_2)/K(\rho_2) \cap K_f) \hookrightarrow \mathrm{Ad}^0\,\bar{\rho} \text{ and } \mathrm{Gal}(K_f/K(\rho_2) \cap K_f) \hookrightarrow \mathrm{Ad}^0\,\bar{\rho}$$

contain $(\mathrm{Ad}^0\,\bar{\rho})_{\sigma_{2L_1}}$. If $K_f \subseteq K(\rho_2, \mu_{p^2})$, then it follows that

$$\dim_{\mathbb{F}_p}(\mathrm{Gal}(K(\rho_2, \mu_{p^2})/K)_{\sigma_{2L_1}}) \geq 2\dim_{\mathbb{F}_p}(\mathrm{Ad}^0\,\bar{\rho})_{\sigma_{2L_1}} = 2[\mathbb{F}_q : \mathbb{F}_p].$$

However, $\mathrm{Gal}(K(\rho_2, \mu_{p^2})/K)_{\sigma_{2L_1}}$ may be identified with

$$\mathrm{Gal}(K(\rho_2)/K)_{\sigma_{2L_1}} \simeq (\mathrm{Ad}^0 \bar{\rho})_{\sigma_{2L_1}}$$

since $K(\mu_{p^2})$ contributes to the trivial eigenspace. Hence, $K_f \not\subseteq K(\rho_2, \mu_{p^2})$. Let v be a prime satisfying conditions (1), (2), (4) and (5). Lemma 3.3.3 asserts that the image of

$$\mathrm{Gal}(K_f/K_f \cap K(\rho_2, \mu_{p^2})) \hookrightarrow \mathrm{Ad}^0 \bar{\rho}$$

contains $(\mathrm{Ad}^0 \bar{\rho})_{\sigma_{2L_1}}$ and thus, we have the freedom to stipulate that the X_{2L_1}-component of $f(\sigma_v)$ be anything we like. By Lemma 3.4.5, it follows that we may alter the X_{2L_1}-component of $f(\sigma_v)$ so that $f \notin \mathcal{N}_v$. Therefore all conditions may be satisfied and the proof is complete. $\square$

Proposition 3.6.2. *There is a finite set $Y \supseteq Z$ such that $Y \backslash S$ consists of trivial primes and $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*) = 0$.*

Proof. Let Y be a finite set of primes containing Z such that $Y \backslash S$ consists of trivial primes. If $H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) \neq 0$, we exhibit a trivial prime v not contained in Y such that

$$h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) < h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}).$$

Therefore, on adjoining a finite set of trivial primes to obtain the set Y such that $Y \backslash S$ consists of trivial primes and the Selmer group $H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) = 0$. Since

$$h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) = h^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*),$$

the dual Selmer group does also vanish.

Let $v \notin Y$ be trivial prime which satisfies the conditions of Proposition 3.6.1. Let $\mathcal{M}$ be the Selmer condition

$$\mathcal{M}_w := \begin{cases} \mathcal{N}_w \text{ if } w \in Y \\ H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}) \text{ if } w = v \\ H^1_{nr}(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho}) \text{ if } w \notin Y \cup \{v\} \end{cases}.$$

Let ψ be the non-zero class as in Proposition 3.6.1. Note that $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*)$ contains $H^1_{\mathcal{M}^\perp}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}^*)$ and since $\psi_{\restriction \mathrm{G}_v} \neq 0$, the element $\psi \in H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*)$, but $\psi \notin H^1_{\mathcal{M}^\perp}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}^*)$. In particular, we have that

$$h^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*) > h^1_{\mathcal{M}^\perp}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}^*). \tag{3.9}$$

By Proposition 3.6.1 condition 4 the maps

$$\Phi_1 : H^1(\mathrm{G}_{\mathbb{Q},Y}, \mathcal{W}) \to \bigoplus_{w\in Y} H^1(\mathrm{G}_w, \mathcal{W})$$

and

$$\Phi_2 : H^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathcal{W}) \to \bigoplus_{w\in Y} H^1(\mathrm{G}_w, \mathcal{W})$$

have the same image, consequently,

$$\begin{aligned} \dim\ker\Phi_2 - \dim\ker\Phi_1 &= h^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathcal{W}) - h^1(\mathrm{G}_{\mathbb{Q},Y}, \mathcal{W}) \\ &= h^1(\mathrm{G}_v, \mathcal{W}) - h^0(\mathrm{G}_v, \mathcal{W}) \\ &= h^2(\mathrm{G}_v, \mathcal{W}) \\ &= \dim \mathcal{W} \\ &= h^1(\mathrm{G}_v, \mathcal{W}) - h^1_{nr}(\mathrm{G}_v, \mathcal{W}). \end{aligned} \tag{3.10}$$

By 3.10, we deduce that the sequence

$$0 \to \ker \Phi_1 \to \ker \Phi_2 \to \frac{H^1(\mathrm{G}_v, \mathcal{W})}{H^1_{nr}(\mathrm{G}_v, \mathcal{W})} \to 0 \tag{3.11}$$

is a short exact sequence.

Define the maps

$$\Phi_3 : H^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) \to \bigoplus_{w\in Y} \frac{H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_w}$$

and

$$\Phi_4 : H^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) \to \bigoplus_{w\in Y} \frac{H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_w}.$$

From the Cassels-Poitou-Tate long exact sequence and the vanishing of $Ш^2_Y(\mathrm{Ad}^0 \bar{\rho})$, we deduce that the following sequences are exact

$$H^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) \xrightarrow{\Phi_3} \bigoplus_{w\in Y} \frac{H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_w} \to H^1_{\mathcal{M}^\perp}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}^*) \to 0$$

$$H^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) \xrightarrow{\Phi_4} \bigoplus_{w\in Y} \frac{H^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_w} \to H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}^*) \to 0.$$

From the assertion made in 3.9 we conclude that the difference in the dimensions of images

$$t' := \dim \mathbf{im}\Phi_3 - \dim \mathbf{im}\Phi_4 \geq 1. \tag{3.12}$$

We claim that it suffices to find $\dim \mathrm{Ad}^0 \bar{\rho} - t' + 1$ elements in $\ker \Phi_3$, no linear combination of which lies in $\mathcal{N}_v$. It follows then that the image of

$$\ker \Phi_3 \to \frac{H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_v}$$

has dimension strictly greater than $\dim \mathrm{Ad}^0 \bar{\rho} - t'$. From the exactness of

$$0 \to H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) \to \ker \Phi_3 \to \frac{H^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho})}{\mathcal{N}_v}$$

one may deduce that

$$\begin{aligned} h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) &< \dim \ker \Phi_3 - \dim \mathrm{Ad}^0 \bar{\rho} + t'. \\ &= h^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) - \dim \mathrm{Ad}^0 \bar{\rho} - \dim \mathrm{im}\, \Phi_4. \end{aligned}$$

Note that $\text{Ш}^1_Y(\mathrm{Ad}^0 \bar{\rho}) = 0$ and thus an application of Wiles' formula (3.2) shows that

$$h^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) = \sum_{w\in Y} (h^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho}) - h^0(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho}))$$

and

$$h^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) = \sum_{w\in Y\cup\{v\}} (h^1(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho}) - h^0(\mathrm{G}_w, \mathrm{Ad}^0 \bar{\rho})).$$

Therefore,

$$\begin{aligned} h^1(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) &= h^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) + h^1(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}) - h^0(\mathrm{G}_v, \mathrm{Ad}^0 \bar{\rho}) \\ &= h^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) + \dim \mathrm{Ad}^0 \bar{\rho}. \end{aligned}$$

Therefore, we have that

$$\begin{aligned} h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y\cup\{v\}}, \mathrm{Ad}^0 \bar{\rho}) &< h^1(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}) - \dim \mathrm{im}\, \Phi_4 \\ &= \dim \ker \Phi_4 \\ &= h^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Y}, \mathrm{Ad}^0 \bar{\rho}). \end{aligned}$$

Therefore in order to complete the proof we proceed to construct $\dim \mathrm{Ad}^0 \bar{\rho} - t' + 1$ elements in $\ker \Phi_3$ no linear combination of which lies in $\mathcal{N}_v$. We are in fact able to construct $\dim \mathrm{Ad}^0 \bar{\rho}$ elements, which suffices since $t' \geq 1$.

Let $Z_1, \ldots, Z_s$ be a basis of $\mathcal{W}$. We observe that $\ker\Phi_2 \subseteq \ker\Phi_3$. By the exactness of 3.11 there exist $\omega_i \in \ker\Phi_2$ such that $\omega_i(\tau_v) = Z_i$ for $i = 1, \ldots, s$. We show that no linear combination of $\{f, \omega_1, \ldots, \omega_s\}$ lies in $\mathcal{N}_v$. Let $Q = c_0 f + \sum_{i=1}^s c_i\omega_i \in \mathcal{N}_v$. Since f is unramified at v, $f(\tau_v) = 0$. On the other hand, $Q(\tau_v) = \sum_{i=1}^s c_i Z_i \in \mathcal{W}$. Since $Q \in \mathcal{N}_v$,

$$Q(\tau_v) = c(\mathrm{Id} + X_{-\alpha})X_\alpha(\mathrm{Id} + X_{-\alpha})^{-1}$$

for $\alpha = 2L_1$ and some constant c. The root vectors X_α and $X_{-\alpha}$ are constant multiples of $e_{1,n+1}$ and $e_{n+1,1}$ respectively. Assume WLOG that $X_\alpha = e_{1,n+1}$ and $X_{-\alpha} = e_{n+1,1}$. Clearly, $X_{-\alpha}^2 = 0$ and hence $(1 + X_{-\alpha})^{-1} = (1 - X_{-\alpha})$. We see that

$$\begin{aligned} Q(\tau_v) =& c(\mathrm{Id} + X_{-\alpha})X_\alpha(\mathrm{Id} - X_{-\alpha}) \\ =& c\left(X_\alpha + [X_{-\alpha}, X_\alpha] - X_{-\alpha}X_\alpha X_{-\alpha}\right) \\ =& c\left(e_{1,n+1} - H_1 - e_{n+1,1}\right). \end{aligned}$$

We deduce that $Q(\tau_v) = 0$ since $e_{n+1,1} \notin \mathcal{W}$. Therefore, $c_i = 0$ for all $i = 1, \ldots, s$. As a consequence, $Q = c_0 f$. However, $f \notin \mathcal{N}_v$. It follows that $c_0 = 0$ and therefore, $Q = 0$. Therefore no linear combination of $\{f, \omega_1, \ldots, \omega_s\}$ lies in $\mathcal{N}_v$ and this completes the proof. □

To conclude the proof of Theorem 3.0.1, we observe that on choosing an appropriately large choice of trivial primes the dual Selmer group vanishes and hence ρ_3 lifts to a characteristic zero representation ρ with similitude character κ. Furthermore, ρ satisfies the local conditions $\mathcal{C}_v$ at the primes $v \in S$. Since the image of ρ_2 contains

$$\widehat{\mathrm{GSp}}_{2n}(\mathrm{W}(\mathbb{F}_q)/p^2) := \left\{\mathrm{GSp}_{2n}(\mathrm{W}(\mathbb{F}_q)/p^2) \to \mathrm{GSp}_{2n}(\mathbb{F}_q)\right\}$$

it follows that ρ is irreducible.

CHAPTER 4

LIFTING REDUCIBLE GALOIS REPRESENTATIONS TO HIDA FAMILIES

4.1 Introduction

Let p be an odd prime and q a power of p and $\mathbb{F}_q$ denote the finite field of order q. Recall that $\mathcal{O}$ denotes the ring of Witt vectors $\mathrm{W}(\mathbb{F}_q)$. As in the last chapter, let χ denote the p-adic cyclotomic character. Let f be a Hecke eigencuspform with weight $k \geq 2$ which is p-ordinary. In other words, if ρ_f is the p-adic Galois representation associated to f,

$$\rho_{f\restriction I_p} \simeq \begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

Hida showed that f may be p-adically interpolated into a family of eigencuspforms, all ordinary at p. Such a family is called the Hida-family of f. The character χ induces an isomorphism

$$\chi : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times.$$

Let $\mathbb{Q}^{cyc}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. It is the subfield of $\mathbb{Q}(\mu_{p^\infty})$ fixed by $\mu_{p-1} \subset \mathbb{Z}_p^\times$. Let $\mathcal{O}'$ be the valuation ring of a finite extension of $\mathbb{Q}_p$. The Iwasawa algebra $\Lambda_{\mathcal{O}'}$ is defined as the completed group algebra

$$\Lambda_{\mathcal{O}'} = \varprojlim_L \mathcal{O}'[\mathrm{Gal}(L/\mathbb{Q})]$$

where the inverse limit runs over all finite extensions of $\mathbb{Q}$ contained in $\mathbb{Q}^{cyc}$.

Let $N \geq 1$ be coprime to p. More precisely, Hida family refers of tame level N refers to an *irreducible component* $\mathbb{T}$ of the Hecke algebra of tame level N, localized at a maximal ideal, with its induced algebra structure over the Iwasawa algebra. Attached to the p-ordinary cusp form f is its Galois representation

$$\rho_f : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p).$$

The Hida-family is a Galois representation

$$\rho_{\mathcal{T}} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}).$$

The eigenform f coincides with a point $\operatorname{Spec} \bar{\mathbb{Z}}_p \to \operatorname{Spec} \mathbb{T}$ over the special point. The Galois representation ρ_f is induced from $\rho_{\mathcal{T}}$.

