AN INVERSE GALOIS DEFORMATION PROBLEM

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

Taoran Chen

August 2018

AN INVERSE GALOIS DEFORMATION PROBLEM

Taoran Chen, Ph.D.

Cornell University 2018

Suppose $\bar{\rho} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\mathbf{k})$ is a residual Galois representation satisfying several mild conditions, where F is a number field and $\mathbf{k}$ is a finite field with characteristics $p \geq 7$. In this work, we show that for any finite flat reduced complete intersection over $W(\mathbf{k})$, $\mathcal{R}$, we can construct a deformation problem defined by local conditions imposed on some finite set of places in F, such that the corresponding universal deformation ring of $\bar{\rho}$ is $\mathcal{R}$. It's a theorem of Wiles that if the local conditions are chosen to express restriction to deformations coming from modular forms, then the corresponding universal deformation ring is a finite flat reduced complete intersection, so our work can be regarded as a converse to Wiles' result.

BIOGRAPHICAL SKETCH

Taoran Chen was born in Guangzhou, China. In 2012, he graduated from MIT with a Bachelor of Science degree in Mathematics. In the same year, he joined the Mathematics Department at Cornell University to pursue his PhD degree.

To my parents

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my advisor, Ravi Ramakrishna, for introducing me to the subject, giving helpful suggestions to and polishing up my thesis. This dissertation could not have come into to being without his guidance. It is a privilege to have a mentor with such immense amount of knowledge, patience and goodwill.

I would also like to thank my family, especially my parents and girlfriend ♡, for their unconditional support on my decision in pursuing a mathematical career, and for their endurance of my absence.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The purpose of this dissertation is to investigate the following problem: Given a residual Galois representation $\bar{\rho} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\mathbf{k})$ and a complete noetherian local ring $\mathcal{R}$ over the ring of Witt vectors $W(\mathbf{k})$, can one realize $\mathcal{R}$ as the universal deformation ring defined by local conditions imposed on a finite set of places? It's largely proven that if the local conditions are chosen to resemble those coming from modular forms, then the corresponding universal deformation ring is a reduced finite flat complete intersection. We give an affirmative answer to the proposed question under some mild assumptions on $\bar{\rho}$ and the assumption that $\mathcal{R}$ is a finite flat reduced complete intersection. It's worthwhile to point out that our approach is purely deformation-theoretic and does not rely on modularity assumption on $\bar{\rho}$. Our work is heavily inspired by [7].

The outline of this work is as follows. In Chapter 1, we start by giving a utilitarian introduction to deformation theory of Galois representation and it's connection with Galois cohomology. In Chapter 2, we develop a ring-theoretic result which roughly says that two Noetherian complete local rings are isomorphic, provided they look close enough. Finally, we describe our allowable local conditions, state and prove the main result 3.3.1 in Chapter 3, utilizing the result proven in the previous Chapter.

1.1 Deformations of Galois Representations

Fix for the rest of this chapter a prime number p and a finite field $\mathbf{k}$ of characteristic p.

Let F be number field with absolute Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$. Let S be a finite set of places of F which contains all of those dividing p and ∞. Denote by F_S the maximal algebraic extension of F unramified outside S and let $G_{F,S} = \mathrm{Gal}(F_S/F)$. For each place $v \in S$, define $G_v = \mathrm{Gal}(\overline{F}_v/F_v)$. An embedding of $\overline{F}$ into $\overline{F}_v$ gives a continuous homomorphism $G_v \to G_{F,S}$. Let G be either $G_{F,S}$ or G_v and let $\overline{\rho} : G \to \mathrm{GL}_2(\mathbf{k})$ be a continuous representation.

Define $\mathcal{C}$ as the category of noetherian local rings with residue field $\mathbf{k}$, whose morphisms are local ring homomorphisms inducing the identity on the residue fields. The objects and morphisms of $\mathcal{C}$ will be referred to as *coefficient rings* and *coefficient ring homomorphisms*. Note that coefficient rings are necessarily algebras over $W(\mathbf{k})$, the ring of Witt vectors.

Suppose R is a coefficient ring with maximal ideal $\mathfrak{m}_R$, we define its *cotangent space* to be the $\mathbf{k}$-vector space

$$t_R^* := \mathfrak{m}_R/(\mathfrak{m}_R^2 + pR).$$

We call the $\mathbf{k}$-dual of t_R^* the *tangent space* of R:

$$t_R := \mathrm{Hom}_{\mathbf{k}-\mathrm{v.sp}}(t_R^*, \mathbf{k}).$$

Let R be an object of $\mathcal{C}$. Two lifts $\rho_1, \rho_2 : G_{F,S} \to \mathrm{GL}_2(R)$ of $\overline{\rho}$ to R are said to be strictly equivalent if there exists $M \in \ker\{\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbf{k})\}$ such that $\rho_2 = M\rho_1 M^{-1}$. A strict equivalence class of lifts of $\overline{\rho}$ to R is called a *deformation*.

We define the deformation functor $\mathrm{Def}_{\overline{\rho}} : \mathcal{C} \to \mathrm{Sets}$ by:

$$\mathrm{Def}_{\overline{\rho}}(R) = \{\text{deformations of } \overline{\rho} \text{ to } R\}. \tag{1.1}$$

Mazur has shown

Theorem 1.1.1. *Given a continuous homomorphism $\overline{\rho} : G \to \mathrm{GL}_2(\mathbf{k})$, the deformation functor $Def_{\overline{\rho}}$ has a hull. In other words, there exists $R^{ver} \in \mathcal{C}$ and a deformation $\rho^{ver} : G \to \mathrm{GL}_2(R^{ver})$ of $\overline{\rho}$ to R^{ver} such that if $\rho_R : G \to \mathrm{GL}_2(R)$ is a deformation of $\overline{\rho}$ to $R \in \mathcal{C}$, then there is a morphism $\phi : R^{ver} \to R$ such that $\rho = \phi \circ \rho^{ver}$. Moreover, if $\overline{\rho}$ is absolutely irreducible, then ϕ is unique.*

In the later case, we can denote R^{ver} by R^{uni} to emphasize universality. We call R^{ver} (R^{uni}, resp.) the *versal* (*universal*, resp.) *deformation ring.*

At times we will restrict our interest to deformations of $\overline{\rho}$ that satisfy certain conditions. A subfunctor $\mathcal{D} \subset \mathrm{Def}_{\overline{\rho}}$ is called a *deformation condition* if it is representable by a quotient of R^{ver}, which we denote by $R_{\mathcal{D}}$. We call $R_{\mathcal{D}}$ the (uni)versal deformation ring associated to the deformation condition $\mathcal{D}$.

Example 1.1.2. As an example, "having fixed determinant" defines a deformation condition. More precisely, let $\phi : G \to W(\mathbf{k})^*$ be a lift of $\det \overline{\rho} : G \to \mathbf{k}^*$. For $R \in \mathcal{C}$, we say that a deformation $\rho_R : G \to \mathrm{GL}_2(R)$ has determinant ϕ if $\det \rho_R$ is the same as the composition $G \xrightarrow{\phi} W(\mathbf{k})^* \to R^*$, where the latter map comes from the natural $W(\mathbf{k})$-algebra structure of R. The subfuntor $\mathrm{Def}^{\phi}_{\overline{\rho}} \subset \mathrm{Def}_{\overline{\rho}}$ defined by

$$\mathrm{Def}^{\phi}_{\overline{\rho}}(R) = \{\text{deformations of } \overline{\rho} \text{ to } R \text{ with determinant } \phi\}$$

is a deformation condition. It is representable by

$$R^{\phi} := R^{\mathrm{ver}}/I, \tag{1.2}$$

where I is the ideal of R generated by the elements $\det \rho^{\mathrm{ver}}(g) - \phi(g)$ for all $g \in G$.

1.2 Galois Cohomology

In this section, we collect some standard results from Galois cohomology, whose proofs can be found in [10], [11] and [21] unless otherwise specified.

Let G be either $G_{F,S}$ or G_v as in the last section and let X be a $\mathbf{k}[G]$-module. By convention, $\mathbf{k}$ itself is a $\mathbf{k}[G]$-module with trivial G-action. By $\mathbf{k}(\phi)$ we mean the twist of $\mathbf{k}$ by a charater ϕ on G. In most of our applications, ϕ will be taken to be a power of the p-adic cyclotomic charater χ. Define $X^* := \mathrm{Hom}_{\mathbf{k}}(X, \mathbf{k}(\chi))$ to be the dual of X. It's again a $\mathbf{k}[G]$-module via $(gx^*)(x) = g(x^*(g^{-1}x))$.

For a $\mathbf{k}[G]$-module X, let

$$X^G := \{x \in X \mid \sigma x = x \text{ for all } g \in G\}.$$

Define the cohomology groups $H^n(G, X)$ to be the right derived functors of the functor $\{\mathbf{k}[G] - \text{module}\} \to \{\text{abelian groups}\}$ given by $X \mapsto X^G$. Explicitly,

$$H^0(G, X) = X^G$$

$$H^1(G, X) = \frac{\{c : G \to X \mid c(g_1g_2) - g_1c(g_2) - c(g_1) = 0 \text{ for all } g_1, g_2 \in G\}}{\{b : G \to X \mid b(g) = gx - x \ \text{ for some } x \in X\}}$$

$$H^2(G, X) = \frac{\left\{\begin{array}{c} c : G \times G \to X \mid c(g_1, g_2g_3) - c(g_1g_2, g_3) + g_1c(g_2, g_3) - c(g_1, g_2) = 0 \\ \text{for all } g_1, g_2, g_3 \in G \end{array}\right\}}{\{b : G \times G \to X \mid b(g_1, g_2) = h(g_1g_2) - g_1h(g_2) - h(g_1) \text{ for some } h : G \to X\}}$$

The maps c, b in the expressions above are called *cocycles* and *coboundaries* respectively.

For finite place v of F, define

$$H^1_{\mathrm{nr}}(G_v, X) := H^1(G_v/I_v, X^{I_v}) \simeq \ker(H^1(G_v, X) \to H^1(I_v, X)),$$

where I_v is the inertial subgroup. We have

Lemma 1.2.1. $\#H^1_{nr}(G_v, X) = \#H^0(G_v, X)$.

Proof. See lemma 19 in [21]. □

The proof of the next two theorems can be found in Chapter 1 of [12].

Theorem 1.2.2 (Local Tate Duality)**.** *Let v be a finite prime of F and let X be a finite $\mathbf{k}[G_v]$-module. Then $H^i(G_v, X)$ are finite for all $i \geq 0$ and $= 0$ for $i \geq 3$. For $i = 0, 1, 2$, the cup product with respect to the natural homomorphism $X \otimes X^* \to \mathbf{k}(\chi)$ gives a perfect pairing*

$$H^i(G_v, X) \times H^{2-i}(G_v, X^*) \to H^2(G_v, \mathbf{k}(\chi)) \simeq \mathbf{k}.$$

If $v \nmid p$, the unramified classes $H^1_{nr}(G_v, X)$ and $H^1_{nr}(G_v, X^*)$ are exact annihilators of each other under the above pairing for $i = 1$.

Theorem 1.2.3 (Local Euler Characteristic)**.** *Let v be a finite prime of F and let X be a finite $\mathbf{k}[G_v]$-module. Then*

1. $\#H^1(G_v, X) = \#H^0(G_v, X)\#H^2(G_v, M)$ *if* $v \nmid p$;
2. $\#H^1(G_v, X) = \#H^0(G_v, X)\#H^2(G_v, M)p^{[F_v:\mathbb{Q}_p]v_p(\#M)}$.

For the remainder of this section, suppose $\overline{\rho} : G \to \mathrm{GL}_2(\mathbf{k})$ is an absolutely continuous irreducible representation whose associated universal deformation ring is R^{uni}. Let $\mathrm{Ad}\,\overline{\rho}$ denote the galois module of 2×2 matrices with entries in $\mathbf{k}$, with G-action through conjugation by $\overline{\rho}$. Define $\mathbf{k}[\epsilon] \in \mathcal{C}$ to be the algebra generated by the relation $\epsilon^2 = 0$. The following theorem develops the first connection between deformation theory and Galois cohomology.