Fix an odd Galois representation $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_q)$ which is reducible and indecomposable. Recall that by Theorem $1.2.3$, if $\bar{\rho}$ satisfies favorable conditions there is a finite set of auxiliary primes X disjoint from S such that $\bar{\rho}$ lifts to a p-adic Galois representation ρ which is unramified outside $S \cup X$. Moreover, ρ arises from a p-ordinary Hecke eigencuspform. There has been some interest in adapting such Galois theoretic constructions to interpolate such lifts in p-adic families of ordinary Galois representations (cf. [26]). When $\bar{\rho}$ is absolutely irreducible, these families coincide with universal deformation rings which represent functors of Galois deformations with prescribed local conditions. However, in the residually reducible case, since the local deformation problems at the auxiliary primes X are not representable, there is no direct analog of a Galois deformation problem which is representable by a Hida family. In this manuscript, adaptations are made to this functor of global deformations so that there is a Hida line of Galois deformations of $\bar{\rho}$ which is the hull. Classical weight points on this line coincide with Hecke eigencuspforms. This Hida-line interpolates a large family of weights.

Let $\mathbb{Q}^{cyc}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let $\Gamma = \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q})$. The Iwasawa-algebra $\Lambda := \Lambda_{\mathcal{O}}$. On fixing an isomorphism $\Gamma \simeq \mathbb{Z}_p$, the Iwasawa algebra Λ may be identified with the power-series ring

$$\Lambda = \mathcal{O}[[T]].$$

In [26] it is shown that if $\bar{\rho}$ is absolutely irreducible, a finite set of auxiliary primes X disjoint from S (called nice primes) may be chosen such that there is a Galois deformation $\tilde{\varrho} : \mathrm{G}_{\mathbb{Q},S\cup X} \to \mathrm{GL}_2(\Lambda)$ which is the universal deformation of $\bar{\rho}$ subject to local conditions at the primes in $S \cup X$. In particular, for each classical weight $k \geq 2$ there is exactly one Galois representation in the family arising from an eigencuspform of weight k. The existence of a universal Hida line has various applications in Galois deformation theory. We list two.

1. In [12], it was shown that if $\mathcal{O}'$ is a p-adic ring with uniformizer π and

$$\rho_n : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}'/\pi^n)$$

is a residually irreducible and odd torsion Galois representation satisfying appropriate conditions, then indeed ρ_n lifts to a Galois representation arising from an eigencuspform. The construction uses the existence of a special Hida family of lifts isomorphic to Λ. It is natural to ask if such results do extend to the residually reducible case.

2. Level lowering constructions are being implemented for certain general classes of residually irreducible p-ordinary Galois representations [24]. In furture work with Ravi Ramakrishna, conditional level lowering results for residually reducible Galois representations shall be obtained. The techniques used in this chapter motivate some level lowering constructions in the residually reducible case.

Let $\mathfrak{C}$ denote the full-subcategory of finite length coefficient rings R over $\mathcal{O}$ with maximal ideal $\mathfrak{m}_R$ for which $p \notin \mathfrak{m}_R^2$.

Theorem 4.1.1. *Let S be a finite set of primes containing p and $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_q)$ be a two-dimensional Galois representation given by $\bar{\rho} = \begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix}$. Let c denote complex-conjugation. Suppose further that*

1. *the characteristic $p \geq 3$,*
2. *the representation $\bar{\rho}$ is indecomposable,*
3. *$\bar{\rho}$ is odd, i.e. $det\bar{\rho}(c) = -1$, where c denotes complex conjugation,*
4. *the character $\varphi_{\restriction I_p} = \chi_{\restriction I_p}^{k-1}$ where $2 \leq k \leq p-1$,*
5. *$\varphi_{\restriction \mathrm{G}_p} \notin \{\bar{\chi}_{\restriction \mathrm{G}_p}, \bar{\chi}_{\restriction \mathrm{G}_p}^{-1}, 1\}$,*
6. *the $\mathbb{F}_p$-span of the image of φ is (the entirety of) $\mathbb{F}_q$.*

On enlarging the set of primes S we may examine a certain global deformation problem associated with $\bar{\rho}$. There exists an auxiliary finite set of primes X disjoint from S such that for the following choices of local deformation conditions, for

1. *the primes $v \in X$ are chosen to be the trivial primes of [9] and $\tilde{\mathcal{C}}_v$ is the versal local deformation condition (made explicit in Definition 4.3.2),*

2. *for $v \in S \backslash \{p\}$ the minimal deformation condition in [23] is prescribed,*

3. *the deformation condition $\tilde{\mathcal{C}}_p$ is the ordinary arbitrary weight deformation condition.*

For the choice $\Phi := \{\tilde{\mathcal{C}}_v\}_{v \in Z \cup X}$ the functor of deformations $\mathcal{D}ef_\Phi$ (cf. Definition 4.4.2) has a hull isomorphic to (a rank 2 representation valued in) $\mathcal{O}[[U]]$. There is a deformation

$$\begin{array}{ccccc} & & & & \mathrm{GL}_2(\mathcal{O}[[U]]) \\ & & \overset{\tilde{\varrho}}{\nearrow} & & \downarrow \\ \mathrm{G}_{\mathbb{Q},S\cup X} & \longrightarrow & \mathrm{G}_{\mathbb{Q},S} & \xrightarrow{\bar{\rho}} & \mathrm{GL}_2(\mathbb{F}_q). \end{array}$$

for which $\tilde{\varrho} \in \mathcal{D}ef_\Phi(\mathcal{O}[[U]])$ and such that for $R \in \mathfrak{C}$, the induced map

$$\tilde{\varrho}^* : \mathrm{Hom}(\mathcal{O}[[U]], R) \to \mathcal{D}ef_\Phi(R)$$

is surjective.

Theorem 4.1.2. *Let R be a coefficient ring in $\mathfrak{C}$ with maximal ideal $\mathfrak{m}_R$. In the context of Theorem 4.1.1, the functor of points of the map to weight space induces on R-points a map*

$$\mathcal{W}t^* : \mathcal{D}ef_\Phi(R) \to \mathrm{Hom}_{\mathfrak{C}}(\Lambda, R)$$

whose image consists weights in the mod $(pR) \cap \mathfrak{m}_R^2$ congruence class of weights which coincide with the weight of the chosen lift ρ_2 modulo $(pR) \cap \mathfrak{m}_R^2$.

Remark 4.1.3. *Theorem* 4.1.2 *implies in particular that on* $\mathcal{O}$*-points, the image of map*

$$\mathcal{W}t^* : \mathcal{D}ef_{\Phi}(\mathcal{O}) \to \mathrm{Hom}_{\mathfrak{C}}(\Lambda, \mathcal{O})$$

is a congruence class of weights modulo p^2.

4.2 The Setup

Let $\bar{\rho} : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_q)$ be such that it satisfies the conditions of Theorem 4.1.1. Recall that k is chosen such that

$$\bar{\rho}_{\restriction I_p} = \begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix}$$

and that $2 \leq k \leq p-1$. In this section we describe some of the local deformation conditions at primes $v \in S$. Recall that $\mathcal{C}_{\mathcal{O}}$ denotes the category of Noetherian coefficient-algebras over $\mathcal{O}$. Let $\mathcal{C}^f = \mathcal{C}^f_{\mathcal{O}}$ be the category of finite-length coefficient-algebras and $\mathfrak{C} \subset \mathcal{C}^f$ be the full subcategory consisting of pairs (R, ϕ) such that the square of the maximal ideal $\mathfrak{m}_R$ does not contain p. In particular, $\mathbb{F}_q$ is excluded from $\mathfrak{C}$. We shall often suppress the map ϕ for the ease of notation. Let $\gamma \in \Gamma$ be a choice of topological generator of Γ. For $R \in \mathcal{C}$ and

$$\rho_R : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$$

a deformation of $\bar{\rho}$, the *weight* of ρ_R is the point

$$\mathcal{W}t(\rho_R) : \mathrm{Spec}\, R \to \mathrm{Spec}\, \Lambda$$

induced by the homomorphism of rings mapping T to $\det \rho_R(\gamma) - 1$.

Deformations of $\bar{\rho}$ shall be required to satisfy certain local conditions. At each prime v at which $\bar{\rho}$ is allowed to ramify, there is a suitable choice of a functor of deformations

$$\tilde{\mathcal{C}}_v : \mathcal{C}^f \to \mathrm{Sets}$$

of $\bar{\rho}_{\restriction \mathrm{G}_v}$. Fix a lift $\psi : \mathrm{G}_{\mathbb{Q},S} \to \mathrm{GL}_1(\mathcal{O})$ of the determinant character $\det \bar{\rho}$ and let $\psi_v := \psi_{\restriction \mathrm{G}_v}$. Once $\tilde{\mathcal{C}}_v$ is defined, $\mathcal{C}_v$ shall denote the subfunctor of $\tilde{\mathcal{C}}_v$ consisting of deformations of $\bar{\rho}_{\restriction \mathrm{G}_v}$ with determinant $\psi_{\restriction \mathrm{G}_v}$. The functors $\mathcal{C}_v$ and $\tilde{\mathcal{C}}_v$ are required to be representable by smooth schemes. This is the case when $\mathcal{C}_v$ and $\tilde{\mathcal{C}}_v$ are liftable deformation conditions. Recall that a scheme is smooth if it satisfies the infinitesimal lifting property. A deformation condition is liftable if it behaves like the functor of points on a smooth scheme. Recall that $\mathrm{Ad}\,\bar{\rho}$ denotes the $\mathbb{F}_q$ vector space of 2×2 matrices over $\mathbb{F}_q$ on which $\mathrm{G}_{\mathbb{Q},S}$ acts via the adjoint action. Set $\mathrm{Ad}^0\,\bar{\rho}$ for the $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$ submodule of trace-zero matrices in $\mathrm{Ad}\,\bar{\rho}$. The functor of deformations of $\bar{\rho}_{\restriction \mathrm{G}_v}$ is denoted Def_v. The subfunctor of deformations with determinant ψ_v is denoted by Def'_v. The set of *infinitesimal deformations* $\mathrm{Def}_v(\mathbb{F}_q[\epsilon])$, resp. $\mathrm{Def}'_v(\mathbb{F}_q[\epsilon])$, acquires the structure of an $\mathbb{F}_q$-vector space and there is a canonical isomorphism

$$\mathrm{Def}_v(\mathbb{F}_q[\epsilon]) \xrightarrow{\sim} H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar{\rho}),$$

resp.

$$\mathrm{Def}'_v(\mathbb{F}_q[\epsilon]) \xrightarrow{\sim} H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho}).$$

Let

$$\tilde{\mathcal{N}}_v := \tilde{\mathcal{C}}_v(\mathbb{F}_q[\epsilon]) \subseteq H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar{\rho})$$

and

$$\mathcal{N}_v := \mathcal{C}_v(\mathbb{F}_q[\epsilon]) \subseteq H^1(\mathrm{G}_v, \mathrm{Ad}^0\,\bar{\rho}).$$

If $\mathcal{C}_v$ is a deformation condition, then it is representable by a universal local deformation

$$\varrho_v : \mathrm{G}_v \to \mathrm{GL}_2(R_v).$$

This follows from an application of the Schlessinger criterion. The local deformation ring R_v is a coefficient ring over $W(\mathbb{F}_q)$. Letting $\mathfrak{m}_v$ denote the maximal ideal of R_v, the space $\mathcal{N}_v$ can be identified with the tangent space

$$\mathcal{N}_v \simeq \left(\mathfrak{m}_v/\mathfrak{m}_v^2\right)^*.$$

The following standard fact is noted in [12, Fact 5] and proceeds from the discussion on local deformation conditions in [23].

Fact 4.2.1. *For all $v \in S\backslash\{p\}$, there exists a liftable local deformation condition $\mathcal{C}_v$ of Steinberg-type*

$$\dim \mathcal{N}_v = h^0(G_v, \mathrm{Ad}^0\,\bar{\rho}).$$

On the other hand, $\mathcal{C}_p$ consists of ordinary deformations of fixed determinant. The functor $\mathcal{C}_p$ is also a liftable deformation condition

$$\dim \mathcal{N}_p = h^0(\mathrm{G}_p, \mathrm{Ad}^0\,\bar{\rho}) + 1.$$

For $v \neq p$, let $\tilde{\mathcal{C}}_v$ denote the unramified central twists of $\mathcal{C}_v$.

Along with deformation conditions at the primes $v \in S$, there are are functors $\mathcal{C}_v$ and $\tilde{\mathcal{C}}_v$ defined at an auxiliary set of primes X called trivial primes. These functors are however not representable by schemes. We simply refer to them as deformation problems at trivial primes. They will be introduced in detail in the next section.