Theorem 1.2.4. *There is a natural isomorphism of* $\mathbf{k}$*-vector spaces*

$$H^1(G, \operatorname{Ad}\overline{\rho}) \simeq \operatorname{Def}_{\overline{\rho}}(\mathbf{k}[\epsilon]) \simeq \operatorname{Hom}_{\mathcal{C}}(R^{uni}, \mathbf{k}[\epsilon]) \simeq t_{R^{uni}} \tag{1.3}$$

Moreover, R^{uni} *can be written as a quotient of the power series ring over* $W(\mathbf{k})$ *in* $\dim_{\mathbf{k}} H^1(G, \operatorname{Ad}\overline{\rho})$ *variables by an ideal minimally generated by at most* $\dim_{\mathbf{k}} H^2(G, \operatorname{Ad}\overline{\rho})$ *elements.*

Proof. The last assertion concerning the number of relations is due to Böckle [2, Theorem 2.4]. The rest goes back to Mazur's original article [10]. We only remind the readers that the correspondence $H^1(G, \operatorname{Ad}\overline{\rho}) \simeq \operatorname{Def}_{\overline{\rho}}(\mathbf{k}[\epsilon])$ is given by $f \mapsto (I + \epsilon f)\overline{\rho}$. □

We will refer to any of the isomorphic spaces in (1.3) as the tangent space of the deformation functor $\operatorname{Def}_{\overline{\rho}}$.

Suppose $A_1 \to A_0$ is a surjection of coefficient rings with kernel J annihilated by $\mathfrak{m}_{A_1}$, then J is a $\mathbf{k}$-vector space. Such surjection is referred to as *small extension.* In fact, one can show that any surjective coefficient rings map can be broken down into composition of index-$\#\mathbf{k}$ small extensions. We have

Theorem 1.2.5. *Suppose* $A_1 \to A_0$ *is a small extension with kernel* J *and let* $\rho_0 : G \to \mathrm{GL}_2(A_0)$ *be a deformation of (the absolutely irreducible)* $\overline{\rho}$ *to* A_0*. Then there is a canonical cohomology class* $c \in H^2(G, J \otimes \operatorname{Ad}\overline{\rho}) = H^2(G, \operatorname{Ad}\overline{\rho}) \otimes J$ *that depends only on* ρ_0*, which vanishes if and only if there is a deformation* ρ_1 *of* $\overline{\rho}$ *to* A_1 *that lifts* ρ_0*.*

If $c = 0$*, then the set of deformations of* $\overline{\rho}$ *to* A_1 *that lifts* ρ_0 *is a principal homogeneous space under the action of* $H^1(G, J \otimes \operatorname{Ad}\overline{\rho})$*. For* $f \in H^1(G, J \otimes \operatorname{Ad}\overline{\rho})$ *and* ρ_1 *lifting* ρ_0*, the action of* f *on* ρ_1 *is given by* $f \cdot \rho_1 = (I + f)\rho_1$*.*

Proof. See section 1.6 of [9] for an explicit description of c and the proof of this theorem. $\square$

Note that if $H^2(G, \mathrm{Ad}\,\overline{\rho}) = 0$, there's no obstruction to deformation. In this case the universal deformation ring is the power series ring over $W(\mathbf{k})$ in $\dim H^1(G, \mathrm{Ad}\,\overline{\rho})$ variables.

If X is a $\mathbf{k}[G_{F,S}]$-module. For $i = 1, 2$, define

$$Ш^i_S(X) := \ker(H^i(G_{F,S}, X) \to \bigoplus_{v \in S} H^i(G_v, S)).$$

By the work of Poitou-Tate, $Ш^1_S(X^*)$ and $Ш^2_S(X)$ are dual. Note that triviality of $Ш^2_S(\mathrm{Ad}\,\overline{\rho})$ signifies any global obstruction can be realized locally.

Consider a deformation condition $\mathcal{D} \subset \mathrm{Def}_{\overline{\rho}}$ that is representable by $R_{\mathcal{D}}$. The quotient map $R^{\mathrm{ver}} \twoheadrightarrow R_{\mathcal{D}}$ induces via (1.3) a subspace of $H^1(G, \mathrm{Ad}\,\overline{\rho})$, which is denoted by $H^1_{\mathcal{D}}(G, \mathrm{Ad}\,\overline{\rho})$ and is called the tangent space of the deformation condition $\mathcal{D}$.

For example, one checks that the deformation condition of "fixed determinant" defined in example 1.1.2 has tangent space $H^1(G, \mathrm{Ad}^0\,\overline{\rho})$, where $\mathrm{Ad}^0\,\overline{\rho}$ is the subset of $\mathrm{Ad}\,\overline{\rho}$ of traceless matrices. At times we assume from the outset that all deformations are of fixed determinant. In that case, all the statements in this chapter still hold if one uses $\mathrm{Ad}^0\,\overline{\rho}$ in place of of $\mathrm{Ad}\,\overline{\rho}$ throughout.

In this thesis, we will consider global deformation condition defined in terms of local ones, in the following way. Let $\overline{\rho} : G_{F,S} \to \mathrm{GL}_2(\mathbf{k})$ be an absolutely irreducible representation. For each $v \in S$, let $\overline{\rho}|_{G_v} : G_v \to \mathrm{GL}_2(\mathbf{k})$ be its restriction to G_v and let $\mathcal{D}_v$ be a deformation condition (i.e. subfunctor of the local deformation functor) of $\overline{\rho}|_{G_v}$. Define the global deformation condition $\mathcal{D}$ by

$$\mathcal{D}(R) := \{\text{deformations } \rho : G_{F,S} \to \mathrm{GL}_2(\mathbf{k}) \text{ s.t. } \rho|_{G_v} \in \mathcal{D}_v(R) \text{ for all } v \in S\}.$$

As before, there correspond to the local deformation conditions $\mathcal{D}_v$ subspaces $\mathcal{L}_v \subset H^1(G_v, \mathrm{Ad}\,\overline{\rho})$. Let $\mathcal{L}_v^{\perp}$ be the annihilator of $\mathcal{L}_v$ under the pairing in Theorem 1.2.2. The kernels

$$H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}\,\overline{\rho}) = \ker(H^1(G_{F,S}, \mathrm{Ad}\,\overline{\rho}) \to \bigoplus_{v\in S} H^1(G_v, \mathrm{Ad}\,\overline{\rho})/\mathcal{L}_v)$$
$$H^1_{\mathcal{L}^{\perp}}(G_{F,S}, (\mathrm{Ad}\,\overline{\rho})*) = \ker(H^1(G_{F,S}, (\mathrm{Ad}\,\overline{\rho})^*) \to \bigoplus_{v\in S} H^1(G_v, (\mathrm{Ad}\,\overline{\rho})^*)/\mathcal{L}_v^{\perp})$$

are called the *Selmer* and *dual Selmer groups.*

We have an analogous

Theorem 1.2.6. *Given a absolutely continuous representation $\overline{\rho} : G_{F,S} \to \mathrm{GL}_2(\mathbf{k})$ and a set of local conditions $(\mathcal{D}_v, \mathcal{L}_v)$ for $v \in S$. The global deformation conditions defined by $\mathcal{D}_v$ is representable (say, by $R_{\mathcal{D}}$) and has tangent space $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}\,\overline{\rho})$. Moreover, $R_{\mathcal{D}}$ is a quotient of the formal power series ring over $W(\mathbf{k})$ in $\dim_{\mathbf{k}} H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}\,\overline{\rho})$ variables by an ideal minimally generated by at most $\dim_{\mathbf{k}} H^1_{\mathcal{L}^{\perp}}(G_{F,S}, (\mathrm{Ad}\,\overline{\rho})^*)$ elements.*

Note that the original statement (see [2]) of the last assertion regarding the minimal number of relations was stated in terms of the dimension of a cohomology group $H^2_{\mathcal{L}}(G_{F,S}, (\mathrm{Ad}\,\overline{\rho}))$, which we will not define. This quantity is in turn equal to $\dim H^1_{\mathcal{L}^{\perp}}(G_{F,S}, (\mathrm{Ad}\,\overline{\rho})^*)$ by global duality. See Propositions 3.6, 3.9, 9.2 in [14] for reference.

The following famous theorem of Wiles (Proposition 1.6 of [22]) allows us to measure the difference between the sizes of Selmer and dual Selmer groups.

Theorem 1.2.7 (Wiles' Formula)**.**

$$\frac{\# H^1_{\mathcal{L}}(G_S, \operatorname{Ad}\overline{\rho})}{\# H^1_{\mathcal{L}^\perp}(G_S, (\operatorname{Ad}\overline{\rho})^*)} = \frac{\# H^0(G_S, \operatorname{Ad}\overline{\rho})}{\# H^0(G_S, (\operatorname{Ad}\overline{\rho})^*)} \prod_{v \in S} \frac{\#\mathcal{L}_v}{\# H^0(G_v, \operatorname{Ad}\overline{\rho})}$$

CHAPTER 2

GENERALIZED KRASNER'S LEMMA

The goal of this chapter is to provide a ring-theoretic generalization of Krasner's lemma. The first section consists of a utilitarian collection of facts needed in our proof.

2.1 Some Algebraic Facts

We starts with a partial generalization of the Weierstrass Preparation Theorem.

Let $\mathbf{k}[[X_1, ..., X_n]]$ be the ring of formal power series over a field $\mathbf{k}$. We call $\leq$ a monomial order if it is a total order on the set of monomials in $\mathbf{k}[[X_1, ..., X_n]]$ and satisfies

1. $1 \leq X^v$ for all $v \in \mathbb{N}^n$.
2. If $X^v \leq X^u$, then $X^{v+w} \leq X^{u+w}$ for all $w \in \mathbb{N}^n$.

An example of such monomial order is the so-called graded lexicographic monomial order, defined in the following way. Let $v_1 = (a_1, a_2, ..., a_n)$, $v_2 = (b_1, b_2, ..., b_n) \in \mathbb{N}^n$. We say that $X^{v_1} > X^{v_2}$ if the the leftmost nonzero component of the $(n+1)$-tuple $(\sum a_i - \sum b_i, a_1 - b_1, a_2 - b_2, ..., a_n - b_n)$ is positive.

Fix a monomial order on $\mathbf{k}[[X_1, ..., X_n]]$. For any nonzero power series $f \in \mathbf{k}[[X_1, ..., X_n]]$, we define the initial term of f, denoted by $IT(f)$, to be the minimal monomial (along with its coefficient) that appears in f.

We have the following division algorithm.

Proposition 2.1.1. *Given $f, g_1, ..., g_m \in \mathbf{k}[[X_1, ..., X_n]]$, there exist $q_1, ..., q_m, r \in \mathbf{k}[[X_1, ..., X_n]]$, such that*

$$f = q_1 g_1 + q_2 g_2 + ... + q_m g_m + r,$$

where none of the terms in the remainder r is divisible by any of $IT(g_1), IT(g_2), ..., IT(g_m)$. Moreover, r is unique.

For a proof, see [5, III 7].

Let $I \subset \mathbf{k}[[X_1, ..., X_n]]$ be an ideal. Define the initial ideal of I to be $IT(I) = (\{IT(f) | f \in I\})$, the ideal generated by the initial terms of all the f in I. Let $S(I) = \{X^v | X^v \notin IT(I)\}$, the (possibly infinite) set of monic monomials that are not in $IT(I)$; we call $S(I)$ the set of standard monomials. By noetherianity, it's easy to see that $IT(I)$ can be finitely generated by monic monomials, say, by $X^{v_1}, ..., X^{v_m}$. Let $g_1, ..., g_m \in I$ be power series such that $IT(g_i) = X^{v_i}$. We claim that $g_1, ..., g_m$ generate I. Indeed, given $f \in I$, we can divide f by $g_1, ..., g_m$ using Proposition 2.1.1, which yields a remainder $r \in I$ that is a (possibly infinite) $\mathbf{k}$-linear combination of the standard monomials in $S(I)$. If $r \neq 0$, then $IT(r)$ would be a scalar multiple of one of the monomial in $S(I)$, hence not in $IT(I)$, contradictory to the fact that $r \in I$. Therefore, $g_1, ..., g_m$ indeed generate I. This allows us to regard Proposition 2.1.1 as a division-by-ideal theorem:

Corollary 2.1.2. *Let $I \subset \mathbf{k}[[X_1, ..., X_n]]$ be an ideal and let $S(I)$ be the corresponding set of standard monomials. Given $f \in \mathbf{k}[[X_1, ..., X_n]]$, there exists a unique $r \in \mathbf{k}[[X_1, ..., X_n]]$, which is a (possibly infinite) $\mathbf{k}$-linear combination of monomials in $S(I)$, such that $f \equiv r$ mod I. In other words, $\mathbf{k}[[X_1, ..., X_n]]/I$ is isomorphic (as a vector space) to the $\#S(I)$-fold direct product of $\mathbf{k}$.*

This corollary and the Nakayama's lemma together can give us information about the rank of an complete algebra over a coefficient ring W with residue field $\mathbf{k}$.