Let $R \to R/I$ be a small extension and t a generator of the maximal ideal of R. Let $v \in S$ and $\tilde{\mathcal{C}}_v$ as above. Let $\varrho \in \tilde{\mathcal{C}}_v(R)$ and $\varrho_0 := \varrho \mod I$. The twist of ϱ by a cohomology class $X \in \tilde{\mathcal{N}}_v$ is precribed by

$$\exp(X \otimes t)\varrho := (\mathrm{Id} + Xt)\varrho.$$

Furthermore, the twist is a deformation of ϱ_0. The fibers of ϱ_0 w.r.t the mod I reduction map

$$\tilde{\mathcal{C}}_v(R) \to \tilde{\mathcal{C}}_v(R/I)$$

is an $\tilde{\mathcal{N}}_v$-pseudotorsor. Likewise, the fibers of

$$\mathcal{C}_v(R) \to \mathcal{C}_v(R/I)$$

is an $\mathcal{N}_v$-pseudotorsor. On the other hand, at a trivial prime (at which the deformation problem is versal) a similar description caries over (cf. Proposition 4.3.5).

We motivate the dimension calculations of this section. Let $U \subset \mathrm{Ad}^0 \bar{\rho}$ be the subspace of upper triangular matrices, and $U^0 \subset U$ be the subspace of strictly upper triangular matrices. The spaces $U^0 \subset U$ are Galois submodules of $\mathrm{Ad}^0 \bar{\rho}$. For $v \in S$,

$$\mathcal{N}_v = \ker\{H^1(G_v, U) \to H^1(I_v, U/U^0)\}.$$

In particular, $\mathcal{N}_v$ does not depend on ψ.

Proposition 4.2.2. *[16, Theorem 8.7.9] Suppose M is an $\mathbb{F}_q[\mathrm{G}_{\mathbb{Q},S}]$ module with finite cardinality and Z a finite set of primes which contains S. Let $\mathcal{L}$ be a Selmer condition on $Z \cup \{\infty\}$. The dimensions of the Selmer and dual Selmer groups are related as follows*

$$\begin{aligned} &h^1_{\mathcal{L}}(\mathrm{G}_{\mathbb{Q},Z}, M) - h^1_{\mathcal{L}^\perp}(\mathrm{G}_{\mathbb{Q},Z}, M^*) \\ =&h^0(\mathrm{G}_{\mathbb{Q}}, M) - h^0(\mathrm{G}_{\mathbb{Q}}, M^*) + \sum_{v \in Z \cup \{\infty\}} (\dim \mathcal{L}_v - h^0(G_v, M)). \end{aligned}$$

Denote by $h^1_{\mathcal{N},S}$ and $h^1_{\mathcal{N}^\perp,S}$ the dimension of $H^1(\mathrm{G}_{\mathbb{Q},S}, \mathrm{Ad}^0\,\bar{\rho})$ and $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},S}, \mathrm{Ad}^0\,\bar{\rho}^*)$ respectively. It is a consequence of Proposition 4.2.2 that the Selmer condition $\mathcal{N}$ on S is balanced, i.e.

$$h^1_{\mathcal{N},S} - h^1_{\mathcal{N}^\perp,S} = 0.$$

It is shown in this section that for the Selmer condition $\tilde{\mathcal{N}}$,

$$h^1_{\tilde{\mathcal{N}},S} - h^1_{\tilde{\mathcal{N}}^\perp,S} = 1.$$

In order to motivative the construction of Hamblen and Ramakrishna we emphasize the role of nice primes in the residually irreducible case. In this particular setting, there is a finite set X of auxiliary primes q known as nice primes at which there are liftable deformation conditions $\tilde{\mathcal{C}}_q$. Denote by $R^{X-new}_{S\cup X}$ the universal deformation ring with local conditions $\tilde{\mathcal{C}}_v$ at all primes $v \in S \cup X$. Consider the Selmer condition $\mathcal{N}$ on the set of primes $S \cup X$, where at each prime $q \in S$, the space $\tilde{\mathcal{N}}_q$ is the tangent space to $\tilde{\mathcal{C}}_q$. The set of primes X may be chosen so as to kill the dual Selmer group, i.e such that

$$h^1_{\tilde{\mathcal{N}}^\perp,S\cup X} = 0. \tag{4.1}$$

The relation

$$h^1_{\tilde{\mathcal{N}},S\cup X} - h^1_{\tilde{\mathcal{N}}^{\perp},S\cup X} = 1$$

is satisfied and therefore,

$$h^1_{\tilde{\mathcal{N}},S\cup X} = 1. \tag{4.2}$$

From 4.1 and 4.2, it is shown via formal arguments that the weight space map induces and isomorphism $R^{X-new}_{S\cup X} \simeq \Lambda$; see the proof of [26, Theorem 2].

We return to the reducible case. In the next section, the versal deformation conditions at auxiliary primes (known as trivial primes) is discussed. Such primes v are known as trivial primes, since $\mathrm{G}_v \subset \ker \bar{\rho}$. Hamblen and Ramakrishna show that on stipulating local conditions at a finite set of trivial primes, one may lift $\bar{\rho}$ to a characteristic zero representation arising from a Hecke eigencuspform. As has been mentioned previously, the question of representing the global deformation problem satisfying auxilary conditions cannot be addressed directly since the auxiliary conditions are versal.

One feature of the deformation condition at a trivial prime $v \in X$ is that it comes with amplified and unmodified tangent spaces. We distinguish between *amplified* and *unmodified* tangent spaces and their associated Selmer conditions in the case in which the weight of our deformations remain fixed. The Selmer condition $\mathcal{N} = \{\mathcal{N}_v\}_{v\in S\cup X}$ is called the *amplified* Selmer condition. For $v \in X$, the amplified tangent space $\mathcal{N}_v$ stabilizes $\mathcal{C}_v(W(\mathbb{F}_q)/p^3)$. The dimension of $\mathcal{N}_v$ for $v \in X$ is

$$h^0(G_v, \mathrm{Ad}^0\,\bar{\rho}) = \dim \mathrm{Ad}^0\,\bar{\rho} = 3.$$

It follows from Proposition 4.2.2 that

$$h^1_{\mathcal{N},S\cup X} - h^1_{\mathcal{N}^\perp,S\cup X} = 0.$$

It is shown in Corollory 4.2.7 that

$$h^1_{\tilde{\mathcal{N}},S\cup X} - h^1_{\tilde{\mathcal{N}}^\perp,S\cup X} = 1.$$

To distinguish the amplified tangent condition to one which is not modified, we have what we call the *unmodified* tangent condition $\mathcal{M} = \{\mathcal{M}_v\}_{v\in S\cup X}$. For $v \in S$, set $\mathcal{M}_v = \mathcal{N}_v$ and for $v \in X$, $\mathcal{M}_v \subsetneq \mathcal{N}_v$ preserves $\mathcal{C}_v$. For $v \in X$, the dimension of $\mathcal{M}_v$ is

$$h^0(G_v, \mathrm{Ad}^0\,\bar{\rho}) - 1 = 2.$$

It follows from Proposition 4.2.2 that

$$\begin{aligned}
&h^1_{\mathcal{M}}(\mathrm{G}_{\mathbb{Q},Z}, \mathrm{Ad}^0\,\bar{\rho}) - h^1_{\mathcal{M}^\perp}(\mathrm{G}_{\mathbb{Q},Z}, \mathrm{Ad}^0\,\bar{\rho}^*) \\
&= \sum_{v\in X}(\dim \mathcal{M}_v - h^0(G_v, \mathrm{Ad}^0\,\bar{\rho})) \\
&= - \mid X \mid .
\end{aligned}$$

For the rest of this section, we collect a few facts about dimensions of the tangent spaces $\tilde{\mathcal{N}}_v$ in preparation for the the proof of Corollory 4.2.7. Once these local dimension calculations are completed, the Corollory follows from a direct application of Proposition 4.2.2.

Definition 4.2.3. *1. For $v \neq p$,*

$$\tilde{\mathcal{N}}_v := \mathcal{N}_v \oplus H^1_{\mathrm{nr}}(\mathrm{G}_v, \mathbb{F}_q).$$

2. *For $v = p$, the tangent space $\tilde{\mathcal{N}}_p$ properly contains the direct sum of $\mathcal{N}_p \oplus H^1_{\mathrm{nr}}(\mathrm{G}_p, \mathbb{F}_q)$. Set $W = \begin{pmatrix} * & * \\ & \end{pmatrix}$, observe that W is stable under conjuagation by upper triangular matrices. Set*

$$\tilde{\mathcal{N}}_p := \ker\{H^1(\mathrm{G}_p, \mathrm{Ad}\,\bar{\rho}) \to H^1(I_p, \mathrm{Ad}\,\bar{\rho}/W)\}$$

as the choice of tangent space at p.

Let $\tilde{U}$ denote the Galois stable space of upper triangular matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, we have that $\tilde{U} = U \oplus \mathbb{F}_q \,\mathrm{Id}$. The quotient $\mathrm{Ad}\,\bar{\rho}/\tilde{U} = \mathbb{F}_q(\varphi^{-1})$ has no fixed points for the action of G_p and hence $H^1_{\mathrm{nr}}(\mathrm{G}_p, \mathrm{Ad}\,\bar{\rho}/\tilde{U}) = 0$. Consequently, $\tilde{\mathcal{N}}_p$ may be identified with the subspace

$$\tilde{\mathcal{N}}_p = \ker\left\{H^1(\mathrm{G}_p, \tilde{U}) \to H^1(I_p, \tilde{U}/W)\right\}$$

of $H^1(\mathrm{G}_p, \tilde{U})$.

For the decomposition

$$H^1(\mathrm{G}_p, \tilde{U}) \xrightarrow{\sim} H^1(\mathrm{G}_p, U) \oplus H^1(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id})$$

let π_1 and π_2 denote the projection maps to $H^1(\mathrm{G}_p, U)$ and $H^1(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id})$ respectively.

The map on restriction $\pi_1' = \pi_{1\restriction \tilde{\mathcal{N}}_p}$ induces an exact sequence.

Proposition 4.2.4. *The map on restriction $\pi_1' = \pi_{1\restriction \tilde{\mathcal{N}}_p}$ induces a short exact sequence*

$$0 \to H^1_{\mathrm{nr}}(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id}) \to \tilde{\mathcal{N}}_p \xrightarrow{\pi_1'} H^1(\mathrm{G}_p, U) \to 0.$$

Proof. As noted earlier, $\tilde{\mathcal{N}}_p$ is identified with the subspace

$$\tilde{\mathcal{N}}_p = \ker \left\{ H^1(\mathrm{G}_p, \tilde{U}) \to H^1(I_p, \tilde{U}/W) \right\}$$

of $H^1(\mathrm{G}_p, \tilde{U})$. The kernel of the projection $\pi_1 : H^1(\mathrm{G}_p, \tilde{U}) \to H^1(\mathrm{G}_p, U)$ is $H^1(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id})$. As a result, the kernel of π_1' is the intersection $H^1(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id}) \cap \tilde{\mathcal{N}}_p$, which consists of unramified central classes $H^1(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id})$. This shows that the sequence is exact in the middle.

The map on the left is clearly injective. We prove that the map π_1' is surjective. Let $f \in H^1(\mathrm{G}_p, U)$, we show that f is in the image of π_1'. It suffices to show that there exists an element $f' \in H^1(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id})$ such that $f - f' \in \tilde{\mathcal{N}}_p$, i.e. the class $f - f'$ must map to zero in $H^1(I_p, \tilde{U}/W)$.

We observe that the composite of the inclusion of $\mathbb{F}_q \cdot \mathrm{Id}$ into $\tilde{U}$ with the quotient $\tilde{U} \to \tilde{U}/W$ is an isomorphism of G_p modules (both spaces are fixed by G_p). We simply take f_1 to coincide with f modulo W w.r.t this isomorphism. This completes the proof. □

We are able to compute the dimension of $\tilde{\mathcal{N}}_p$.

Proposition 4.2.5. *For the dimension of $H^1(\mathrm{G}_p, U)$ we are to consider two cases*

$$h^1(\mathrm{G}_p, U) = \begin{cases} 2 \text{ if } \bar{\rho}_{\restriction \mathrm{G}_p} \text{ is indecomposable} \\ 3 \text{ otherwise if } \bar{\rho}_{\restriction \mathrm{G}_p} \text{ is a sum of characters} \end{cases}$$

in other words,

$$h^1(\mathrm{G}_p, U) = 2 + h^0(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho}).$$

Consequently, dimension of $\tilde{\mathcal{N}_p}$ is

$$\begin{aligned}\dim \tilde{\mathcal{N}_p} =& h^1_{\mathrm{nr}}(\mathrm{G}_p, \mathbb{F}_q \cdot \mathrm{Id}) + h^1(\mathrm{G}_p, U)\\ =& 3 + h^0(\mathrm{G}_p, \mathrm{Ad}^0\,\bar{\rho})\\ =& 2 + h^0(\mathrm{G}_p, \mathrm{Ad}\,\bar{\rho}).\end{aligned}$$

Proof. We will make use of the cohomology sequence associated with the short exact sequence

$$0 \to U^0 \to U \to U/U^0 \to 0.$$

From the isomorphism $U^0 \simeq \mathbb{F}_q(\varphi)$ and the fact that $\varphi_{\restriction \mathrm{G}_p} \neq 1, \bar{\chi}^{-1}_{\restriction \mathrm{G}_p}$. The assumptions on $\varphi_{\restriction \mathrm{G}_p}$ ensure that $H^2(\mathrm{G}_p, U^0) = 0$. From the Euler characteristic formula we have that $H^1(\mathrm{G}_p, U^0)$ is 1 dimensional.

From the Euler characteristic formula,

$$h^1(\mathrm{G}_p, U/U^0) = 2$$

and

$$h^1(\mathrm{G}_p, U^0) = 1.$$

From the long exact sequence, we have the following formula for the dimension of $H^1(\mathrm{G}_p, U)$

$$\begin{aligned}h^1(\mathrm{G}_p, U) =& h^1(\mathrm{G}_p, U^0) + h^1(\mathrm{G}_p, U/U^0) + h^0(\mathrm{G}_p, U) - 1\\ =& 2 + h^0(\mathrm{G}_p, U)\\ =& \begin{cases} 2 \text{ if } \bar{\rho}_{\restriction \mathrm{G}_p} \text{ is indecomposable} \\ 3 \text{ otherwise.}\end{cases}\end{aligned}$$

□

Condition 4 requires that $\varphi_{\restriction I_p} = \chi^{k-1}_{\restriction I_p}$ where $2 \leq k \leq p-1$. We first enumerate the possibilities which arise when $k \geq 3$.

Proposition 4.2.6. *Suppose the weight $k \neq 1, 2$ so that $3 \leq k \leq p-1$ and if $k = p-1$ by the requirement of condition 5,*

$$\varphi_{\restriction \mathrm{G}_p} \neq \bar{\chi}^{-1}_{\restriction \mathrm{G}_p}.$$

Let $\tau = \varphi_{\restriction \mathrm{G}_p}$ be a product of an unramified character with $\bar{\chi}^{k-1}$. With these assumptions, there are the following cases to consider

1. $\bar{\rho}_{\restriction \mathrm{G}_p} = \begin{pmatrix} \tau & \\ & 1 \end{pmatrix}$ *up to twisting by an unramified character. The ordinary arbitrary-weight deformation ring is smooth in 4 variables and*

$$\dim \tilde{\mathcal{N}}_p = 4,$$

$$h^0(\mathrm{G}_p, \mathrm{Ad}\, \bar{\rho}) = 2,$$

or,

2. $\bar{\rho}_{\restriction \mathrm{G}_p} = \begin{pmatrix} \tau & * \\ & 1 \end{pmatrix}$ *is indecomposable in which case, the ordinary arbitrary-weight deformation ring is smooth in 3 variables and*

$$\dim \tilde{\mathcal{N}}_p = 3,$$

$$h^0(\mathrm{G}_p, \mathrm{Ad}\, \bar{\rho}) = 1.$$

Proof. There is an unramified character $\eta : \mathrm{G}_p \to \mathbb{F}_q^\times$ such that $\tau = \eta\bar{\chi}_{\restriction \mathrm{G}_p}^{k-1}$. It follows from the assumptions on k and φ that the characters $\tau, \tau\bar{\chi}_{\restriction \mathrm{G}_p}$ and $\tau\bar{\chi}_{\restriction \mathrm{G}_p}^{-1}$ are all nontrivial. In both cases we compare the ordinary deformation problem to the upper triangular deformation problem. Observe that $\mathrm{Ad}\,\bar{\rho}/\tilde{U}$ can be identified with $\mathbb{F}_q(\tau^{-1})$.

Since $\tau \neq 1$, we have that $H^1_{\mathrm{nr}}(\mathrm{G}_p, \mathrm{Ad}\,\bar{\rho}/\tilde{U}) = 0$ and consequently

$$\tilde{\mathcal{N}}_p = \ker\{H^1(\mathrm{G}_p, \tilde{U}) \to H^1(I_p, \tilde{U}/W)\}$$

where we recall that $W \subset \tilde{U}$ consists of matrices $\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$.

In both cases $\tilde{\mathcal{C}}_p$ can be derived from the upper triangular deformation problem by imposing the condition that a generator of $Gal(\mathbb{Q}^{cyc}/\mathbb{Q}) \simeq \mathbb{Z}_p$ maps to an upper triangular matrix for which the lower right entry is trivial.

1. In the first case, $\tilde{U} \simeq \mathbb{F}_p^2 \oplus \mathbb{F}_q(\tau)$. An application of Local-Duality implies that

$$\begin{aligned} & h^2(\mathrm{G}_p, \tilde{U}) \\ =& h^0(\mathrm{G}_p, \tilde{U}^*) \\ =& 2h^0(\mathrm{G}_p, \mathbb{F}_q(\bar{\chi}_{\restriction \mathrm{G}_p})) + h^0(\mathrm{G}_p, \mathbb{F}_q(\tau^{-1}\bar{\chi}_{\restriction \mathrm{G}_p})) \\ =& 0. \end{aligned}$$

An application of the Euler Characteristic Formula shows that

$$
\begin{aligned}
&h^1(\mathrm{G}_p, \tilde{U}) \\
=&h^0(\mathrm{G}_p, \tilde{U}) + h^2(\mathrm{G}_p, \tilde{U}) + \dim \tilde{U} \\
=&5.
\end{aligned}
$$

Consequently, the deformation ring of unrestricted upper triangular deformations of $\bar{\rho}_{\restriction \mathrm{G}_p}$ is a power series ring in five variables. The relation imposed for a deformation to be ordinary comes from setting the ramified part of the lower right entry when evaluated at a topological generator of the cyclotomic extension of $\mathbb{Q}_p$. This restriction cuts down dimension of the tangent space by one and corresponds to going modulo one of the variables in the tangent space. We can take this to be a variable in a power series ring in five variables and so the quotient is a power series ring in four variables, in particular the deformation ring is smooth. This completes the proof of the first part.

Since the diagonal characters of $\tilde{U}^*$ are nontrivial and consequently $H^2(\mathrm{G}_p, \tilde{U}) = 0$. Since we are assuming that $\bar{\rho}_{\restriction \mathrm{G}_p}$ is indecomposable $h^0(\mathrm{G}_p, \tilde{U}) = 2$. From the Euler characteristic formula it follows that $h^1(\mathrm{G}_p, \tilde{U}) = 4$. The rest follows just as in part 1.

$\square$

The proof of Proposition 4.2.6 is more or less the same as the first two cases outlined in [12, Proposition 11], in which k is prescribed to be 2. We refer to [12, Proposition 11] for an enumeration of all the possibilities for $k = 2$.

Corollary 4.2.7. *Let $\bar{\rho}$ be subject to the conditions enumerated in Theorem* 4.1.1*. Let X be a finite set of trivial primes disjoint from S. Then*

$$h^1_{\tilde{\mathcal{N}},S\cup X} - h^1_{\tilde{\mathcal{N}}^{\perp},S\cup X} = 1.$$

Proof. The dimension of the local tangent spaces at p for the full-adjoint deformation problems are as follows,

$$\begin{aligned}
&\dim \tilde{\mathcal{N}}_\infty = 0\\
&\dim \tilde{\mathcal{N}}_p = h^0(\mathrm{G}_p, \mathrm{Ad}\,\bar{\rho}) + 2\\
&\dim \tilde{\mathcal{N}}_v = h^0(G_v, \mathrm{Ad}\,\bar{\rho}) \text{ for } v \in S\backslash\{p\}\\
&\dim \tilde{\mathcal{N}}_v = h^0(G_v, \mathrm{Ad}\,\bar{\rho}) \text{ for } v \notin S \text{ a trivial prime.}
\end{aligned}$$

An application of Wiles' formula yields

$$\begin{aligned}
&h^1_{\tilde{\mathcal{N}},S\cup X} - h^1_{\tilde{\mathcal{N}}^{\perp},S\cup X}\\
&= h^0(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}\,\bar{\rho}) - h^0(\mathrm{G}_{\mathbb{Q}}, \mathrm{Ad}\,\bar{\rho}^*) + \sum_{v\in S\cup X\cup\{\infty\}} \Big(\dim \tilde{\mathcal{N}}_v - h^0(G_v, \mathrm{Ad}\,\bar{\rho})\Big)\\
&= 1 + \sum_{v\in S\cup X\cup\{\infty\}} \Big(\dim \tilde{\mathcal{N}}_v - h^0(G_v, \mathrm{Ad}\,\bar{\rho})\Big) \qquad (4.3)\\
&= 3 - h^0(Gal(\mathbb{C}/\mathbb{R}), \mathrm{Ad}\,\bar{\rho})\\
&= 1.
\end{aligned}$$

□

4.3 Versal Deformations at Trivial Primes

In this section we outline deformation problems at the primes which will constitute the auxiliary primes introduced in the previous chapter. Unlike nice primes, the deformation problems at trivial primes are only versal. Recall that a prime v is a trivial prime if

1. $\mathrm{G}_v \subset \ker \bar{\rho}$,
2. the prime $v \equiv 1 \mod p$ but $v \not\equiv 1 \mod p^2$.

Fact 4.3.1. *For a trivial prime v,*

$$h^i(G_v, \mathrm{Ad}^0 \bar{\rho}) = \begin{cases} 3 \textit{ if } i = 0, 2, \\ 6 \textit{ if } i = 1, \end{cases}$$

$$h^i(G_v, \mathrm{Ad}\, \bar{\rho}) = \begin{cases} 4 \textit{ if } i = 0, 2, \\ 8 \textit{ if } i = 1. \end{cases}$$

All higher cohomology groups are zero. This follows from an application local duality and the local Euler Characteristic formula (cf. [16]).

Let v be a trivial prime. Choose a square root of v in $W(\mathbb{F}_q)$. Fix a basis with respect to which $\bar{\rho}$ is upper triangular. Let v be a trivial prime, $\bar{\rho}_{\restriction G_v}$ is tamely ramified. Let σ_v be a choice of Frobenius at v and τ_v a generator of the maximal pro-p tame inertia. The maximal pro-p extension of $\mathbb{Q}_v$ is generated by σ_v and τ_v

which are subject to a single relation

$$\sigma_v \tau_v \sigma_v^{-1} = \tau_v^v.$$

Set $\psi = \tilde{\varphi}\chi^{p^3(p-1)/2}$. This is the choice of character lifting $\det \bar{\rho}$ specified in [9]. We define the deformation condition $\mathcal{C}_v$ at v by specifying the values taken on the elements σ_v and τ_v. These definitions make their first appearance in Sections 4 of [9]. Fix the basis $\mathcal{B}$ with respect to which

$$\bar{\rho} = \begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix}.$$

Definition 4.3.2. *We proceed to prescribe deformation problems at trivial primes.*

- *Let $\mathcal{D}_v$ be the class of deformations of $\bar{\rho}_{\restriction G_v}$ containing representatives taking*

$$\sigma_v \mapsto v^{(p^3-p^2-1)/2} \begin{pmatrix} v & x \\ 0 & 1 \end{pmatrix}$$
$$\tau_v \mapsto \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

  with respect to a basis lifting $\mathcal{B}$ and insist that p^2 divides x.

- *Separate $\mathcal{D}_v$ into two classes, the first class of deformations are those that are ramified modulo p^2, i.e. $\mathcal{D}_v^{\mathrm{ram}}$ consists of those deformations for which p divides y but p^2 does not divide y. Those that are unramified modulo p^2 are denoted $\mathcal{D}_v^{\mathrm{nr}}$.*

- *We let $\tilde{\mathcal{D}}_v$ be the deformations obtained as unramified central twists of those in $\mathcal{D}_v$.*

In other words, deformations $\mathcal{D}_v$ are those with a representative taking

$$\sigma_v \mapsto z \begin{pmatrix} v & x \\ 0 & 1 \end{pmatrix}$$

$$\tau_v \mapsto \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

where $z \equiv 1 \mod p$, $x \equiv 0 \mod p^2$. We emphasize that the requirement that $x \equiv 0 \mod p^2$ is an additional assumption in our setting.

We proceed to describe a pair of spaces $\mathcal{Q}_v \subset \mathcal{P}_v^* \subset H^1(G_v, \operatorname{Ad}^0 \bar{\rho})$ such that $\mathcal{Q}_v$ stabilizes $\mathcal{D}_v$ and $\mathcal{P}_v^*$ stabilizes the set of mod p^N deformations $\mathcal{D}_v(W(\mathbb{F}_q)/p^N)$ for $N \geq 3$. Here, $* \in \{\mathrm{ram}, \mathrm{nr}\}$ depending on whether we consider the case when deformations are ramified mod p^2 or unramified mod p^2. The larger space $\mathcal{N}_v$ has dimension equal to $h^0(\mathrm{G}_v, \operatorname{Ad}^0 \bar{\rho}) = 3$. As discussed in the previous section, this facilitates for a balanced Selmer condition, i.e.

$$h^1_{\mathcal{N}, S\cup X} = h^1_{\mathcal{N}^\perp, S\cup X}.$$

The key observation of Hamblen and Ramakrishna is that one may allow ramification at a number of trivial primes X_1 disjoint from S so as to lift $\bar{\rho}$ to an irreducible mod p^3 representation ρ_3 the local constraints at the set S and the set of trivial primes X_1. At this stage, the versal deformation functors at trivial primes play the exact role of the deformation conditions at nice primes. It becomes possible to adapt Ramakrishna's lifting argument from [23], namely, allow ramification at a finite set of trivial primes $X \supseteq X_1$ so the dual Selmer group $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho}^*) = 0$. The Galois representation ρ_3 lifts to a characteristic zero representation $\rho : \mathrm{G}_{\mathbb{Q},S\cup X} \to \mathrm{GL}_2(W(\mathbb{F}_q))$ which is irreducible and odd. It follows from the results of Skinner and Wiles [20] that ρ arises from a Hecke eigencuspform. The reader may also refer to the modern treatments in [28] and [19], which discuss Ramakrishna's lifting construction in the residually irreducible case.