Finally we record a version of Hensel's lemma.

Let W be a ring. Let $f_1, ..., f_n \in W[[X_1, ..., X_n]]$. We use $\boldsymbol{f}$ to denote the n-tuple $(f_1, ..., f_n)$. Let

$$J_{\boldsymbol{a}}(\boldsymbol{f}) = (\partial_j f_i(\boldsymbol{a}))_{i,j}$$

be the jacobian of $\boldsymbol{f}$ evaluated at some **suitable** $\boldsymbol{a}$.

Theorem 2.1.3. *Let W be a ring, and let $\mathfrak{X} = (X_1, ..., X_n)$ be the ideal of $W[[X_1, ..., X_n]]$ generated by the indeterminates. Let $f_1, ..., f_n \in \mathfrak{X}$. The W-algebra endomorphism*

$$\varphi : W[[X_1, ..., X_n]] \to W[[X_1, ..., X_n]]$$

$$X_i \mapsto f_i$$

is an isomorphism if $\det J_{\mathbf{0}}(\boldsymbol{f})$ *is a unit.*

Proof. Say $\varphi(X_i) = \sum_j a_{ij} X_j$ + terms of degree ≥ 2. Note that $\det((a_{ij})_{i,j}) = \det J_{\mathbf{0}}(\boldsymbol{f})$, which is a unit by assumption. Let $(b_{ij})_{i,j}$ be the inverse of $(a_{ij})_{i,j}$ and let ψ be the automorphism of $W[[X_1, ..., X_n]]$ defined by $X_i \mapsto \sum_j b_{ji} X_j$. Then $\varphi \circ \psi$ has the form $X_i \mapsto X_i +$ terms of degree ≥ 2, which is an automorphism by [23, Chapter VII, lemma 2]. Therefore, φ is an isomorphism. □

Theorem 2.1.4 (Hensel's Lemma)**.** *Let W be a ring that is complete with respect to an ideal $\mathfrak{a}$, and let $f_1, ..., f_n \in W[[X_1, ..., X_n]]$. Let us use $(\mathfrak{a})^n$ to denote the set of column vectors with entries in $\mathfrak{a}$. If $\boldsymbol{a} \in (\mathfrak{a})^n$ is an approximate root of $\boldsymbol{f}$ in the sense that*

$$\boldsymbol{f}(\boldsymbol{a}) \equiv 0 \quad (mod \ \det J_{\boldsymbol{a}}(\boldsymbol{f})^2 \mathfrak{a}),$$

then there is a root $\boldsymbol{b} \in (\mathfrak{a})^n$ *of* $\boldsymbol{f}$ *near* $\boldsymbol{a}$ *in the sense that*

$$\boldsymbol{f}(\boldsymbol{b}) = 0 \quad \text{and} \quad \boldsymbol{b} \equiv \boldsymbol{a} \quad (\text{mod } \det J_{\boldsymbol{a}}(\boldsymbol{f})\mathfrak{a}).$$

Proof. Set $e = \det J_{\boldsymbol{a}}(\boldsymbol{f})$. Let M be the adjoint of $J_{\boldsymbol{a}}(\boldsymbol{f})$ so that $MJ_{\boldsymbol{a}}(\boldsymbol{f}) = J_{\boldsymbol{a}}(\boldsymbol{f})M = eI$. We have

$$\begin{aligned}\boldsymbol{f}(\boldsymbol{a} + eM\boldsymbol{X}) &= \boldsymbol{f}(\boldsymbol{a}) + J_{\boldsymbol{a}}(\boldsymbol{f})eM\boldsymbol{X} + e^2\boldsymbol{h}(M\boldsymbol{X}) \\ &= \boldsymbol{f}(\boldsymbol{a}) + e^2(\boldsymbol{X} + \boldsymbol{h}(M\boldsymbol{X}))\end{aligned}$$

for some $\boldsymbol{h} \in \mathfrak{X}^2$. By Theorem 2.1.3, the W-algebra endomorphism

$$\begin{aligned}\varphi : W[[X_1, ..., X_n]] &\to W[[X_1, ..., X_n]] \\ \boldsymbol{X} &\mapsto \boldsymbol{X} + \boldsymbol{h}(M\boldsymbol{X})\end{aligned}$$

is an isomorphism. Applying φ^{-1} to the above equation, we obtain

$$\boldsymbol{f}(\boldsymbol{a} + eM\varphi^{-1}(\boldsymbol{X})) = \boldsymbol{f}(\boldsymbol{a}) + e^2\boldsymbol{X}$$

By hypothesis, we may write $\boldsymbol{f}(\boldsymbol{a}) = e^2\boldsymbol{c}$ with $\boldsymbol{c} \in (\mathfrak{a})^n$. Let $\psi : W[[X_1, ..., X_n]] \to W$ be the W-algebra homomorphism defined by $\boldsymbol{X} \mapsto -\boldsymbol{c}$. Applying it, we get

$$\boldsymbol{f}(\boldsymbol{a} + eM\psi\varphi^{-1}(\boldsymbol{X})) = 0,$$

so $\boldsymbol{b} = \boldsymbol{a} + eM\psi\varphi^{-1}(\boldsymbol{X})$ is an actual solution. □

2.2 Generalized Krasner's Lemma

First let us fix some notations for the rest of this chapter. Let (W, π) be a complete discrete valuation ring with uniformizer π and finite residual field. Let $W[[X_1, X_2, ..., X_n]]$ be the ring of power series in n variables and let $\mathfrak{m} = (\pi, X_1, ..., X_n)$ be its maximal ideal. Fix $f_1, f_2, ..., f_n \in W[[X_1, X_2, ..., X_n]]$. We use

$\boldsymbol{f}$ to denote the n-tuple of power series $(f_1, ..., f_n)$. Let $I_{\boldsymbol{f}}$ be the ideal generated by the $f_i's$ and let $R_{\boldsymbol{f}} = W[[X_1, X_2, ..., X_n]]/I_{\boldsymbol{f}}$. Assume further that $R_{\boldsymbol{f}}$ is finite and flat (hence free) over W so that it possesses a W-basis $\overline{u}_1, \overline{u}_2, ..., \overline{u}_d$. Throughout, we use $\overline{g}$ to denote the image of the power series g in $R_{\boldsymbol{f}}$. For simplicity, we will denote the ideals $\mathfrak{m}/I_{\boldsymbol{f}}$ and $\mathfrak{m}_W W[[X_1, ..., X_n]]/I_{\boldsymbol{f}}$ of $R_{\boldsymbol{f}}$ also by $\mathfrak{m}$ and $\mathfrak{m}_W$. We will sometimes make the implicit identification $R_{\boldsymbol{f}} \simeq W^d$. Given $\overline{g} \in R_{\boldsymbol{f}}$, by abuse of notation, we also regard it as a linear endomorphism on $R_{\boldsymbol{f}} \simeq W^d$, given by multiplication by $\overline{g}$. In particular, it makes sense to speak of $\det \overline{g}$.

Let $\epsilon_1, \epsilon_2, ..., \epsilon_n \in W[[X_1, X_2, ..., X_n]]$, which we allow to vary. Define $\boldsymbol{\epsilon}, \boldsymbol{f} + \boldsymbol{\epsilon}, I_{\boldsymbol{f}+\boldsymbol{\epsilon}}, R_{\boldsymbol{f}+\boldsymbol{\epsilon}}$ similarly. Consider the following system of equations

$$
\begin{aligned}
(f_1 + \epsilon_1)(\overline{X}_1 + \delta_1, ..., \overline{X}_n + \delta_n) &= 0 \\
(f_2 + \epsilon_2)(\overline{X}_1 + \delta_1, ..., \overline{X}_n + \delta_n) &= 0 \\
&... \\
(f_n + \epsilon_n)(\overline{X}_1 + \delta_1, ..., \overline{X}_n + \delta_n) &= 0
\end{aligned}
\tag{2.1}
$$

in $\boldsymbol{\delta} = (\delta_1, ..., \delta_n) \in (R_{\boldsymbol{f}})^n$, which we abbreviate $(\boldsymbol{f} + \boldsymbol{\epsilon})(\overline{\boldsymbol{X}} + \boldsymbol{\delta}) = 0$. Since $R_{\boldsymbol{f}} \simeq W\overline{u}_1 \oplus W\overline{u}_2 \oplus ... \oplus W\overline{u}_d$, we can write

$$
\begin{aligned}
\delta_1 &= \delta_{11}\overline{u}_1 + \delta_{12}\overline{u}_2 + ... + \delta_{1d}\overline{u}_d \\
\delta_2 &= \delta_{21}\overline{u}_1 + \delta_{22}\overline{u}_2 + ... + \delta_{2d}\overline{u}_d \\
&... \\
\delta_n &= \delta_{n1}\overline{u}_1 + \delta_{n2}\overline{u}_2 + ... + \delta_{nd}\overline{u}_d
\end{aligned}
$$

for some $\delta_{ij} \in W$. Therefore, we can also regard (2.1) as a system of nd equations in the nd unknowns δ_{ij}. In particular, this allows us to speak of the jacobian determinant of the system (2.1). The notation $\boldsymbol{\delta}$ should be understood both as a column vector in $R_{\boldsymbol{f}}^n$ and as a column vector in W^{nd}; there shall be no ambiguity from the context.

Our goal is to show that the system (2.1) admits solution under small perturbation $\boldsymbol{\epsilon}$. With a view to applying the Hensel's lemma, we will compute the jacobian determinant of the system (2.1) at $\boldsymbol{\delta} = \mathbf{0}$. We observe,

$$(\boldsymbol{f}+\boldsymbol{\epsilon})(\overline{\boldsymbol{X}}+\boldsymbol{\delta}) = (\boldsymbol{f}+\boldsymbol{\epsilon})(\overline{\boldsymbol{X}}) + (J(\boldsymbol{f}+\boldsymbol{\epsilon})(\overline{\boldsymbol{X}}))\cdot\boldsymbol{\delta} + \boldsymbol{h}(\overline{\boldsymbol{X}},\boldsymbol{\delta})$$

where $\boldsymbol{h}(\overline{\boldsymbol{X}},\boldsymbol{\delta})$ is some power series that only contains terms of total degree ≥ 2 in the δ_i (hence also in the δ_{ij}). Therefore, the jacobian determinant of the system (2.1) at $\boldsymbol{\delta} = \mathbf{0}$ is

$$\det\det J(\boldsymbol{f}+\boldsymbol{\epsilon})(\overline{\boldsymbol{X}}),$$

which is the determinant of the linear endomorphism

$$J(\boldsymbol{f}+\boldsymbol{\epsilon})(\overline{\boldsymbol{X}}) : W^{nd} \longrightarrow W^{nd}.$$

We first show

Proposition 2.2.1. *Preserve all the notations above, then* $\det\det J(\boldsymbol{f})(\overline{\boldsymbol{X}}) \neq 0$.

Proof. Let $F = F(W)$ be the field of fraction of W and let $\overline{F}$ be its algebraic closure. Write $R = R_{\boldsymbol{f}}$ for simplicity. We first show that $\overline{F} \otimes_W R$ is reduced.

Let $v_1, ..., v_d$ be a W-basis of R. Let $S = F \otimes_W R$ and suppose x is a nilpotent element in S. Write $x = \sum_i \alpha_i \otimes v_i$ with $\alpha_i \in F$. We may clear denominators and assume that $\alpha_i \in W$. Then $x = \sum_i \alpha_i \otimes v_i = 1 \otimes (\sum_i \alpha_i v_i) \in R$. Since R is reduced, we deduce that $x = 0$ and that S is reduced.