The two classes of deformations (ramified mod p^2 and unramified mod p^2) play different roles in the deformation theoretic arguments. Trivial primes at which deformations are ramified modulo p^2 are used to lift $\bar{\rho}$ to a mod p^3 representation ρ_3 satisfying local constraints. The trivial primes at which deformations are unramified modulo p^2 are used to kill the dual Selmer group and thereby lift ρ_3 to a characteristic zero rerpesentation. The reader is not required to fully understand the role of the two choices of deformation problems to understand and appreciate the arguments in this manuscript.

We recall some notation from [9, section 4].

Definition 4.3.3. *Set*

$$f_1(\sigma_v) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f_1(\tau_v) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$f_2(\sigma_v) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, f_2(\tau_v) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$g^{\mathrm{nr}}(\sigma_v) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, g^{\mathrm{nr}}(\tau_v) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$g^{\mathrm{ram}}(\sigma_v) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, g^{\mathrm{ram}}(\tau_v) = \begin{pmatrix} -\frac{y}{v-1} & 0 \\ 0 & \frac{y}{v-1} \end{pmatrix}.$$

The space $\mathcal{Q}_v$ denotes the subspace of $H^1(G_v, \mathrm{Ad}^0\,\bar{\rho})$ spanned by f_1 and f_2, let $\mathcal{P}_v^{\mathrm{nr}}$ the subspace spanned by f_1, f_2 and g^{nr} and $\mathcal{P}_v^{\mathrm{ram}}$ the subspace spanned by f_1, f_2 and g^{ram}.

Definition 4.3.4.

1. *For trivial primes v whose mod p^2 deformations are unramified $\mathcal{M}_v$, $\mathcal{N}_v$ and $\mathcal{C}_v$ to consist of conjugates by $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ of elements of $\mathcal{Q}_v$, $\mathcal{P}_v^{\mathrm{nr}}$ and $\mathcal{D}_v^{\mathrm{nr}}$ respectively.*
2. *For trivial primes v whose mod p^2 deformations are ramified $\mathcal{M}_v$, $\mathcal{N}_v$ and $\mathcal{C}_v$ consist of conjugates by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of elements of $\mathcal{Q}_v$, $\mathcal{P}_v^{\mathrm{ram}}$ and $\mathcal{D}_v^{\mathrm{ram}}$ respectively.*
3. *In both cases, let $\tilde{\mathcal{N}}_v$, $\tilde{\mathcal{M}}_v$ and $\tilde{\mathcal{C}}_v$ be the unramified central twists of $\mathcal{N}_v$, $\mathcal{M}_v$ and $\mathcal{C}_v$ respectively.*

Proposition 4.3.5. *Let $R \in \mathfrak{C}$ a coefficient ring with maximal ideal $\mathfrak{m}$ (recall that it is stipulated that $p \notin \mathfrak{m}^2$). For $k \geq 1$ let $\mathfrak{n}_k := pR \cap \mathfrak{m}^k$. For both ramified and unramified* *mod p^2 deformations, the space $\mathcal{N}_v \otimes \mathfrak{n}_k/\mathfrak{n}_{k+1}$ preserves $\mathcal{C}_v(R/\mathfrak{n}_{k+1})$ for $k \geq 2$.*

Proof. Let $k \geq 2$ and $\varrho_k \in \mathcal{C}_v(R/\mathfrak{n}_{k+1})$ and let $pr \in \mathfrak{n}_k$. Consider the case when p^2 divides y. Since $k \geq 2$ the assumption $p \notin \mathfrak{m}^2$ implies that $p \notin \mathfrak{n}_k$ and consequently, $r \in \mathfrak{m}$. Let

$$\varrho_k' := \exp(g^{\mathrm{nr}} \otimes pr)\varrho_k = (Id + prg^{\mathrm{nr}})\varrho_k$$

we show that ϱ_k' belongs to $\mathcal{C}_v(R/\mathfrak{n}_{k+1})$.

We recall that

$$\varrho_k(\sigma_v) = v^{(p^3-p^2-1)/2}\begin{pmatrix} v & x \\ 0 & 1 \end{pmatrix}.$$

It is easy to see that $p\mathfrak{n}_k \subseteq \mathfrak{n}_{k+1}$. Since v is 1 mod p and $x \in \mathfrak{m}$,

$$(Id + prg^{\mathrm{nr}})\varrho_k(\sigma_v) = v^{(p^3-p^2-1)/2}\begin{pmatrix} v & x \\ pr & 1 \end{pmatrix}$$

$$(Id + prg^{\mathrm{nr}})\varrho_k(\tau_v) = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}.$$

Since $v \not\equiv 1 \mod p^2$, we have that $\frac{p}{v-1}$ is a unit. Since the element x is divisible by p^2 we have that $\frac{xpr}{v-1} \in \mathfrak{n}_{k+1}$. We see that

$$\left(Id + r\begin{pmatrix} 0 & 0 \\ \frac{p}{v-1} & 0 \end{pmatrix}\right)^{-1} v^{(p^3-p^2-1)/2}\begin{pmatrix} v & x \\ pr & 1 \end{pmatrix}\left(Id + r\begin{pmatrix} 0 & 0 \\ \frac{p}{v-1} & 0 \end{pmatrix}\right) \tag{4.4}$$

$$= v^{(p^3-p^2-1)/2}\begin{pmatrix} v & x \\ 0 & 1 \end{pmatrix} = \varrho_k(\sigma)$$

and as p^2 divides y, the element $\frac{pry}{v-1} \in \mathfrak{n}_{k+1}$ and as a consequence,

$$\left(Id + r\begin{pmatrix} 0 & 0 \\ \frac{p}{v-1} & 0 \end{pmatrix}\right)^{-1} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \left(Id + r\begin{pmatrix} 0 & 0 \\ \frac{p}{v-1} & 0 \end{pmatrix}\right)$$

$$= \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \varrho_k(\tau).$$

Next consider deformations for which p^2 does not divide y. The conclusion of 4.4 remains unchanged as $g^{\text{ram}}(\sigma_v) = g^{\text{nr}}(\sigma_v)$. We observe that

$$\left(Id + r\begin{pmatrix} 0 & 0 \\ \frac{p}{v-1} & 0 \end{pmatrix}\right) \varrho_k(\tau) \left(Id + r\begin{pmatrix} 0 & 0 \\ \frac{p}{v-1} & 0 \end{pmatrix}\right)^{-1}$$

$$= (Id + prg^{\text{ram}})\varrho_k(\tau) = \begin{pmatrix} 1 - \frac{pry}{v-1} & y \\ 0 & 1 + \frac{pry}{v-1} \end{pmatrix}$$

(unlike in the case for which p^2 divides y this matrix need not be unipotent). The case for f_1 and f_2 follows similarly. □

4.4 A Purely Galois Theoretic Lifting Construction

In [9], it is shown that there exists a finte set of trivial primes X_1, that are disjoint from S such that $\bar{\rho}$ lifts to an irreducible mod p^3 representation

$$\rho_3 : \mathrm{G}_{\mathbb{Q}, S \cup X_1} \to \mathrm{GL}_2(W(\mathbb{F}_q)/p^3).$$

Furthermore, ρ_3 satisfies the local deformation conditions $\mathcal{C}_v$ at each prime $v \in X_1$. The set of trivial primes X_1 in particular has the property that $Ш^2_{S\cup X_1}(\mathrm{Ad}^0\,\bar{\rho}) = 0$. It is then shown that the set of primes X_1 may be further extended to a finite set of trivial primes X containing X_1 such that $h^1_{\mathcal{N}^\perp, S\cup X} = 0$. Denote by Φ the collection of versal deformation problems $\Phi = \{\tilde{\mathcal{C}}_v\}_{v\in S\cup X}$. Denote by $\rho_2 := \rho_3 \mod p^2$.

Definition 4.4.1. *A ring $R \in \mathfrak{C}$ with maximal ideal $\mathfrak{m}_R$ is endowed with a decreasing chain of ideals $\{\mathfrak{n}_k\}_{k\geq 1}$ defined by $\mathfrak{n}_k := pR \cap \mathfrak{m}_R^k$. In dealing with more than one ring R we will use $\mathfrak{n}_k(R)$ instead of $\mathfrak{n}_k$.*

Definition 4.4.2. *For $R \in \mathfrak{C}$, let $\rho_{2,R}$ denote the deformation with image in $\mathrm{GL}_2(R/\mathfrak{n}_2)$ induced from ρ_2 by the structure map $W(\mathbb{F}_q) \to R$. Let $\mathcal{D}ef_\Phi : \mathfrak{C} \to \mathrm{Sets}$ be the functor such that $\mathcal{D}ef_\Phi(R)$ consists of deformations $\rho_R : \mathrm{G}_{\mathbb{Q},Y} \to \mathrm{GL}_2(R)$ for which*

$$\rho_{2,R} = \rho_R \mod \mathfrak{n}_2.$$

Definition 4.4.3. *Let $R \in \mathfrak{C}$ have maximal ideal $\mathfrak{m}_R$ and let J an ideal in R. The map of coefficient rings $R \to R/J$ is said to be nearly small $\mathfrak{m}_R J = 0$. It is said to be small if it is nearly small and if J is principal.*

Fact 4.4.4. *Let $R \to R/J$ be nearly small and $v \in S$. The exponential map of a pure tensor*

$$X \otimes j \in H^1(G_v, \mathrm{Ad}\,\bar{\rho}) \otimes_{\mathbb{F}_q} J$$

takes $\varrho \in \tilde{\mathcal{C}}_v(R)$ to

$$\exp(X \otimes j)\varrho := (\mathrm{Id} + X \otimes J)\varrho.$$

The fibers of the mod J reduction map $\tilde{\mathcal{C}}_v(R) \to \tilde{\mathcal{C}}_v(R/J)$ are $H^1(\mathrm{G}_v, \mathrm{Ad}\,\bar{\rho}) \otimes_{\mathbb{F}_q} J$ pseudotorsors.

Remark 4.4.5. *Let $R \in \mathfrak{C}$,*

1. $\mathfrak{n}_1 = pR$ *and that* $\mathfrak{n}_k/\mathfrak{n}_{k+1}$ *is an* $R/\mathfrak{m} \simeq \mathbb{F}_q$ *vector space.*

2. *If R is a power series ring $R = W(\mathbb{F}_q)[[U_1, \dots, U_s]]$ and $k \geq 1$, the quotient $\mathfrak{n}_k/\mathfrak{n}_{k+1}$ is an $\mathbb{F}_q$ vector space with basis representatives $[p^{k-b}U_1^{a_1} \dots U_s^{a_s}] \in \mathfrak{n}_k/\mathfrak{n}_{k+1}$ for $a_1, \dots, a_s, b \geq 0, b = a_1 + \cdots + a_s < k$, for instance,*

$$\mathfrak{n}_1/\mathfrak{n}_2 = \mathbb{F}_q[p],$$

$$\mathfrak{n}_2/\mathfrak{n}_3 = \mathbb{F}_q[p^2] \oplus \mathbb{F}_q[pU_1] \oplus \cdots \oplus \mathbb{F}_q[pU_s].$$

Definition 4.4.6. *For $R \in \mathfrak{C}$ the structure map $W(\mathbb{F}_q) \to R/\mathfrak{n}_3R$ factors through*

$$\gamma_R : W(\mathbb{F}_q)/p^3 \to R/\mathfrak{n}_3.$$

Likewise, the structure map induces an inclusion in $\mathfrak{C}$

$$\beta_R : W(\mathbb{F}_q)/p \hookrightarrow R/\mathfrak{n}_1.$$

Before commencing with the proof of Theorem 4.1.1, let us briefly outline the strategy. Let $\mathcal{R} := W(\mathbb{F}_q)[[U]] \in \mathfrak{C}$ and $\mathfrak{m} = (p, U)$ its maximal ideal. The first step of the proof involves producing an appropriately chosen deformation

$$\begin{array}{ccc} & & \mathrm{GL}_2(\mathcal{R}) \\ & \overset{\tilde{\varrho}}{\nearrow} & \downarrow \\ \mathrm{G}_{\mathbb{Q},S\cup X} & \xrightarrow{\bar{\rho}} & \mathrm{GL}_2(\mathcal{R}/\mathfrak{m}). \end{array}$$

The second step involves showing that $\tilde{\varrho}$ is a versal hull in the sense of Theorem 4.1.1.

Lemma 4.4.7. *Let X be the set of primes chosen as indicated at the start of this section. Then*

1. $h^1_{\tilde{\mathcal{N}},S\cup X} = 1$ *and* $h^1_{\tilde{\mathcal{N}}^\perp,S\cup X} = 0$,
2. $\text{Ш}^2_{S\cup X}(\mathrm{Ad}\,\bar{\rho}) = 0$.