To show that $\overline{F} \otimes_F S$ is reduced, assume afresh that $v_1, ..., v_d$ is a F-basis of S. Suppose x is a nilpotent element in $\overline{F} \otimes_F S$. Write $x = \sum_i \alpha_i \otimes v_i$ with $\alpha_i \in \overline{F}$. There exists a finite galois extension L/F containing all the α_i. Therefore, $x \in L \otimes_F S$ and it suffices to show that $T := L \otimes_F S$ is reduced. Let $G = \mathrm{Gal}(L/F)$

be the galois group. We define an action of G on T by $\sigma(\alpha \otimes s) = \sigma(\alpha) \otimes s$. Let N be the nilradical ideal of T. One checks that the galois image of an nilpotent element is nilpotent, so $\sigma N \subset N$. The same argument also shows that $\sigma^{-1} N \subset N$, so $\sigma N = N$ for all $\sigma \in G$. Recall by assumption that $x \in N$. For any $\beta \in L$, we create a nilpotent element of S using the trace function:

$$Tr_{L/F}(\beta x) = Tr_{L/F}(\sum_i \beta\alpha_i \otimes v_i) = \sum_\sigma \sum_i \sigma(\beta\alpha_i) \otimes v_i$$
$$= \sum_i Tr_{L/F}(\beta\alpha_i) \otimes v_i = 1 \otimes \sum_i Tr_{L/F}(\beta\alpha_i) v_i \in S.$$

Since S is reduced, $Tr_{L/F}(\beta\alpha_i) = 0$ for all $\beta \in L$ and all i. By separability, $Tr_{L/F}$ is a non-degenerate bilinear form, so $\alpha_i = 0$ for all i and $x = 0$, which implies $\overline{F} \otimes_W R$ is reduced.

Now since $\overline{F} \otimes_W R$ is reduced, its module of Kahler differentials $\Omega_{\overline{F}\otimes_W R/\overline{F}}$ is 0. Since formation of differentials commutes with base change, we have $\overline{F} \otimes_W \Omega_{R/W} = \Omega_{\overline{F}\otimes_w R/\overline{F}} = 0$.

Now consider the module of continuous differentials $\hat{\Omega}_{R/W}$. (Its definition, basic properties, distinction and connection with the module of Kahler differentials can be found in Exercise 16.14 in[3].) We know that

$$\hat{\Omega}_{R/W} = \operatorname{coker} R^n \xrightarrow{J^T(\boldsymbol{f})(\overline{\boldsymbol{X}})} R^n.$$

Since taking tensor products is right exact, it preserves cokernel; we have

$$\overline{F} \otimes_W \hat{\Omega}_{R/W} = \operatorname{coker} \overline{F}^{nd} \xrightarrow{J^T(\boldsymbol{f})(\overline{\boldsymbol{X}})} \overline{F}^{nd}.$$

Since $\overline{F} \otimes_W \Omega_{R/W} = 0$, $\overline{F} \otimes_W \hat{\Omega}_{R/W} = \overline{F} \otimes_W \Omega_{R/W}/(\cap_k \mathfrak{m}^k \Omega_{R/W}) = 0$. It follows that $\det\det J(\boldsymbol{f})(\overline{\boldsymbol{X}}) \neq 0$. □

We next show that sufficiently $\mathfrak{m}$-adically small $\epsilon_i \in \mathcal{R}_{\boldsymbol{f}}$ are also π-adically small.

Lemma 2.2.2. *Recall $R_{\boldsymbol{f}}$ is a finite complete intersection over W. The $\mathfrak{m}$-adic topology and π-adic topology are equivalent on $\mathcal{R}_{\boldsymbol{f}}$.*

Proof. Consider the identity map from $\mathcal{R}_{\boldsymbol{f}}$ to itself, with the domain equipped with the π-adic topology and the range equipped with the $\mathfrak{m}_R$-adic topology. Since W is compact in π-adic topology, so is $\mathcal{R}_{\boldsymbol{f}}$ because it's finite and free over W.The lemma follows from the standard fact that a continuous bijection from a compact space to a Hausdorff space is a homeomorphism. □

Corollary 2.2.3. *Preserve all the notations above so that $R_{\boldsymbol{f}}$ is reduced, finite and free over W, where W is a complete discrete valuation ring with uniformizer π. The system* (2.1) *has a solution $\boldsymbol{\delta} \equiv 0$ mod π, whenever $\boldsymbol{\epsilon}$ is sufficiently small in the $\mathfrak{m}$-adic topology.*

Proof. Let $e = \det\det J(\boldsymbol{f})(\overline{\boldsymbol{X}}) \in W$. By the lemma 2.2.1, $e \neq 0$, so there exists an integer M such that $e \in (\pi^M) \setminus (\pi^{M+1})$. We recall that, by lemma 2.2.2, the condition "$\mathfrak{m}$-adically small" is equivalent to "π-adically small" in the ring $R_{\boldsymbol{f}}$. Therefore there exists an integer N such that whenever $\boldsymbol{\epsilon} \in \mathfrak{m}^N$, the following two conditions are satisfied simultaneously

1. $\boldsymbol{\delta} = 0$ is an approximate solution to the system (2.1) mod π^{2M+1}.
2. $\det\det J(\boldsymbol{f} + \boldsymbol{\epsilon})(\overline{\boldsymbol{X}}) \in (\pi^M)$.

Indeed, one just needs to let $\boldsymbol{\epsilon} \in (\pi^{2M+1})$. Hensel's lemma (Theorem 2.1.4) then provides us with a desired solution. □

Finally, we conclude

Proposition 2.2.4 (Generalized Krasner's Lemma). *Preserve all the notations above so that* $R_{\boldsymbol{f}} = W[[X_1, ..., X_n]]/(f_1, ..., f_n)$ *is reduced, finite and free over* W*, where* W *is a complete discrete valuation ring with uniformizer* π*. There exists an integer* N *such that whenever* $\boldsymbol{\epsilon} = (\epsilon_1, ..., \epsilon_n) \in \mathfrak{m}^N$*, there is an isomorphism of* W*-algebras* $R_{\boldsymbol{f}+\boldsymbol{\epsilon}} \simeq R_{\boldsymbol{f}}$*, where* $R_{\boldsymbol{f}+\boldsymbol{\epsilon}} = W[[X_1, ..., X_n]]/(f_1 + \epsilon_1, ..., f_n + \epsilon_n)$*.*

Proof. For sufficiently large N, corollary 2.2.3 provides us with a solution $\boldsymbol{\delta}$ of (2.1) that is $\equiv 0 \bmod \pi$ whenever $\boldsymbol{\epsilon} \in \mathfrak{m}^N$. By lemma 2.2.2, we may assume $\mathfrak{m}^N \subseteq (\pi)$ as ideals in $R_{\boldsymbol{f}}$. We have a W-algebra homomorphism

$$W[[X_1, X_2, ..., X_n]] \to R_{\boldsymbol{f}}$$
$$\boldsymbol{X} \mapsto \overline{\boldsymbol{X}} + \boldsymbol{\delta}$$

The kernel of this map contains $I_{\boldsymbol{f}+\boldsymbol{\epsilon}}$, so the above map induces a homomorphism

$$\Phi : R_{\boldsymbol{f}+\boldsymbol{\epsilon}} \to R_{\boldsymbol{f}}.$$

Since $\boldsymbol{\delta} \equiv 0 \bmod \pi$, the reduction mod π of Φ is surjective. We have a commutative diagram,

$$\begin{array}{ccc} R_{\boldsymbol{f}+\boldsymbol{\epsilon}} & \xrightarrow{\Phi} & R_{\boldsymbol{f}} \\ \downarrow & & \downarrow \\ R_{\boldsymbol{f}+\boldsymbol{\epsilon}}/\pi R_{\boldsymbol{f}+\boldsymbol{\epsilon}} & \twoheadrightarrow & R_{\boldsymbol{f}}/\pi R_{\boldsymbol{f}} \end{array}$$

Since the composed map $R_{\boldsymbol{f}+\boldsymbol{\epsilon}} \to R_{\boldsymbol{f}+\boldsymbol{\epsilon}}/\pi R_{\boldsymbol{f}+\boldsymbol{\epsilon}} \to R_{\boldsymbol{f}}/\pi R_{\boldsymbol{f}}$ is surjective, so is the composed map $R_{\boldsymbol{f}+\boldsymbol{\epsilon}} \to R_{\boldsymbol{f}} \to R_{\boldsymbol{f}}/\pi R_{\boldsymbol{f}}$. If follows that $\Phi(R_{\boldsymbol{f}+\boldsymbol{\epsilon}}) + (\pi R_{\boldsymbol{f}}) = R_{\boldsymbol{f}}$ and by Nakayama's lemma that $\Phi(R_{\boldsymbol{f}+\boldsymbol{\epsilon}}) = R_{\boldsymbol{f}}$. Therefore, Φ is surjective.

Let $\mathbf{k} = W/\pi$ be the residue field of W. We will use an $\tilde{}$ to denote the mod π reduction of a power series or an ideal in $W[[X_1, ..., X_n]]$. To establish injectivity of Φ, we compare the initial ideals $IT(\tilde{I}_{\boldsymbol{f}+\boldsymbol{\epsilon}})$ and $IT(\tilde{I}_{\boldsymbol{f}})$ in $\mathbf{k}[[X_1, ..., X_n]]$, where the underlying monomial order is chosen to be the graded lexicographic monomial order, defined at the beginning of this chapter. We claim that $IT(\tilde{I}_{\boldsymbol{f+\epsilon}}) \supseteq IT(\tilde{I}_{\boldsymbol{f}})$ when $\boldsymbol{\epsilon}$ is sufficiently $\mathfrak{m}$-adically small. Indeed, let $\tilde{g}$ be a monic monomial in $IT(\tilde{I}_{\boldsymbol{f}})$. Then for some $h_1, ..., h_n \in W[[X_1, ..., X_n]]$, we have

$$IT(\tilde{h}_1\tilde{f}_1 + ... + \tilde{h}_n\tilde{f}_n) = \tilde{g}.$$

Clearly if $\boldsymbol{\epsilon} \in \mathfrak{m}^N$ for sufficiently large N (that depends on $\tilde{g}$), it does not alter the initial term of the expression above. That is,

$$IT(\tilde{h}_1(\tilde{f}_1 + \tilde{\epsilon}_1) + ... + \tilde{h}_n(\tilde{f}_n + \tilde{\epsilon}_n)) = \tilde{g}.$$

By noetherianity, $IT(\tilde{I}_{\boldsymbol{f}})$ can be finitely generated by monic monomials, so we may choose a uniform N that works for a set of generators of $IT(\tilde{I}_{\boldsymbol{f}})$. Therefore, $IT(\tilde{I}_{\boldsymbol{f+\epsilon}}) \supseteq IT(\tilde{I}_{\boldsymbol{f}})$ when $\boldsymbol{\epsilon}$ is sufficiently $\mathfrak{m}$-adically small. For such $\boldsymbol{\epsilon}$, we have the following reverse containment on the sets of standard monomials:

$$S(\tilde{I}_{\boldsymbol{f+\epsilon}}) \subseteq S(\tilde{I}_{\boldsymbol{f}}).$$

By corollary 2.1.2,

$$\dim_{\mathbf{k}} R_{\boldsymbol{f+\epsilon}}/\pi R_{\boldsymbol{f+\epsilon}} = \#S(\tilde{I}_{\boldsymbol{f+\epsilon}}) \leq \#S(\tilde{I}_{\boldsymbol{f}}) = \dim_{\mathbf{k}} R_{\boldsymbol{f}}/\pi R_{\boldsymbol{f}} = d,$$

where we recall that d is the W-rank of $R_{\boldsymbol{f}}$. By Nakayama's lemma a $\mathbf{k}$-basis of $R_{\boldsymbol{f+\epsilon}}/\pi R_{\boldsymbol{f+\epsilon}}$ lift to a set of W-generators of $R_{\boldsymbol{f+\epsilon}}$, so $R_{\boldsymbol{f+\epsilon}}$ can be generated by at most d elements as a W-module. On the other hand, $R_{\boldsymbol{f+\epsilon}}$ surjects via Φ onto the free W-module $R_{\boldsymbol{f}}$ of rank d, so Φ has to be an isomorphism. □

Corollary 2.2.5. *Let $R = W[[X_1, ..., X_n]]/(f_1, ..., f_n)$ be a reduced, finite flat complete intersection over W, where W is a complete discrete valuation ring with uniformizer π. There exists an integer N such that, if S is a quotient of*

$W[[X_1, ..., X_n]]$ *by an ideal generated by at most* n *elements and if there is a surjection* $\Phi : S \to R/\pi^N R$ *which induces an isomorphism* $S/\pi S \simeq R/\pi R$*, then* $S \simeq R$*.*

Proof. We may assume $S = W[[X_1, ..., X_n]]/(g_1, ..., g_n)$ and Φ sends X_i to X_i. Note $R/\pi^N R = W[[X_1, ..., X_n]]/(f_1, ..., f_n, \pi^N)$. Since Φ is surjective, $(g_1, ..., g_n) \subset (f_1, ..., f_n, \pi^N)$. We may assume $g_i = \sum_j \alpha_{ij} f_j + \pi^N \beta_i$, where α_{ij} and β_i are power series.