Proof. The set of primes X is chosen so that among other conditions satisfied, $h^1_{\mathcal{N}^\perp,S\cup X} = 0$. We show that it follows that $h^1_{\tilde{\mathcal{N}}^\perp,S\cup X} = 0$. From this, it will follow from Corollory 4.2.7 that $h^1_{\tilde{\mathcal{N}},S\cup X} = 1$. Recall that $\tilde{\mathcal{N}_v} = H^1_{\mathrm{nr}}(G_v, \mathbb{F}_q) \oplus \mathcal{N}_v$ at all primes $v \in S \cup X\backslash\{p\}$ and $\tilde{\mathcal{N}_p} \supsetneq H^1_{\mathrm{nr}}(\mathrm{G}_p, \mathbb{F}_q) \oplus \mathcal{N}_p$. A class

$$f \in H^1_{\tilde{\mathcal{N}}^\perp}(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}\,\bar{\rho}^*)$$

is represented a sum of

$$f = f_1 + f_2$$

where

$$f_1 \in H^1(\mathrm{G}_{\mathbb{Q},S\cup X}, (\mathbb{F}_q \cdot \mathrm{Id})^*)$$

and

$$f_2 \in H^1(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho}^*).$$

We observe that $f_2 \in H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho}^*)$. At each prime $v \in S\cup X$, the restriction of the class f to G_v is perpendicular to $\mathcal{N}_v \subset \tilde{\mathcal{N}_v}$. Since f_1 takes values in $(\mathbb{F}_q \cdot \mathrm{Id})^*$ and $\mathcal{N}_v \subset \mathrm{Ad}^0\,\bar{\rho}$, f_1 on restriction to G_v is perpendicular to $\mathcal{N}_v$. Consequently, $f_2 = f - f_1$ lies in $\mathcal{N}_v^\perp$ on restriction to G_v. We deduce that f_2 lies in the dual Selmer group $H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho}^*)$ are therefore $f_2 = 0$.

Since $\tilde{\mathcal{N}}_v$ contains the unramified classes $H^1_{\mathrm{nr}}(\mathrm{G}_v, \mathbb{F}_q \cdot \mathrm{Id})$, similar reasoning shows that f_1 is unramified everywhere.

Let $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ denote the class group of $\mathbb{Q}(\mu_p)$ with induced $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ action. By [30][Proposition 6.16] the $\bar{\chi}$ isotypic component

$$\left(\mathrm{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_q\right)(\bar{\chi}) = 0.$$

From an application of inflation-restriction we have that

$$H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{F}_q^*) \simeq H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{F}_q(\bar{\chi}))^{\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})} \simeq \mathrm{Hom}(G_{\mathbb{Q}(\mu_p)}, \mathbb{F}_q(\bar{\chi}))^{Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})}.$$

We conclude that the unramified class $f_1 = 0$ and as a consequence, $f = f_1 + f_2 = 0$.

Since $h^1_{\tilde{\mathcal{N}}^\perp, S\cup X} = 0$ we deduce in particular that $\text{Ш}^1_{S\cup X}(\mathrm{Ad}\,\bar{\rho}^*) = 0$. By Global duality, $\text{Ш}^2_{S\cup X}(\mathrm{Ad}\,\bar{\rho}) \simeq \text{Ш}^1_{S\cup X}(\mathrm{Ad}\,\bar{\rho}^*)^\vee = 0$. □

Proof. (of Theorem 4.1.1)

By Lemma 4.4.7, we have that $h^1_{\tilde{\mathcal{N}}^\perp, S\cup X} = 0$ and therefore, from the Poitou-Tate long exact sequence, we get the short the short exact sequence

$$0 \to H^1_{\tilde{\mathcal{N}}}(G_{\mathbb{Q}, Z\cup X}, \mathrm{Ad}\,\bar{\varrho}) \to H^1(\mathrm{G}_{\mathbb{Q}, Z\cup X}, \mathrm{Ad}\,\bar{\varrho}) \to \bigoplus_{v\in Z\cup X} \frac{H^1(G_v, \mathrm{Ad}\,\bar{\varrho})}{\tilde{\mathcal{N}}_v} \to 0. \quad (4.5)$$

Pushing forward by the map $\gamma_{\mathcal{R}}$,

$$\rho_3 : \mathrm{G}_{\mathbb{Q}, Z\cup X} \to \mathrm{GL}_2(R/\mathfrak{n}_3).$$

By Lemma 4.4.7, the Selmer group $H^1_{\tilde{\mathcal{N}}}(\mathrm{G}_{\mathbb{Q}, Z\cup X}, \mathrm{Ad}\,\bar{\varrho})$ is one-dimensional. Pick a basis $\{g\}$ for this Selmer group. As a vector space of $\mathcal{R}/\mathfrak{m} = \mathbb{F}_q$

$$\mathfrak{n}_2/\mathfrak{n}_3 = \mathbb{F}_q[p^2] \oplus \mathbb{F}_q[pU].$$

Set $\alpha := g \otimes [pU]$ and set $\varrho_3 = \exp(\alpha)\rho_3$. Since ρ_3 satisfies Φ, so does ϱ_3. Since $\text{Ш}^2_{S\cup X}(\mathrm{Ad}^0\,\bar{\rho})$ and there are no local obstructions to lifting ϱ_3 to a mod p^4 representation, it follows that ϱ_3 lifts to

$$\rho_4 : \mathrm{G}_{\mathbb{Q},S\cup X} \to \mathrm{GL}_2(\mathcal{R}/\mathfrak{n}_4).$$

From the surjectivity of the restriction map on the right of the the short exact sequence 4.5, it follows that there exists a cohomology class

$$\beta^{(4)} \in H^1(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}\,\bar{\rho}) \otimes \mathfrak{n}_4/\mathfrak{n}_3$$

such that the twist $\varrho_4 := \exp(\beta^{(4)})\rho_4$ satisfies Φ and hence lifts to ρ_5. In this fashion, a compatible system of deformations $\{\varrho_k\}_{k\geq 2}$ is constructed and the passage to the inverse limit of which yields a deformation

$$\tilde{\varrho} : \mathrm{G}_{\mathbb{Q},S\cup X} \to \mathrm{GL}_2(\mathcal{R})$$

satisfying Φ. It is only at the mod p^3 level that the deformation is modified by α. This is done so that $\tilde{\varrho}$ is a versal hull for $\mathcal{D}ef_\Phi$. Moreover, since $\mathfrak{n}_k$ is contained in $p\mathcal{R}$ for all k, the deformation $\tilde{\varrho}$ equal $\bar{\rho}$ modulo p. Consequently, $\tilde{\varrho} \in \mathcal{D}ef_\Phi(\mathcal{R})$.

Next, it is shown that $\tilde{\varrho}$ represents a versal hull of $\mathcal{D}ef_\Phi$. Let $\sigma \in \mathcal{D}ef_\Phi(\mathcal{S})$ and let $\mathfrak{m}_\mathcal{S}$ denote the maximal ideal of $\mathcal{S}$ and for $k \geq 1$

$$\mathfrak{n}_k(\mathcal{S}) := p\mathcal{S} \cap \mathfrak{m}^k_\mathcal{S}.$$

Let

$$f_3 : \mathcal{R} \to W(\mathbb{F}_q)/p^3$$

be the $W(\mathbb{F}_q)$-algebra homomorphism in $\mathfrak{C}$ for which $f_3(U) = 0$ and let

$$\varphi_3 : \mathcal{R} \to \mathcal{S}/\mathfrak{n}_3(\mathcal{S})$$

be the composite $\varphi_3 := \gamma_{\mathcal{S}} \circ f_3$ (see 4.4.6 for the definition of $\gamma_{\mathcal{S}}$). We successively lift φ_3 to a map $\varphi : \mathcal{R} \to \mathcal{S}$ such that $\sigma = \tilde{\varrho}^*(\varphi)$. Let $\varphi_2 := \varphi_3 \mod \mathfrak{n}_2(\mathcal{S})$ and set $\sigma_k := \sigma \mod \mathfrak{n}_k(S)$. Since $\sigma_2 = \tilde{\varrho}_2$, it may be observed from the construction of $\tilde{\varrho}$ that $\sigma_2 = \tilde{\varrho}^*(\varphi_2)$. Suppose that for $k \geq 3$, σ_{k-1} and φ_{k-1} satisfy the relation $\sigma_{k-1} = \tilde{\varrho}^*(\varphi_{k-1})$, we show that one may lift φ_{k-1} to φ_k

$$\begin{array}{ccc} & & \mathcal{S}/\mathfrak{n}_k(\mathcal{S}) \\ & \overset{\varphi_k}{\nearrow} & \downarrow \\ \mathcal{R} & \xrightarrow{\varphi_{k-1}} & \mathcal{S}/\mathfrak{n}_{k-1}(\mathcal{S}) \end{array} \tag{4.6}$$

so that $\sigma_k = \tilde{\varrho}^*(\varphi_k)$. The lift $\varphi := \varprojlim_k \varphi_k$ need not be the unique map for which $\sigma = \tilde{\varrho}^*(\varphi)$ and the deformation $\tilde{\varrho}$ is only versal.

Being a formal power ring, $\mathcal{R}$ satisfies the infinitesimal lifting property, and consequently, φ_{k-1} lifts to $g_k : \mathcal{R} \to \mathcal{S}/\mathfrak{n}_k(\mathcal{S})$. Let

$$\mu_k : \mathrm{G}_{\mathbb{Q},Z\cup X} \to \mathrm{GL}_2(\mathcal{S}/\mathfrak{n}_k)$$

be the push-forward of $\tilde{\varrho}$ by g_k^*, that is, $\mu_k := \tilde{\varrho}^*(g_k)$.

Both σ_k and μ_k are deformations of σ_{k-1} in $\mathcal{D}ef_\Phi(\mathcal{S}/\mathfrak{n}_k(\mathcal{S}))$. There is a class

$$\gamma \in H^1_{\mathcal{N}}(\mathrm{G}_{\mathbb{Q},Z}, \mathrm{Ad}\,\bar{\rho}) \otimes \mathfrak{n}_{k-1}(\mathcal{S})/\mathfrak{n}_k(\mathcal{S})$$

for which

$$\sigma_k = \exp(\gamma)\mu_k = (\mathrm{Id} + \gamma)\mu_k.$$

Let $G = g_k(U)$ and $\gamma = g \otimes [pH]$ with $[pH] \in \mathfrak{n}_{k-1}(\mathcal{S})/\mathfrak{n}_k(\mathcal{S})$ (the choice of the H is not unique). Since $\mathcal{S} \in \mathfrak{C}$, we note that H is in the maximal ideal of $\mathcal{S}$.

Let $\varphi_k : \mathcal{R} \to \mathcal{S}/\mathfrak{n}_k(\mathcal{S})$ be the $W(\mathbb{F}_q)$-algebra map which takes

$$U \mapsto G + H.$$

We will now show that the effect of replacing g_k by φ_k is that $\mu_k = g_k^*(\tilde{\varrho})$ gets replaced by $\sigma_k = \exp(\gamma)\mu_k$. This will conclude the proof.

Recall from the construction of $\tilde{\varrho}$ that in matrix notation

$$\tilde{\varrho} = (\mathrm{Id} + gpU)\rho_3 = \rho_3 + gpU\bar{\rho} \mod \mathfrak{n}_3(\mathcal{R}). \tag{4.7}$$

The ideal $\mathfrak{n}_3(\mathcal{R})$ is generated by monomials p^3, p^2U, pU^2. Since $pH \in \mathfrak{n}_{k-1}(\mathcal{S})$, we have that $pHG \in \mathfrak{n}_k(\mathcal{S})$ for any $G \in \mathfrak{m}_{\mathcal{S}}$. Consequently, an application of the binomial theorem yields that for a monomial p^aU^b for which $a + b = 3$ and $a \geq 1$

$$\begin{aligned}\varphi_k(p^aU^b) &= p^a(G+H)^b \\ &= p^aG^b \\ &= g_k(p^aU^b).\end{aligned}$$

Hence $\varphi_k(x) = g_k(x)$ for $x \in \mathfrak{n}_3(\mathcal{R})$. From the relation, 4.7 we deduce that as a function to 2×2 matrices $M_2(\mathcal{S}/\mathfrak{n}_k(\mathcal{S}))$

$$\tilde{\varrho}^*(\varphi_k) - \mu_k : \mathrm{G}_{\mathbb{Q}, Z \cup X} \to M_2(\mathcal{S}/\mathfrak{n}_k(\mathcal{S}))$$

evaluates to

$$\begin{aligned}\tilde{\varrho}^*(\varphi_k) - \mu_k &= \tilde{\varrho}^*(\varphi_k) - \tilde{\varrho}^*(g_k) \\ &= \varphi_k \circ (\rho_3 + g\bar{\rho}pU + \mathfrak{n}_3(\mathcal{R})) - g_k \circ (\rho_3 + g\bar{\rho}pU + \mathfrak{n}_3(\mathcal{R}))\,.\end{aligned}$$

Since $\phi_k(x) = g_k(x)$ for $x \in \mathfrak{n}_3(\mathcal{R})$, the above may be represented as

$$\begin{aligned}&= (\rho_3 + g\bar{\rho}p\varphi_k(U)) - (\rho_3 + g\bar{\rho}pg_k(U)) \\ &= gpH.\bar{\rho}\end{aligned}$$

Consequently

$$\tilde{\varrho}^*(\varphi_k) = \mu_k + \gamma\bar{\rho} = \mu_k + \gamma\mu_k = (\mathrm{Id} + \gamma)\mu_k = \sigma_k.$$

This completes the induction step. □

Remark 4.4.8. *Having shown that for $R \in \mathfrak{C}$, the map induced by $\tilde{\varrho}$*

$$\tilde{\varrho}^* : \mathrm{Hom}(\mathbb{Z}_p[[U]], R) \to \mathcal{D}ef_{\Phi}(R)$$

is surjective. However, it is not injective when the p torsion in R is non-zero. We refer to the proof of the above Theorem, the choice of the element H are not uniquely determined.