Let us show that $\det(\alpha_{ij})$ is a unit by showing that $\det(\overline{\alpha}_{ij})$ is a unit. We consider the reduction mod π map and will use $\bar{\ }$ to denote the reduction of a power series. Since $S/\pi S \simeq R/\pi R$, we have $(\overline{g}_1, ..., \overline{g}_n) = (\overline{f}_1, ..., \overline{f}_n)$. By assumption, $\overline{g}_i = \sum_j \overline{\alpha}_{ij} \overline{f}_j$. Since R is a finite free complete intersection, so is $R/\pi R$. In particular, none of the $\overline{f}_i$ is a linear combination of the others (with coefficients in $W[[X_1, ..., X_n]]$). Since $(\overline{g}_1, ..., \overline{g}_n) = (\overline{f}_1, ..., \overline{f}_n)$, $\overline{f}_1 - \sum_i \overline{\gamma_i g_i} = 0$ for some $\overline{\gamma}_i \in (W/\pi W)[[X_1, ..., X_n]]$. Using $\overline{g}_i = \sum_j \overline{\alpha}_{ij} \overline{f}_j$ we may express $\overline{f}_1 - \sum_i \overline{\gamma_i g_i}$ as a linear combination of the $\overline{f}_i$, which evaluates to 0. If all the $\overline{\alpha}_{i1}$ are in the maximal ideal of $(W/\pi W)[[X_1, ..., X_n]]$, then the coefficient of $\overline{f_1}$ in the linear combination $\overline{f}_1 - \sum_i \overline{\gamma_i g_i}$ is a unit. This implies $\overline{f}_1$ is a linear combination of $\overline{f}_2, ..., \overline{f}_n$, which is a contradiction by the above discussion. Therefore, the first column of the matrix $(\overline{\alpha}_{ij})$ contains a unit. By row and column reduction, we may assume $\overline{\alpha}_{11} = 1$ and $\overline{\alpha}_{1i} = \overline{\alpha}_{i1} = 0$. Note that a column (row resp.) reduction amounts to replace $\overline{g}_1, ..., \overline{g}_n$ ($\overline{f}_1, ..., \overline{f}_n$ resp.) by a new set of generators $\overline{g}'_1, ..., \overline{g}'_n$ ($\overline{f}'_1, ..., \overline{f}'_n$ resp.) of the same ideal. It should be clear we can repeat the above procedure to the second column and so on to reduce the matrix $(\overline{\alpha}_{ij})$ to the identity matrix. This shows that $\det(\overline{\alpha}_{ij})$ is a unit.

As a consequence, $\det(\alpha_{ij})$ is a unit and the matrix (α_{ij}) has an inverse, say

(α'_{ij}). Set $f'_i = \sum_j \alpha'_{ij} f_i$. Then we can replace $f_1, ..., f_n$ by the new set of generators $f'_1, ..., f'_n$ of the same ideal. Moreover, we now have $g_i = f'_i + \pi^N \beta_i$. An application of Proposition 2.2.4 implies $S \simeq R$ for sufficiently large N. $\square$

CHAPTER 3

THE FIXED DETERMINANT INVERSE GALOIS PROBLEM

Throughout this chapter, fix a prime $p \geq 7$ and a finite field $\mathbf{k}$ of characteristic p. Let F be a totally real field that is linearly disjoint from $\mathbb{Q}(\mu_p)$ (e.g. $\mathbb{Q}$). Let $\overline{\rho} : G_{F,S} \to GL_2(\mathbf{k})$ be a continuous, totally odd, residual representation with determinant χ (the cyclotomic character), whose image contains $SL_2(\mathbf{k})$. That $\mathrm{Im}\overline{\rho} \supseteq \mathrm{SL}_2(\mathbf{k})$ implies that $\overline{\rho}$ and $\mathrm{Ad}^0\,\overline{\rho}$ are absolutely irreducible and the minimal field of definition of $\mathrm{Ad}^0\,\overline{\rho}$ is $\mathbf{k}$. See Lemma 17 in [15]. Once and for all we fix the determinant of all deformations of $\overline{\rho}$ to be χ.

Fix $\mathcal{R}$ to be a reduced, complete Noetherian local algebra that is a finite flat complete intersection over $W(\mathbf{k})$. Assume that the dimension of its cotangent space $t^*_{\mathcal{R}} := \mathfrak{m}_{\mathcal{R}}/(\mathfrak{m}^2_{\mathcal{R}} + p\mathcal{R})$ is n so that it can be written as a quotient of the power series ring with n (and no less) variables over $W(\mathbf{k})$. Say $\mathcal{R} = W(\mathbf{k})[[X_1, ..., X_n]]/(F_1, ..., F_n)$. Our assumption implies that when reduced mod p, F_i contains no linear term. The goal of this note is to find a suitable set of auxiliary primes Q and a set of local condition $\{(\mathcal{D}_v, \mathcal{L}_v)\}_{v \in S \cup Q}$ so that the global universal deformation ring subjected to these local conditions is $\mathcal{R}$.

First of all, we describe the local conditions at primes $v \in S$.

3.1 Local Conditions

In this section, we record a list of our allowable local deformation conditions, which can be found in [4].

A1 Suppose that $v \nmid p$ and that $p \nmid \#\overline{\rho}(I_v)$. We take $\mathcal{D}_v$ to be the class of deformations which factor through $G_v/(I_v \cap \ker \overline{\rho})$. The corresponding tangent space is $\mathcal{L}_v = H^1_{\mathrm{nr}}(G_v, \mathrm{Ad}^0 \overline{\rho})$.

A2 Suppose that $v \nmid p$ and that either $\mathrm{N}v \not\equiv 1 \pmod p$ or $p \mid \#\overline{\rho}(G_v)$. If

$$\overline{\rho} \mid_{G_v} \sim \begin{pmatrix} \chi\overline{\alpha} & * \\ 0 & \overline{\alpha} \end{pmatrix}$$

for some character $\overline{\alpha} : G_v \to \mathbf{k}^*$, we take $\mathcal{D}_v$ to be the class of deformations of the form

$$\rho \mid_{G_v} \sim \begin{pmatrix} \chi\alpha & * \\ 0 & \alpha \end{pmatrix},$$

with α lifting $\overline{\alpha}$. The corresponding tangent space is $\mathcal{L}_v = H^1(G_v, U^0) \subset H^1(G_v, \mathrm{Ad}^0 \overline{\rho})$, where $U^0 = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \mid a \in \mathbf{k} \right\} \subset \mathrm{Ad}^0 \overline{\rho}$.

B1 Suppose that $v \mid p$ and

$$\overline{\rho} \mid_{G_v} \sim \begin{pmatrix} \chi\overline{\alpha} & * \\ 0 & \overline{\beta} \end{pmatrix}$$

for some characters $\overline{\alpha}, \overline{\beta} : G_v \to \mathbf{k}^*$ such that $\overline{\alpha} \neq \overline{\beta}$ and that $\chi\overline{\alpha} \neq \overline{\beta}$. We take $\mathcal{D}_v$ to be the class of deformations of the form

$$\rho \mid_{G_v} \sim \begin{pmatrix} \chi\alpha & * \\ 0 & \beta \end{pmatrix},$$

with α, β tamely ramified lifts of $\overline{\alpha}, \overline{\beta}$ respectively. The corresponding tangent space is $\mathcal{L}_v = \ker(H^1(G_v, \mathrm{Ad}^0 \overline{\rho}) \to H^1(I_v, \mathrm{Ad}^0 \overline{\rho}/U^0)^{G_v/I_v})$.

B2 Suppose that $v \mid p$ and

$$\overline{\rho} \mid_{G_v} \sim \begin{pmatrix} \chi\overline{\alpha} & * \\ 0 & \overline{\alpha} \end{pmatrix}$$

for some unramified character $\overline{\alpha} : G_v \to \mathbf{k}^*$, we take $\mathcal{D}_v$ to be the class of flat deformations of the form

$$\rho\,|_{G_v} \sim \begin{pmatrix} \chi\alpha & * \\ 0 & \alpha \end{pmatrix},$$

where α is any unramified lift of $\overline{\alpha}$. The corresponding tangent space is $\mathcal{L}_v = H^1(G_v, U^0) \subset H^1(G_v, \mathrm{Ad}^0\,\overline{\rho})$

Note that by lemma 3.1 in [4], under the assumption $p \geq 7$, A1 and A2 provide a complete list of possible $\overline{\rho}|_{G_v}$ for (ramified) $v \nmid p$.

Proposition 3.1.1. *Suppose $\overline{\rho}|_{G_v}$ takes the form of one of $B1, B2$ for all $v \mid p$. For all $v \in S$, the local conditions described above induces a smooth quotient the the local versal deformation ring and hence a subspace $\mathcal{L}_v \in H^1(G_v, \mathrm{Ad}^0\,\overline{\rho})$ that preserves $\mathcal{D}_v$ such that*

$$\dim \mathcal{L}_v = \begin{cases} \dim H^0(G_v, \mathrm{Ad}^0\,\overline{\rho}) & \textit{if } v \nmid p \\ \dim H^0(G_v, \mathrm{Ad}^0\,\overline{\rho}) + [F_v : \mathbb{Q}_p] & \textit{if } v \mid p. \end{cases}$$

In particular,

$$\dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) = \dim H^1_{\mathcal{L}^\perp}(G_{F,S}, (\mathrm{Ad}^0\,\overline{\rho})^*).$$

Proof. The computation of $\dim \mathcal{L}_v$ was done in [4]. The last equality follows from Wiles' formula (Theorem 1.2.7). Note that the assumption that F is totally real and that $\overline{\rho}$ is totally odd are used here: each of the $[F : \mathbb{Q}]$ real embeddings of F into $\mathbb{C}$ contributes a -1 to the right side of Wiles' formula . $\square$

3.2 Nice Primes

In this section, we describe the auxiliary primes at which we allow additional ramifications. For prime w of F, define the norm map as $\mathrm{N}w := q^{f(w/q)}$, where q is the rational prime lying below w and $f(w/q)$ is the inertial degree of w over q. Note that $\chi(\sigma_w) = \mathrm{N}w$ when $w \nmid p$, where σ_w is the Frobenius at w.

Definition 3.2.1. We say a prime w in F is nice (for $\overline{\rho}$) if

- $Nw \not\equiv \pm 1 \bmod p$
- $\overline{\rho}$ is unramified at w
- the ratio of the eigenvalues of $\overline{\rho}(\sigma_w)$ is $\chi(\sigma_w)$.

Let B be an Artinian coefficient-ring with residue field $\mathbf{k}$. If ρ_B is a lift of $\overline{\rho}$ to $GL_2(B)$, then we say w is ρ_B-nice if

- w is nice for $\overline{\rho}$
- ρ_B is unramified at w
- the ratio of the eigenvalues of $\rho_B(\sigma_w)$ is $\chi(\sigma_w)$
- $\rho_B(\sigma_w)$ has the same (prime to $\mathrm{N}w$) order as $\overline{\rho}(\sigma_w)$.