Proof. (of Theorem 4.1.2) Let $R \in \mathfrak{C}$ and $\mathfrak{f} \in \mathrm{Hom}_{\mathfrak{C}}(W(\mathbb{F}_q)[|U|], R)$ with associated deformation $\rho_{\mathfrak{f}} \in \mathcal{D}ef_{\Phi}(R)$. We take note that the weight of $\rho_{\mathfrak{f}}$ is defined as the composite

$$\mathcal{W}t^*\rho_{\mathfrak{f}} : \Lambda \xrightarrow{\mathcal{W}t} W(\mathbb{F}_q)[|U|] \xrightarrow{\mathfrak{f}} R$$

and that $\mathcal{W}t(T) = \det\tilde{\varrho}$. Let $\Omega(R) \subseteq \mathrm{Hom}_{\mathfrak{C}}(\Lambda, R)$ be the subset of weights which are congruent to the weight of the prescribed deformation

$$\Omega(R) := \{\lambda \in \mathrm{Hom}_{\mathfrak{C}}(\Lambda, R) \mid \lambda \equiv \mathcal{W}t^*\rho_2 \mod (pR \cap \mathfrak{m}_R^2)\}.$$

We observe that since $\mathcal{W}t \in \Omega(W(\mathbb{F}_q)[|U|])$, it follows that $\mathcal{W}t^*\rho_{\mathfrak{f}} \in \Omega(R)$. Let $\lambda \in \Omega(R)$, we show that there exists a deformation $\varrho^\lambda \in \mathcal{D}ef_\Phi(R)$ with weight $\mathcal{W}t^*\varrho^\lambda = \lambda$. We refer to the proof of Theorem 4.1.1 to the choice of the set of primes X, these are chosen so that the dual Selmer group of the fixed weight Selmer conditions is zero. We fix the weight λ and examine if ρ_2 has a deformation to $\mathcal{D}ef_\Phi(R)$. Standard techniques in deformation theory discussed in this manuscript (cf. [9]) imply that a lift does indeed exist provided (fixed weight) dual Selmer group

$$H^1_{\mathcal{N}^\perp}(\mathrm{G}_{\mathbb{Q},S\cup X}, \mathrm{Ad}^0\,\bar{\rho}^*) = 0.$$

This concludes the proof of Theorem 4.1.1. □

CHAPTER 5

CONSTRUCTING CERTAIN SPECIAL GALOIS EXTENSIONS

5.1 Introduction

Let p be a prime number, the tame Fontaine-Mazur conjecture (conjecture 5a in [6]) posits that an infinite Galois extension of a number field K whose Galois group over K is isomorphic to a p-adic analytic group is either ramified at infinitely many primes or is infinitely ramified at a prime dividing p. It is natural to ask if such extensions exist once we pass up an infinite cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})$. In this chapter, we show that there are abundantly many primes p for which there exists such a Galois extension of $\mathbb{Q}(\mu_{p^\infty})$ whose Galois group is isomorphic to a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ with tame ramification above finitely many rational primes and unramified at primes above p.

Let $p \geq 5$ be a prime and let μ_p denote the set of p-th roots of unity. Let $\zeta_p \in \mu_p$ be a primitive p-th root of unity. Denote by $H'_{\mathbb{Q}(\mu_p)}$ the p-Hilbert Class field of $\mathbb{Q}(\mu_p)$, we identify $\mathrm{Gal}(H'_{\mathbb{Q}(\mu_p)}/\mathbb{Q}(\mu_p))$ with the p-part of the class group $\mathrm{Cl}(\mathbb{Q}(\mu_p))$.

Associate a Galois representation to class group data. Denote by

$$\mathcal{C} := \mathrm{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p$$

and $\bar{\chi}$ the mod p cyclotomic character. The Galois module $\mathcal{C}$ decomposes into isotypic components

$$\mathcal{C} = \bigoplus_{i=0}^{p-2} \mathcal{C}(\bar{\chi}^i),$$

where

$$\mathcal{C}(\bar{\chi}^i) = \{x \in \mathcal{C} \mid g \cdot x = \bar{\chi}^i(g)x \text{ for all } g \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})\}. \tag{5.1}$$

By class field theory, an $\mathbb{F}_p$-line in $\mathcal{C}(\bar{\chi}^i)$ gives rise to an extension $L/\mathbb{Q}$ contained in the p-Hilbert Class field $H'_{\mathbb{Q}(\mu_p)}$. Since such a line is Galois stable, the extension L is Galois over $\mathbb{Q}$. Any choice of isomorphism $\mathrm{Gal}(L/\mathbb{Q}(\mu_p)) \xrightarrow{\sim} \mathbb{F}_p$ gives rise to an element

$$\beta \in H^1\left(G_{\mathbb{Q}}, \mathbb{F}_p(\bar{\chi}^i)\right) \simeq \mathrm{Hom}\left(G_{\mathbb{Q}(\mu_p)}, \mathbb{F}_p(\bar{\chi}^i)\right)^{\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})}.$$

This class does not depend on the choice of isomorphism. The class β coincides with a reducible Galois representation

$$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

defined by $\bar{\rho} = \begin{pmatrix} \bar{\chi}^i & \beta \\ 0 & 1 \end{pmatrix}$. The representation satisfies a number of conditions:

1. $\bar{\rho}_{\restriction G_{\mathbb{Q}(\mu_p)}}$ is indecomposable,
2. $\bar{\rho}_{\restriction G_{\mathbb{Q}(\mu_p)}} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ is unramified at every prime,
3. the local Galois representation at p splits into a sum of characters $\bar{\rho}_{\restriction \mathrm{G}_p} \simeq \begin{pmatrix} \bar{\chi}^i_{\restriction \mathrm{G}_p} & 0 \\ 0 & 1 \end{pmatrix}$.

The extension $L \neq \mathbb{Q}(\mu_p)$ and thus the cohomology class β is non-trivial, from which condition 1 follows. As L is contained in the Hilbert class field of $\mathbb{Q}(\mu_p)$ every prime of $\mathbb{Q}(\mu_p)$ is unramified in L. Condition 2 follows from this. By class field theory the principal prime-ideal $(1-\zeta_p)$ is split in the Hilbert class field of $\mathbb{Q}(\mu_p)$ and thus in L. Let E denote the completion of $\mathbb{Q}(\mu_p)$ at $(1-\zeta_p)$. One deduces that $\beta_{\restriction G_E} \in H^1(G_E, \mathbb{F}_p(\bar{\chi}^i))$ is trivial. We observe that the order of Gal$(E/\mathbb{Q}_p)$ is coprime to p. From a standard argument appealing to the vanishing of $H^1(\text{Gal}(E/\mathbb{Q}_p), \mathbb{F}_p(\bar{\chi}^i))$ and the inflation-restriction sequence it follows that $\beta_{\restriction \mathrm{G}_p} = 0$. Condition 3 follows as a consequence.

We examine deformations of $\bar{\rho}$ with some prescribed local properties. In particular, the local deformation condition at p should ensure that on passing up the infinite cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})$, our deformations are unramified at primes $\mathfrak{p}|p$.

The construction is based on that of Hamblen and Ramakrishna. Their method is based on a local to global deformation theoretic argument. Implicit to this construction is a choice of a local deformation condition at each prime at which the residual representation is allowed to ramify. Deformations of the residual representation are to satisfy these local conditions. In particular, at p there is a choice of a local deformation condition which is liftable and balanced.

Theorem 5.1.1. *Let $p \geq 5$ be a prime and $\mathcal{C} := \mathrm{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p$. Suppose that there exists an odd integer $i \neq \frac{p-1}{2}$ such that $2 \leq i \leq p-3$ such that $\mathcal{C}(\bar{\chi}^i) \neq 0$. Let* $\bar{\rho} = \begin{pmatrix} \bar{\chi}^i & * \\ 0 & 1 \end{pmatrix}$

be the Galois representation associated to an $\mathbb{F}_p$-line in $\mathcal{C}(\bar{\chi}^i)$. There exist infinitely many lifts ρ of $\bar{\rho}$

$$\begin{array}{ccc} & & GL_2(\mathbb{Z}_p) \\ & \overset{\rho}{\nearrow} & \downarrow \\ G_{\mathbb{Q}} & \xrightarrow[\bar{\rho}]{} & GL_2(\mathbb{F}_p), \end{array}$$

such that the following conditions are satisfied

- *$\rho(G_{\mathbb{Q}(\mu_{p^\infty})})$ contains the principal congruence subgroup of $SL_2(\mathbb{Z}_p)$*
- *the determinant of ρ is $\chi^{i+p^2(p-1)}$*
- *$\rho_{\restriction \mathrm{G}_p}$ is a direct sum of characters $\rho_{\restriction \mathrm{G}_p} = \varphi_1 \oplus \varphi_2$. In particular, ρ is abelian at I_p.*
- *ρ is unramified outside a finite set of primes.*

The lift ρ gives rise to an extension $\mathbb{Q}(\rho)$ of $\mathbb{Q}(\mu_{p^\infty})$ which is taken to be the fixed field of ker$\rho \subset G_{\mathbb{Q}}$. This extension is unramified at primes above p. Furthermore, at a prime $l \neq p$, since the residual representation $\bar{\rho}$ is unramified, the lift ρ is tamely ramified at all primes $l \in S/\{p\}$, we are left with the following result.

Corollary 5.1.2. *Suppose that $p \geq 5$ be a prime and $i \neq \frac{p-1}{2}$ an odd integer between $2 \leq i \leq p-3$ for which the isotypic space $\mathcal{C}(\bar{\chi}^i) \neq 0$ (cf. 5.1). There are infinitely many Galois extensions $F/\mathbb{Q}(\mu_{p^\infty})$ for which*

- *the Galois group Gal$(F/\mathbb{Q}(\mu_{p^\infty}))$ topologically isomorphic to a subgroup of $SL_2(\mathbb{Z}_p)$ which contains the principal congruence subgroup.*

- *F is unramified at primes above p and ramified above finitely many rational primes at which it is tamely ramified.*

Proposition 5.1.3. *The conclusion of Corollary 5.1.2 is satisfied at any prime p such that*

1. *$p \geq 5$,*
2. *p is irregular,*
3. *$p \equiv 1 \mod 4$,*
4. *p does not divide the class number of the totally real subfield $\mathbb{Q}(\mu_p)^+ \subset \mathbb{Q}(\mu_p)$, i.e. Vandiver's conjecture is satisfied at p.*

This seems to indicate that there are infinitely many primes at which p the implication of Corollary 5.1.2 is satisfied.

Such p-adic extensions F were first constructed by Ohtani [17] and Blondeau [1] and their methods relied on lifting suitable irreducible Galois representations which are *extraordinary* at p. The construction in [17] and [1] relies on the existence of an eigenform f with *companion forms* (and thus extraordinary at p) such the image of the residual representation $\bar{\rho}_f$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. Computations for $p < 3500$ show that there are precisely four primes $107, 139, 271$ and 379 for which such an eigenform f exists.

5.2 Lifting to Characteristic Zero

We proceed to describe the local deformation condition at p which will in particular ensure that our deformations are unramified over $\mathbb{Q}(\mu_{p^\infty})$ at all primes $\mathfrak{p}|p$.

Definition 5.2.1. *Let $\mathcal{F}_p : \mathcal{C}_{\mathbb{Z}_p} \to$ Sets be the functor of deformations of $\bar{\rho}$ which consist of a sum of two characters, we refer deformations $\mathcal{F}_p$ as diagonal. In greater detail, $\mathcal{F}_p(R)$ consists of deformations $\rho_R : \mathrm{G}_p \to \mathrm{GL}_2(R)$ of $\bar{\rho}$ such that*

- $\rho_{\restriction \mathrm{G}_p} \simeq \varphi_1 \oplus \varphi_2$ *where φ_1 and φ_2 are two characters (possibly ramified)*
- $\det \rho = \chi^{i+p^2(p-1)}$.

The tangent space $\mathcal{N}_p$ is defined as the set of deformations of $\bar{\rho}$ to the dual numbers $\mathcal{F}_p(\mathbb{F}_p[\epsilon])$ which has a natural structure of an $\mathbb{F}_p$ vector space and is realized as a subspace of $H^1(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho})$.