Proposition 3.2.2. *Let $\overline{\rho}$ be as above and let ρ_B be a lift of $\overline{\rho}$ to an Artinian coefficient-ring B. Then there's a Cebotarev set of ρ_B-nice primes.*

Proof. We can pick $x \not\equiv \pm 1 \bmod p$ and lift $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Im}(\overline{\rho})$ to an element $\alpha = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} + \beta \in \mathrm{Im}(\rho_B)$, where β is a matrix with entries in the maximal ideal of B. Note that we've used the assumption that F is linearly disjoint from $\mathbb{Q}(\mu_p)$ to guarantee $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ is indeed an element of $\mathrm{Im}(\overline{\rho})$. For sufficiently large a, $\alpha^{p^a} = \begin{pmatrix} x^{p^a} & 0 \\ 0 & 1 \end{pmatrix}$ have the same (tame) order as its image in $\mathrm{GL}_2(\mathbf{k})$. Any prime w in $F(\rho_B)$ with Frobineus in the conjugacy class of $\alpha^{p^a} \in \mathrm{Im}(\rho_B) = \mathrm{Gal}(F(\rho_B)/F)$ is ρ_B-nice. Note this is a complete splitting condition from $F(\overline{\rho})$ to $F(\rho_B)$. □

Let w be a nice prime. For suitable choice of basis of the representation $\overline{\rho}$ we may assume that up to twist $\overline{\rho}(\sigma_w) = \begin{pmatrix} \chi(\sigma_w) & 0 \\ 0 & 1 \end{pmatrix}$. Any local deformation of $\overline{\rho}|_{G_w}$ is tamely ramified and factors through the Galois group of the maximal tamely ramified extension of F_w, which is generated by σ_w and τ_w, where τ_w generates inertia. Define $\mathcal{D}_w$ to be all deformations of the form $\sigma_w \mapsto \begin{pmatrix} \chi(\sigma_w) & 0 \\ 0 & 1 \end{pmatrix}$ and $\tau_w \mapsto \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

One computes that there are G_w-module homomorphisms

$$\mathrm{Ad}^0 \overline{\rho} \simeq \mathbf{k} \oplus \mathbf{k}(\chi) \oplus \mathbf{k}(\chi^{-1})$$

$$(\mathrm{Ad}^0 \overline{\rho})^* \simeq \mathbf{k}(\chi) \oplus \mathbf{k} \oplus \mathbf{k}(\chi^2).$$

Since cohomology commutes with direct sums,

$$H^1(G_w, \mathrm{Ad}^0 \overline{\rho}) \simeq H^1(G_w, \mathbf{k}) \oplus H^1(G_w, \mathbf{k}(\chi)) \oplus 0$$

$$H^1(G_w, (\mathrm{Ad}^0 \overline{\rho})^*) \simeq H^1(G_w, \mathbf{k}(\chi)) \oplus H^1(G_w, \mathbf{k}) \oplus 0.$$

The non-zero summands on the right are 1-dimensional. It is shown in [15] that the corresponding tangent space for the local condition $\mathcal{D}_w$ is $\mathcal{L}_w = H^1(G_w, \mathbf{k}(\chi)) \subset H^1(G_w, \mathrm{Ad}^0 \overline{\rho})$ so that $\mathcal{L}_w^{\perp} = H^1(G_w, \mathbf{k}(\chi)) \subset H^1(G_w, (\mathrm{Ad}^0 \overline{\rho})^*)$.

Proposition 3.2.3. *Let* $\overline{\rho} : G_{F,S} \to \mathrm{GL}_2(\mathbf{k})$ *be as above. Let* f_i $(i = 1, ..., r)$ *be linearly independent elements in* $H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ *and* ϕ_j $(j = 1, ..., s)$ *be linearly independent elements in* $H^1(G_{F,S}, (\mathrm{Ad}^0\,\overline{\rho})^*)$. *We denote by* K_{f_i} *and* K_{ϕ_j} *the fixed field of the kernels of the restrictions of* f_i *and* ϕ_j *to the absolute Galois group of* $K := F(\overline{\rho})$. *Then* K_{f_i} *and* K_{ϕ_i} *are* $\mathrm{Ad}^0\,\overline{\rho}$*- and* $(\mathrm{Ad}^0\,\overline{\rho})^*$*-extensions of* K. *Each of the fields* K_{f_i}, K_{ϕ_j} *is linearly disjoint over* K *with the compositum of the others. The short exact sequences*

$$1 \to \mathrm{Gal}(K_{f_i}/K) \to \mathrm{Gal}(K_{f_i}/F) \to \mathrm{Gal}(K/F) \to 1$$
$$1 \to \mathrm{Gal}(K_{\phi_j}/K) \to \mathrm{Gal}(K_{\phi_j}/F) \to \mathrm{Gal}(K/F) \to 1$$

split.

Proof. Consider the inflation-restriction sequence

$$0 \to H^1(\mathrm{Gal}(K/F), \mathrm{Ad}^0\,\overline{\rho}) \to H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) \to H^1(\mathrm{Gal}(F_S/K), \mathrm{Ad}^0\,\overline{\rho})$$

Note $H^1(\mathrm{Gal}(K/F), \mathrm{Ad}^0\,\overline{\rho}) \simeq H^1(\mathrm{Im}(\overline{\rho}), \mathrm{Ad}^0\,\overline{\rho})) = 0$ because $\mathrm{Im}(\overline{\rho}) \supseteq \mathrm{SL}_2(\mathbf{k})$. See Lemma 19 in [7]. Therefore, each $f_i \in H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ is restricted to a nonzero element in $\tilde{f}_i$ in $H^1(\mathrm{Gal}(F_S/K), \mathrm{Ad}^0\,\overline{\rho}) = \mathrm{Hom}(\mathrm{Gal}(F_S/K), \mathrm{Ad}^0\,\overline{\rho})$. We know that $\tilde{f}_i$ is necessarily surjective, (See Lemma 7 in [15]), so it cuts out an $\mathrm{Ad}^0\,\overline{\rho}$-extension of K_{f_i}/K. The same thing can be said about the dual cohomology classes ϕ_j. The rest of proof is a straight repeat of section 7 in [15]. □

Let $f \in H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ and w be a nice prime. We will by abuse of notation denote the diagonal value of $f(\sigma_w)$ again by $f(\sigma_w)$. In other words, $f(\sigma_w)$ is the value of the projection of f in $H^1(G_w, \mathbf{k}) \subset H^1(G_w, \mathrm{Ad}^0\,\overline{\rho})$, evaluated at σ_w. Note that $f(\sigma_w) = 0$ if and only if $f|_{G_w} \in \mathcal{L}_w$, which further implies $f|_{G_w} = 0$ provided f is unramified at w. Suppose f is unramified at the nice prime w, then $f|_{G_w}$

is completely determined by $f(\sigma_w)$. Indeed, it can be shown that two 1-cocycles $f_1, f_2 : G_w \to \mathrm{Ad}^0 \overline{\rho}$ unramified at w represent the same cohomology class if and only if the diagonal values of $f_1(\sigma_w)$ and $f_2(\sigma_w)$ are the same. Given any $x \in \mathbf{k}$, we see from the proof above that choosing a nice prime (at which f is unramified) with $f(\sigma_w) = x$ can be realized as a Ceboterov condition in K_f/F, with density $1/\#k$ within the set of nice primes. We make a similar convention for any dual cohomology class $\phi \in H^1(G_{F,S}, (\mathrm{Ad}^0 \overline{\rho})^*)$.

So far we've defined local conditions $\mathcal{D}_v$ for $v \in S$ and for nice primes. Throughout this chapter, we will use the symbols $\mathcal{D}_v, \mathcal{L}_v$ to denote these prescribed local conditions and their corresponding tangent spaces. For any set of nice primes Q, we denote the universal deformation ring with local conditions $\mathcal{D}_v$ imposed on the set $S \cup Q$ by $R^{S \cup Q}$.

3.3 The Construction

Finally, we can state and are ready to prove the main result of this work:

Theorem 3.3.1. *Let $p \geq 7$ be a prime and $\mathbf{k}$ be a finite field with characteristic p. Let F be a totally real field that is disjoint from $\mathbb{Q}(\mu_p)$. Suppose $\mathcal{R} = W(\mathbf{k})[[X_1, ..., X_n]]/(F_1, ..., F_n)$ is a reduced, finite flat complete intersection over the ring of Witt vectors $W(\mathbf{k})$. Let $\overline{\rho} : G_{F,S} \to GL_2(\mathbf{k})$ be a continuous, totally odd, residual representation with determinant χ (the cyclotomic character), whose image contains $\mathrm{SL}_2(\mathbf{k})$. Suppose $\bar{\rho}|_{G_v}$ takes the form of one of $B1, B2$ in section 3.1, for all $v|p$, then there exists a set of nice primes, Q, such that $R^{S \cup Q} \simeq \mathcal{R}$.*

We remark that the local conditions in section 3.1 are chosen for definiteness purpose. Theorem 3.3.1 holds as long as the local conditions provide the right numerics $\dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) = \dim H^1_{\mathcal{L}^\perp}(G_{F,S}, (\mathrm{Ad}^0\,\overline{\rho})^*)$.

We break our proof into several steps:

Proposition 3.3.2. *There exists a set of nice primes Q such that for any $T \supseteq S \cup Q$, $\text{Ш}^1_T((\mathrm{Ad}^0\,\overline{\rho})^*) = 0$. For any nice prime $w \notin T$, the inflation map $H^1(G_{F,T}, \mathrm{Ad}^0\,\overline{\rho}) \to H^1(G_{F,T\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho})$ has one-dimensional cokernel.*

Proof. Let $\phi_1, ..., \phi_r$ be basis of $H^1(G_{F,S}, (\mathrm{Ad}^0\,\overline{\rho})^*)$. Let $w_1, ..., w_r$ be nice primes such that $\phi_i(\sigma_{w_i}) \neq 0$ and $\phi_i(\sigma_{w_j}) = 0$ if $i \neq j$. Set $Q = \{w_1, ..., w_r\}$. The existence of such primes is guaranteed by Proposition 3.2.3 and its following discussion. Recall there is a natural injection $\text{Ш}^1_{S\cup Q}((\mathrm{Ad}^0\,\overline{\rho})^*) \to \text{Ш}^1_S((\mathrm{Ad}^0\,\overline{\rho})^*)$. If $\phi \in \text{Ш}^1_{S\cup Q}((\mathrm{Ad}^0\,\overline{\rho})^*)$, then $\phi = \sum_{i=1}^r a_i\phi_i$ with $a_i \in \mathbf{k}$. Since $\phi|_{G_{w_i}} = 0$, $0 = \phi(\sigma_{w_i}) = a_i\phi_i(\sigma_{w_i})$ and $a_i = 0$. This shows that $\phi = 0$ and $\text{Ш}^1_{S\cup Q}((\mathrm{Ad}^0\,\overline{\rho})^*) = 0$. As $T \supseteq S \cup Q$, $\text{Ш}^1_T((\mathrm{Ad}^0\,\overline{\rho})^*)$ injects into $\text{Ш}^1_{S\cup Q}((\mathrm{Ad}^0\,\overline{\rho})^*)$ and is of course trivial.

The last claim can be seen by setting local conditions $\mathcal{M}_v = H^1(G_v, \mathrm{Ad}^0\,\overline{\rho})$ for all $v \in T \cup \{w\}$ and applying Wiles' formula twice, first to the set T then to the set $T \cup \{w\}$. The increase on the left is $\dim H^1(G_{F,T\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho}) - \dim H^1(G_{F,T}, \mathrm{Ad}^0\,\overline{\rho})$ and the increase on the right is $\dim H^1(G_w, \mathrm{Ad}^0\,\overline{\rho}) - \dim H^0(G_w, \mathrm{Ad}^0\,\overline{\rho}) = 1$. □

Henceforth we will assume $\text{Ш}^1_S((\mathrm{Ad}^0\,\overline{\rho})^*) = 0$. By Global duality, $\text{Ш}^2_S(\mathrm{Ad}^0\,\overline{\rho}) = 0$.

We next adjust the Selmer group $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ to have the same dimension as the tangent space of $\mathcal{R}$, namely n.

Proposition 3.3.3. *1. Let $\phi_1, ..., \phi_r \in H^1_{\mathcal{L}^\perp}(G_{F,S}, (\mathrm{Ad}^0 \overline{\rho})^*)$ be linearly independent and $w_1, ..., w_r$ be nice primes such that $\phi_i|_{G_{w_i}} \neq 0$ and $\phi_i|_{G_{w_j}} = 0$ if $i \neq j$. Set $Q = \{w_1, ..., w_r\}$, then the maps*

$$H^1(G_{F,S}, \mathrm{Ad}^0 \overline{\rho}) \to \bigoplus_{v \in S} \frac{H^1(G_v, \mathrm{Ad}^0 \overline{\rho})}{\mathcal{L}_v} \text{ and}$$
$$H^1(G_{F,S \cup Q}, \mathrm{Ad}^0 \overline{\rho}) \to \bigoplus_{v \in S} \frac{H^1(G_v, \mathrm{Ad}^0 \overline{\rho})}{\mathcal{L}_v}$$

have the same kernel.

2. Let $f \in H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0 \overline{\rho})$ and $\phi \in H^1_{\mathcal{L}^\perp}(G_{F,S}, (\mathrm{Ad}^0 \overline{\rho})^*)$ be nonzero. If w is a nice prime such that $f(\sigma_w) \neq 0, \phi|_{G_w} \neq 0$. Then $\dim H^1_{\mathcal{L}}(G_{F,S \cup \{w\}}, \mathrm{Ad}^0 \overline{\rho}) = \dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0 \overline{\rho}) - 1$.

3. Let $\phi \in H^1_{\mathcal{L}^\perp}(G_{F,S}, (\mathrm{Ad}^0 \overline{\rho})^*)$ be nonzero. If w is a nice prime such that $H^1_{\mathcal{L}^\perp}(G_{F,S}, \mathrm{Ad}^0 \overline{\rho})|_{G_w} = 0$, $\phi|_{G_w} \neq 0$. Then $H^1_{\mathcal{L}}(G_{F,S \cup \{w\}}, \mathrm{Ad}^0 \overline{\rho}) = H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0 \overline{\rho})$.

4. There exists a set Q of one or two nice primes such that $\dim H^1_{\mathcal{L}}(G_{F,S \cup Q}, \mathrm{Ad}^0 \overline{\rho}) \geq \dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0 \overline{\rho}) + 1$.

We need the assumption $Ш^1_S((\mathrm{Ad}^0 \overline{\rho})^*) = 0$ in part (3) but not in parts (1), (2), (4).

Proof. 1. Let $Q_i = \{w_1, ..., w_i\}$. It suffices by induction to show that the maps

$$H^1(G_{F,S \cup Q_i}, \mathrm{Ad}^0 \overline{\rho}) \to \bigoplus_{v \in S} \frac{H^1(G_v, \mathrm{Ad}^0 \overline{\rho})}{\mathcal{L}_v} \text{ and}$$
$$H^1(G_{F,S \cup Q_{i+1}}, \mathrm{Ad}^0 \overline{\rho}) \to \bigoplus_{v \in S} \frac{H^1(G_v, \mathrm{Ad}^0 \overline{\rho})}{\mathcal{L}_v}$$

have the same kernel. We define local conditions $\mathcal{M}_v = \mathcal{L}_v$ for $v \in S$ and $\mathcal{M}_v = H^1(G_w, \mathrm{Ad}^0 \overline{\rho})$ for $v \in Q$. The kernels of the maps above are $H^1_{\mathcal{M}}(G_{F,S \cup Q_i}, \mathrm{Ad}^0 \overline{\rho})$ and $H^1_{\mathcal{M}}(G_{F,S \cup Q_{i+1}}, \mathrm{Ad}^0 \overline{\rho})$. Clearly

$H^1_{\mathcal{M}}(G_{F,S\cup Q_i}, \mathrm{Ad}^0\,\overline{\rho}) \subset H^1_{\mathcal{M}}(G_{F,S\cup Q_{i+1}}, \mathrm{Ad}^0\,\overline{\rho})$. Applying Wiles' formula to the sets $S \cup Q_i$ ant $S \cup Q_{i+1}$, we get

$$\begin{aligned} &\dim H^1_{\mathcal{M}}(G_{F,S\cup Q_{i+1}}, \mathrm{Ad}^0\,\overline{\rho}) - \dim H^1_{\mathcal{M}}(G_{F,S\cup Q_i}, \mathrm{Ad}^0\,\overline{\rho}) \\ =&\dim H^1_{\mathcal{M}^\perp}(G_{F,S\cup Q_{i+1}}, (\mathrm{Ad}^0\,\overline{\rho})^*) - \dim H^1_{\mathcal{M}^\perp}(G_{F,S\cup Q_i}, (\mathrm{Ad}^0\,\overline{\rho})^*) + 1 \end{aligned}$$

By former discussion, the left side of the equation is ≥ 0. As $\mathcal{M}^\perp_{w_{i+1}} = 0$, we have $H^1_{\mathcal{M}^\perp}(G_{F,S\cup Q_{i+1}}, (\mathrm{Ad}^0\,\overline{\rho})^*) \subset H^1_{\mathcal{M}^\perp}(G_{F,S\cup Q_i}, (\mathrm{Ad}^0\,\overline{\rho})^*)$. By assumption, ϕ_{i+1} is in $H^1_{\mathcal{M}^\perp}(G_{F,S\cup Q_i}, (\mathrm{Ad}^0\,\overline{\rho})^*)$ but not in $H^1_{\mathcal{M}^\perp}(G_{F,S\cup Q_{i+1}}, (\mathrm{Ad}^0\,\overline{\rho})^*)$, so the containment is proper. This implies the right side of the equation above is ≤ 0, which forces both sides of the equation to be 0. We conclude that $H^1_{\mathcal{M}}(G_{F,S\cup Q_i}, \mathrm{Ad}^0\,\overline{\rho}) = H^1_{\mathcal{M}}(G_{F,S\cup Q_{i+1}}, \mathrm{Ad}^0\,\overline{\rho})$.

2. By definition $H^1_{\mathcal{L}}(G_{F,S\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho})$ is the kernel of

$$H^1(G_{F,S\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho}) \to \bigoplus_{v\in S} \frac{H^1(G_v, \mathrm{Ad}^0\,\overline{\rho})}{\mathcal{L}_v} \bigoplus \frac{H^1(G_w, \mathrm{Ad}^0\,\overline{\rho})}{\mathcal{L}_w},$$

which is clearly contained in the kernel of

$$H^1(G_{F,S\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho}) \to \bigoplus_{v\in S} \frac{H^1(G_v, \mathrm{Ad}^0\,\overline{\rho})}{\mathcal{L}_v},$$

which is the same as $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ by part (1). The codimension of the containment $H^1_{\mathcal{L}}(G_{F,S\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho}) \hookrightarrow H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ is 0 or 1, as $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ maps trivially to the 1-dimensional space $H^1(G_w, \mathrm{Ad}^0\,\overline{\rho})/\mathcal{L}_w$ or not. The latter situation occurs because by assumption the restriction of $f \in H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ to G_w is not in $\mathcal{L}_w$. Therefore, $\dim H^1_{\mathcal{L}}(G_{F,S\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho}) = \dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) - 1$.

3. As in the proof of (2), we have an inclusion $H^1_{\mathcal{L}}(G_{F,S\cup\{w\}}, \mathrm{Ad}^0\,\overline{\rho}) \hookrightarrow H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ whose codimension is 0 or 1, depending on whether $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ maps trivially to the 1-dimensional space $H^1(G_w, \mathrm{Ad}^0\,\overline{\rho})/\mathcal{L}_w$ or not. The former case occurs.

4. By Proposition 10 in [6], we may find a set Q of one or two nice primes and a nontrivial $f \in H^1(G_{F,S\cup Q}, \mathrm{Ad}^0\,\overline{\rho})$ such that

   - $f(\sigma_w) = 0$ for all $w \in Q$,
   - $f|_{G_v} = 0$ for all $v \in S$.

   The prime(s) in Q are chosen in a way to satisfy several independent Cebotarev conditions imposed on a linearly independent subset of the dual cohomology, and in addition, on an element in $H^1(G_{F,S\cup\{w_1\}}, \mathrm{Ad}^0\,\overline{\rho}) \setminus H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ if $Q = \{w_1, w_2\}$ contains two nice primes. The point is, we may (and do) further require that $H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})|_{G_w} = 0$ for all $w \in Q$; this is a Cebotarev condition independent from the previously mentioned ones. Now since $H^1(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$ is trivial at the primes in Q, $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) \subseteq H^1_{\mathcal{L}}(G_{F,S\cup Q}, \mathrm{Ad}^0\,\overline{\rho})$. This containment is proper because f is an element in $H^1_{\mathcal{L}}(G_{F,S\cup Q}, \mathrm{Ad}^0\,\overline{\rho})$ but not in $H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho})$.

□

By parts (2) and (4) of Proposition 3.3.3, we can assume henceforth that $\dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) = n$. We will eventually need to enlarge the set S of ramifications by adding more nice primes. Every time we've done so we will make sure the dimension of the Selmer group is preserved.

We next show that universal deformation has large image. We say $\rho_R : G_{F,S} \to \mathrm{GL}_2(R)$ has full image if $\mathrm{Im}(\rho_R) \supseteq \mathrm{SL}_2(R)$. The following lemma is due to Boston, see the appendix of [11].

Lemma 3.3.4. *Let R be a coefficient ring, $\rho_R : G_{F,S} \to \mathrm{GL}_2(R)$ be a representation and $\rho_{R/\mathfrak{m}_R^2} : G_{F,S} \to \mathrm{GL}_2(R/\mathfrak{m}_R^2)$ be its projection. Then ρ_R has full image if and only if $\rho_{R/\mathfrak{m}_R^2}$ has full image.*

Lemma 3.3.5. *Let R be a coefficient ring with residue field $\mathbf{k}$ and $\mathfrak{m}$ be its maximal ideal. Let $\mathcal{G}$ be a subgroup of $\mathrm{SL}_2(R/\mathfrak{m}^2)$. If $\mathcal{G}$ surjects onto $\mathrm{SL}_2(R/(pR+\mathfrak{m}^2))$ under the natural projection, then $\mathcal{G} = \mathrm{SL}_2(R/\mathfrak{m}^2)$.*

Proof. We will write $R/\mathfrak{m}^2$ as R and keep in mind that $\mathfrak{m}$ is square-zero. We need to show that if $\mathcal{G}$ is a subgroup of $\mathrm{SL}_2(R)$ that surjects onto $\mathrm{SL}_2(R/pR)$, then $\mathcal{G} = \mathrm{SL}_2(R)$. Given $A \in \mathrm{SL}_2(R)$, we will denote its projection to $\mathrm{SL}_2(R/pR)$ by $\overline{A}$.

Let $A \in \mathrm{SL}_2(R)$, and let $\overline{A}^{-1}$ be the inverse of $\overline{A} \in \mathrm{SL}_2(R/pR)$. By assumption, there exists $B \in \mathcal{G}$ that lifts $\overline{A}^{-1}$. To show that $A \in \mathcal{G}$, it suffices to show that $AB \in \mathcal{G}$. Note that $\overline{AB} = \overline{I} \in \mathrm{SL}_2(R/pR)$. Therefore, we may assume afresh that A is a matrix such that $\overline{A} = \overline{I}$. Our goal is to prove $A \in \mathcal{G}$.