The functor $\mathcal{F}_p$ is a liftable deformation condition. Observe that since G_p acts diagonally, the 1 dimensional space Diag$(\bar{\rho}_{\restriction \mathrm{G}_p})$ is a summand of $\mathrm{Ad}^0 \bar{\rho}_{\restriction \mathrm{G}_p}$ and

$$Ad^0 \bar{\rho}_{\restriction \mathrm{G}_p} \simeq \mathbb{F}_p(\bar{\chi}^i_{\restriction \mathrm{G}_p}) \oplus \text{Diag}(\bar{\rho}_{\restriction \mathrm{G}_p}) \oplus \mathbb{F}_p(\bar{\chi}^{-i}_{\restriction \mathrm{G}_p}).$$

Definition 5.2.2. *Let $\mathcal{F}$ be a deformation condition for $\bar{\rho}_{\restriction \mathrm{G}_p}$ with tangent space $\mathcal{N}_p$.*

- *The deformation condition $\mathcal{F}$ is balanced if*

$$\dim \mathcal{N}_p = \dim H^0(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho}) + 1 = 2.$$

Proposition 5.2.3. *The deformation condition $\mathcal{F}_p$ is liftable and balanced.*

Proof. That $\mathcal{F}_p$ is liftable follows from Lemma 4.5 of [1]. We show that it is balanced, i.e. we deduce that

$$\dim \mathcal{N}_p = \dim H^0(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho}) + 1 = 2.$$

Explicitly, $\mathcal{N}_p$ is the set of elements $X \in H^1(\mathrm{G}_p, \mathrm{Ad}^0 \bar{\rho})$ for which the twist $\bar{\rho}(Id + \epsilon X)$ is diagonal, we deduce that $\mathcal{N}_p = H^1(\mathrm{G}_p, \mathrm{Diag}(\bar{\rho}))$.

Since $\bar{\chi}^i_{\restriction \mathrm{G}_p} \neq 1$,

$$\begin{aligned}
&\dim H^0(\mathrm{G}_p, Ad^0 \bar{\rho}) \\
&= \dim H^0(\mathrm{G}_p, \mathbb{F}_p(\bar{\chi}^i)) + \dim H^0(\mathrm{G}_p, \mathbb{F}_p) + \dim H^0(\mathrm{G}_p, \mathbb{F}_p(\bar{\chi}^{-i})) \\
&= 1.
\end{aligned}$$

We employ the Euler characteristic formula and local duality to compute $\dim \mathcal{N}_p$

$$\begin{aligned}
\dim \mathcal{N}_p &= \dim H^1(\mathrm{G}_p, \mathrm{Diag}(\bar{\rho})) \\
&= 1 + \dim H^0(\mathrm{G}_p, \mathrm{Diag}(\bar{\rho})) + \dim H^2(\mathrm{G}_p, \mathrm{Diag}(\bar{\rho})) \\
&= 1 + \dim H^0(\mathrm{G}_p, \mathbb{F}_p) + \dim H^0(\mathrm{G}_p, \mathbb{F}_p(\bar{\chi})) \\
&= \dim H^0(\mathrm{G}_p, Ad^0 \bar{\rho}) + 1 = 2.
\end{aligned}$$

□

The assumptions on $\bar{\rho}$ satisfy those on the assumptions laid out on the residual representations examined in [9].

Lemma 5.2.4. *The conditions stipulated in [9, Theorem 2] are satisfied by the representation $\bar{\rho}$.*

Proof. The reducible representation $\bar{\rho} = \begin{pmatrix} \phi & * \\ 0 & 1 \end{pmatrix}$ with $\phi = \bar{\chi}^i$, we recall that $i \neq (p-1)/2$ is odd and $2 \leq i \leq p-3$. We enumerate the six conditions and show that they are satisfied:

- Condition (0) is satisfied since $p \neq 2$.
- Condition (1) requires that $\bar{\rho}$ is indecomposable (or in other words, not semi-simple), this follows by construction as the extension $L/\mathbb{Q}(\mu_p)$ is a non-trivial extension.
- Condition (2) requires that $\phi^2 \neq 1$, or equivalently, $2i \not\equiv 0 \bmod (p-1)$ which is satisfied.
- Condition (3) requires that $\phi \neq \bar{\chi}^{\pm 1}$ which follows from the assumption on i.
- Condition (4) is automatically satisfied since the field in question $\mathbb{F}_q$ is $\mathbb{F}_p$.
- Since i is odd, $\bar{\rho}$ is odd. Condition (5) requires that $\bar{\rho}$ that $\bar{\rho}_{\restriction \mathrm{G}_p}$ is not unramified of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ (where $*$ may be trivial). The integer i is not divisible by $p-1$ and as a consequence, this condition is satisfied.

$\square$

In the proof of Theorem $5.1.1$, the following Lemma is applied in deducing that the image of a suitably constructed lift ρ of $\bar{\rho}$ contains the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$.

Lemma 5.2.5. *Let $p \geq 5$ be a prime, X be a closed subgroup of $SL_2(\mathbb{Z}_p)$ and let X_2 be the image of X in $SL_2(\mathbb{Z}/p^2\mathbb{Z})$. Suppose that X_2 contains the principal congruence subgroup of $SL_2(\mathbb{Z}/p^2\mathbb{Z})$, then X contains the principal congruence subgroup of $SL_2(\mathbb{Z}_p)$.*

Proof. The proof follows from that of Lemma 3 in [27, Chapter 4, Section 3.4] with very little modification. □

Proof. (of Theorem $5.1.1$)

This result shall follow from the main result of [9] after a single modification is made to their construction. Their method relies on the existence of a balanced liftable deformation condition at each prime at which the residual Galois representation is allowed to ramify. There are cohomological obstructions to lifting a residual Galois representation which satisfies these local conditions. More specifically if a certain *Selmer group* does vanish the local to global deformation theoretic construction can be applied. On adjoining some auxiliary deformation conditions at a finite set of *trivial primes* (cf. Definition 12 in [9]) the associated Selmer group can be shown to vanish (cf. Proposition 46 in [9]). Hamblen and Ramakrishna work throughout with the ordinary deformation condition (cf. [23] and [28]) at p. Instead, we shall prescribe the diagonal deformation condition which is also a balanced and liftable deformation. This was established in Proposition $5.2.3$. The construction of Hamblen and Ramakrishna does not in any specific way utilize the ordinary deformation condition and the diagonal deformation condition may as well be used in its place since this condition is also liftable and balanced. It follows that there are infinitely many characteristic zero deformations ρ satisfying the conditions of the main theorem.

In greater detail, it is a consequence of Proposition 42 of [9] that

$$\text{image}\{\rho(G_{\mathbb{Q}(\mu_{p^\infty})}) \to \mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})\}$$

contains the principal congruence subgroup. It follows from Lemma $5.2.5$ that $\rho(G_{\mathbb{Q}(\mu_{p^\infty})})$ contains the principal congruence subgroup in $\mathrm{SL}_2(\mathbb{Z}_p)$. □

Proof. (of Corollary 5.1.2)

Let ρ be a lift of $\bar{\rho}$ satisfying the conditions of Theorem $5.1.2$. We let F be the fixed field of ρ. The infinite cyclotomic field $\mathbb{Q}(\mu_{p^\infty})$ is the fixed field of $\det\rho = \chi^{i+p^2(p-1)}$. Since $\rho(G_{\mathbb{Q}(\mu_{p^\infty})})$ contains the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ we see that $\mathrm{Gal}(F/\mathbb{Q}(\mu_{p^\infty}))$ is topologically isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ which contains the principal congruence subgroup.

The local representation $\rho_{\restriction \mathrm{G}_p}$ is a sum of characters φ_1 and φ_2, we deduce that F is unramified at all primes above p.

Since $\bar{\rho}_{\restriction G_{\mathbb{Q}(\mu_p)}}$ is unramified at all primes, it follows that at the primes at which F is ramified, F must be tamely ramified. □

Proof. (of Proposition 5.1.3)

Indeed if p is such a prime, since p is irregular, the quotient $\mathcal{C} = \mathrm{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p \neq 0$. By assumption each even eigenspace $\mathcal{C}(\bar{\chi}^{2j}) = 0$. Thus there exists an odd integer $1 \leq i \leq p-2$ for which $\mathcal{C}(\bar{\chi}^i) \neq 0$. Since $p \equiv 1 \mod 4$, and i is odd, we have that $i \neq \frac{p-1}{2}$. On the other hand, $i \neq 1$ since $\mathcal{C}(\bar{\chi}) = 0$ (cf. Proposition 6.16 of [30]). By Herbrand's theorem implies that p divides the numerator of the Bernoulli number B_{p-i}. Since $B_2 = \frac{1}{6}$ we deduce that $i \neq p-2$ and thus lies in the range $2 \leq i \leq p-3$. □

BIBLIOGRAPHY

[1] J. Blondeau, Lifting of nearly extraordinary Galois representations, J. Number Theory 133.6 (2013) 2066-2082.

[2] Booher, Jeremy. ”Geometric deformations of orthogonal and symplectic galois representations.” arXiv preprint arXiv:1612.04237 (2016).

[3] Brinon, O., and B. Conrad. ”p-adic Hodge theory, notes from the 2009 Clay Mathematics Institute summer school.”

[4] Fakhruddin, Najmuddin, Chandrashekhar Khare, and Stefan Patrikis. ”Lifting irreducible Galois representations.” arXiv preprint arXiv:1810.05803 (2018).

[5] Fakhruddin, Najmuddin, Chandrashekhar Khare, and Stefan Patrikis. ”Relative deformation theory and lifting irreducible Galois representations.” arXiv preprint arXiv:1904.02374 (2019).

[6] Fontaine, Jean-Marc, and Barry Mazur. ”Geometric Galois representations.” Elliptic curves, modular forms, and Fermat’s last theorem (Hong Kong, 1993), Ser. Number Theory, I (1995): 41-78.

[7] Gross, Benedict, and Ch VI. ”Odd galois representations.” preprint (2007).

[8] Hall, Brian. Lie groups, Lie algebras, and representations: an elementary introduction. Vol. 222. Springer, 2015.

[9] Hamblen, Spencer, and Ravi Ramakrishna. ”Deformations of certain reducible Galois representations, II.” American journal of mathematics 130.4 (2008): 913-944.

[10] Humphreys, James E. Introduction to Lie algebras and representation theory. Vol. 9. Springer Science and Business Media, 2012.

[11] Khare, Chandrashekhar, Michael Larsen, and Ravi Ramakrishna. ”Constructing semisimple p-adic Galois representations with prescribed properties.” American Journal of Mathematics 127.4 (2005): 709-734.

[12] Khare, Chandrashekhar and Ramakrishna, Ravi. "Lifting torsion Galois representations". In: Forum Math. Sigma 3 (2015), e14, 37.

[13] Khare, Chandrashekhar, and Jean-Pierre Wintenberger. "Serre's modularity conjecture (II)." Inventiones mathematicae 178.3 (2009): 505.

[14] Kisin, Mark. "The Fontaine-Mazur conjecture for GL_2" Journal of the American Mathematical Society 22.3 (2009): 641-690.

[15] Mazur, Barry. "Deforming galois representations." Galois Groups over $\mathbb{Q}$. Springer, New York, NY, 1989. 385-437.

[16] Neukirch, Jürgen, Alexander Schmidt, and Kay Wingberg. Cohomology of number fields. Vol. 323. Springer Science and Business Media, 2013.

[17] Ohtani, Deformations of locally abelian Galois representations and unramified extensions, J. Number Theory 120.2 (2006) 272-286.

[18] Patrikis, Stefan. Lifting symplectic galois representations. Diss. Harvard College, 2006.

[19] Patrikis, Stefan. "Deformations of Galois representations and exceptional monodromy." Inventiones mathematicae 205.2 (2016): 269-336.

[20] Skinner, Christopher M., and Andrew J. Wiles. "Residually reductible representations and modular forms." Publications Mathématiques de l'IHÉS 89 (1999): 5-126.

[21] Ribet, Kenneth A. "A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$." Invent. math 34.3 (1976): 151-162.

[22] Ribet, Kenneth A. "Report on mod l representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$." Proceedings of Symposia in Pure Mathematics. Vol. 55. No. 2. 1994.

[23] Ramakrishna, Ravi. "Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur." Annals of mathematics 156.1 (2002): 115-154.

[24] Ramakrishna, Ravi. and Ray, Anwesh. ”Level Optimization in the Ordinary Case via Deformation theory of Galois Representations” (preprint).

[25] Ramakrishna, Ravi. ”Lifting Galois representations.” Inventiones mathematicae 138.3 (1999): 537-562.

[26] Ramakrishna, Ravi. ”Maps to weight space in Hida families.” Indian Journal of Pure and Applied Mathematics 45.5 (2014): 759-776.

[27] J.-P. Serre, Abelian l-adic representations and elliptic curves, AK Peters/CRC Press (1997).

[28] R. Taylor, On icosahedral Artin representations, II, Amer. J. Math. 125.3 (2003) 549-566.

[29] Taylor, Richard. ”Remarks on a conjecture of Fontaine and Mazur.” Journal of the Institute of Mathematics of Jussieu 1.1 (2002): 125-143.

[30] L. Washington, Introduction to Cyclotomic Fields , 2nd edition, Grad. Texts in Math. , vol. 83, Springer- Verlag, Berlin, 1997.