Since $\overline{A} = \overline{I}$, we can write $A = I + pU$ for some $U \in M_2(R)$. The condition $\det(A) = 1$ implies U is a traceless matrix. Note that U can be written as the sum of square-zero traceless matrices, say $U_1, ..., U_n$. For example,

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \frac{1}{2}\begin{pmatrix} a & -a \\ a & -a \end{pmatrix} + \frac{1}{2}\begin{pmatrix} a & a \\ -a & -a \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}.$$

Since $I + p(\sum_i U_i) = \prod_i (I + pU_i)$, it's enough to show that $I + pU_i \in \mathcal{G}$. Hence, we may assume $U^2 = 0$. Observe that $\overline{I} + \overline{U} \in \mathrm{SL}_2(R/pR)$, so by assumption there is a matrix $C \in \mathcal{G}$ that lifts $\overline{I} + \overline{U}$. It has the form $C = I + U + pV$ for some $V \in M_2(R)$. Using the facts $U^2 = 0$, $\mathfrak{m}^2 = 0$ and $p \geq 5$, one checks that $C^p = (I+U+pV)^p = I + p(U+pV) + \binom{p}{2}(U+pV)^2 + ... + (U+pV)^p = I + pU = A$. We conclude that $A \in \mathcal{G}$. $\square$

Proposition 3.3.6. *Recall $\overline{\rho}$ has full image. As above, let R^S be the universal deformation ring and let $\rho_{R^S} : G_{F,S} \to \mathrm{GL}_2(R^S)$ be the universal deformation to the deformation problem with local conditions $\mathcal{L}_v$ imposed on the set S. Then ρ_{R^S}*

has full image.

Proof. For simplicity, write $G = G_{F,S}$, $R = R^S$, $\mathfrak{m} = \mathfrak{m}_R$. By the two lemmas above, it suffices to show that the projection $\rho_{R/(pR+\mathfrak{m}^2)} : G \to \mathrm{GL}_2(R/(pR+\mathfrak{m}^2))$ has full image. Recall from Theorem 1.2.4 there's an equivalence

$$\mathrm{Hom}_{\mathbf{k}-\mathrm{alg}}(R/(pR+\mathfrak{m}^2), \mathbf{k}[\epsilon]) \simeq \mathrm{Hom}_{\mathbf{k}-\mathrm{v.sp}}(\mathfrak{m}/(pR+\mathfrak{m}^2), \mathbf{k}) \simeq H^1_{\mathcal{L}}(G, \mathrm{Ad}^0\,\overline{\rho}).$$

Explicitly, let $R = W(\mathbf{k})[[T_1, ..., T_n]]/I$ so that $R/(pR+\mathfrak{m}^2) \simeq \mathbf{k} \oplus \mathfrak{m}/(pR+\mathfrak{m}^2) \simeq \mathbf{k}\oplus(\mathbf{k}\tilde{T}_1\oplus ...\oplus\mathbf{k}\tilde{T}_n)$, where $\tilde{T}_i$ is the image of T_i. Let $e_i^* \in \mathrm{Hom}_{\mathbf{k}-\mathrm{v.sp}}(\mathfrak{m}/(pR+\mathfrak{m}^2), \mathbf{k})$ be the functional that maps $\tilde{T}_i$ to 1 and $\tilde{T}_j$ to 0 if $j \neq i$. Suppose e_i^* corresponds to the element $f_i \in H^1_{\mathcal{L}}(G, \mathrm{Ad}^0\,\overline{\rho})$ under the equivalence above. Then explicitly,

$$\rho_{R/(pR+\mathfrak{m}^2)} = (I + \sum f_i\tilde{T}_i)\overline{\rho}. \tag{3.1}$$

We claim that $\mathrm{Im}(\rho_{R/(pR+\mathfrak{m}^2)})$ contains $(I \oplus_i \mathrm{Ad}^0\,\overline{\rho}\tilde{T}_i) \times \mathrm{SL}_2(\mathbf{k})$, which in turns contains $\mathrm{SL}_2(R/(pR+\mathfrak{m}^2))$. We leave the latter containment as an exercise. To prove the former containment, we only need to note that for any $A \in \mathrm{SL}_2(\mathbf{k})$ and $B_1, ..., B_n \in \mathrm{Ad}^0\,\overline{\rho}$, we can find by Proposition 3 a prime w such that $\overline{\rho}(\sigma_w) = A$ and $f_i(\sigma_w) = B_i$. Then $\rho_{R/(pR+\mathfrak{m}^2)}(\sigma_w) = (I + \sum B_i\tilde{T}_i)A$ represents a general element in $(I \oplus_i \mathrm{Ad}^0\,\overline{\rho}\tilde{T}_i) \times \mathrm{SL}_2(\mathbf{k})$. □

Recall $\mathcal{R} = W(\mathbf{k})[[X_1, ..., X_n]]/(F_1, ..., F_n)$ is a reduced, finite flat complete intersection. By Corollary 2.2.5 of Chapter 2, there exists a sufficiently large N such that, if R is a quotient of $W(k)[[X_1, ..., X_n]]$ by an ideal generated by at most n elements and if $R \to R/p^N R$ is a surjection which induces an isomorphism $R/pR \simeq \mathcal{R}/p\mathcal{R}$, then $R \simeq \mathcal{R}$ as W-algebras. Moreover, by lemma 2.2.2 of chapter 2, there exists an integer M such that $(p, X_1, ..., X_n)^M \subset (F_1, ..., F_n, p^N)$. We will choose M large enough so that it also satisfies $(p, X_1, ..., X_n)^M \subset (F_1, ..., F_n, p)(p, X_1, ..., X_n)$.

Set

$$A = W(\mathbf{k})[[X_1, ..., X_n]]/(p, X_1, ..., X_n)^M$$

and

$$B = \mathcal{R}/(p, X_1, ..., X_n)^M = W(\mathbf{k})[[X_1, ..., X_n]]/((F_1, ..., F_n) + (p, X_1, ..., X_n)^M).$$

We have $A \twoheadrightarrow B$.

Recall R^S is the universal deformation ring associated to the set S. We first build a lift of $\rho_{R^S/(pR^S+\mathfrak{m}_{R^S}^2)}$ to $\mathrm{GL}_2(A)$.

Proposition 3.3.7. *There exists a set of nice primes Q and a lift $\rho_A : G_{F,S\cup Q} \to \mathrm{GL}_2(A)$ of $\rho_{R^S/(pR^S+\mathfrak{m}_{R^S}^2)}$ such that $\rho_A|_{G_v} \in \mathcal{D}_v$ for all $v \in S \cup Q$. Moreover, $H^1_{\mathcal{L}}(G_{F,S\cup Q}, \mathrm{Ad}^0 \overline{\rho}) = H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0 \overline{\rho})$.*

Proof. The idea is that of [17] and we only sketch the proof. There is a chain of small, index-$\#k$ extensions of coefficient rings:

$$A_s := A \twoheadrightarrow A_{s-1} \twoheadrightarrow ... \twoheadrightarrow A_1 \twoheadrightarrow A_0 := R^S/(pR^S + \mathfrak{m}_{R^S}^2).$$

Suppose by induction hypothesis that we've found a set of nice primes Q_i and a lift $\rho_{A_i} : G_{F,S\cup Q_i} \to \mathrm{GL}_2(A_i)$ of $\rho_{R^S/(pR^S+\mathfrak{m}_{R^S}^2)}$ such that $\rho_{A_i}|_{G_v} \in \mathcal{D}_v$ for all $v \in S \cup Q_i$. We will lift ρ_{A_i} to $\mathrm{GL}_2(A_{i+1})$. Triviality of $Ш^2_S(Ad^0\overline{\rho})$ signifies any global obstruction can be realized locally. The local deformation problems are unobstructed because $\rho_{A_i}|_{G_v} \in \mathcal{D}_v$ for all $v \in S \cup Q_i$. Thus there is a $\rho'_{A_{i+1}} : G_{F,S\cup Q_i} \to \mathrm{GL}_2(A_{i+1})$ that lifts ρ_{A_i}. Let J be the kernel of $A_{i+1} \to A_i$. There are local cohomology classes $z_v \in H^1(G_v, \mathrm{Ad}^0 \overline{\rho} \otimes J) \simeq H^1(G_v, \mathrm{Ad}^0 \overline{\rho})$ such that $(I + z_v)\rho'_{A_{i+1}}|_{G_v} \in \mathcal{D}_v$ for $v \in S \cup Q_i$. Note that z_v is unique up to elements of $\mathcal{L}_v$.

Let $\Phi : H^1(G_{F,S\cup Q_i}, \mathrm{Ad}^0 \overline{\rho}) \to \oplus_{v\in S\cup Q_i} H^1(G_v, \mathrm{Ad}^0 \overline{\rho})$ be the natural restriction map. If $(z_v)_{v\in S\cup Q_i} \in \oplus_{v\in S\cup Q_i}\mathcal{L}_v \oplus \Phi(H^1(G_{F,S\cup Q_i}, \mathrm{Ad}^0 \overline{\rho}))$, there's a

$h \in H^1(G_{F,S\cup Q_i}, \mathrm{Ad}^0\,\overline{\rho})$ such that $h|_{G_v} \equiv z_v \bmod \mathcal{L}_v$ for all $v \in S \cup Q_i$. Then $\rho_{A_{i+1}} := (I + h)\rho'_{A_{i+1}} : G_{F,S\cup Q_i} \to \mathrm{GL}_2(A_{i+1})$ is the desired lift. In this case $Q_{i+1} = Q_i$, so the Selmer group is preserved.

If $(z_v)_{v\in S\cup Q_i} \notin \oplus_{v\in S\cup Q_i}\mathcal{L}_v \oplus \Phi(H^1(G_{F,S\cup Q_i}, \mathrm{Ad}^0\,\overline{\rho}))$, we apply Proposition 3.6 in [17] to get a set T of one or two ρ_{A_i}-nice primes and a $f \in H^1(G_{F,S\cup Q_i\cup T}, \mathrm{Ad}^0\,\overline{\rho})$ such that $f(\sigma_w) = 0$ for $w \in T$ and $h|_{G_v} = z_v$ for $v \in S \cup Q_i$. Then $\rho_{A_{i+1}} := (1 + f)\rho'_{A_{i+1}} : G_{F,S\cup Q_i\cup T} \to \mathrm{GL}_2(A_{i+1})$ is a lift of ρ_{A_i} that satisfies $\rho_{A_{i+1}}|_{G_v} \in \mathcal{L}_v$ for all $v \in S \cup Q_i \cup T$. In this case we take $Q_{i+1} = Q_i \cup T$. A straight repeat of proposition 4.1 in [17] gives that $H^1_{\mathcal{L}}(G_{F,S\cup Q_{i+1}}, \mathrm{Ad}^0\,\overline{\rho}) = H^1_{\mathcal{L}}(G_{F,S\cup Q_i}, \mathrm{Ad}^0\,\overline{\rho})$, which completes the induction.

To prove fullness of $\rho_A : G_{S\cup Q} \to \mathrm{GL}_2(A)$, it suffices by lemmas 3.3.4 and 3.3.5 to prove the fullness of the induced map $\rho_{A/(pA+\mathfrak{m}_A^2)} : G_{S\cup Q} \to \mathrm{GL}_2(A/(pA+\mathfrak{m}_A^2))$, but the latter map is the same as $\rho_{R^S/(pR^S+\mathfrak{m}_{R^S}^2)}$, which has full image by Proposition 3.3.6. □

Rename the set $S\cup Q$ we found in the above proposition to S. As a brief recap, by adding nice primes to the set S if necessary, we have $\dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) = n$ and a deformation $\rho_A : G_{F,S} \to GL_2(A)$ of $\overline{\rho}$ such that $\rho|_{G_v} \in \mathcal{D}_v$ for all $v \in S$. Let ρ_B be the composition $G_{F,S} \xrightarrow{\rho_A} GL_2(A) \to GL_2(B)$.

Let $\phi_1, ..., \phi_n$ be a basis of $H^1_{\mathcal{L}}(G_{F,S}, (\mathrm{Ad}^0\,\overline{\rho})^*)$. For $1 \le i \le n$, we define Q_i to be the set of nice primes w that satisfy the following properties:

1. $H^1_{\mathcal{L}}(G_{F,S}, Ad^0\overline{\rho})|_{G_w} = 0$
2. $\phi_1, ..., \phi_{i-1}, \phi_{i+1}, ..., \phi_n|_{G_w} = 0$ and $\phi_i|_{G_w} \neq 0$
3. w is ρ_B-nice

4. $\rho_A(\sigma_w) = \begin{pmatrix} \chi(\sigma_w)(1+F_i) & 0 \\ 0 & (1+F_i)^{-1} \end{pmatrix}$

Proposition 3.3.8. *The set Q_i is not empty.*

Proof. The second condition is a $(\mathrm{Ad}^0 \overline{\rho})^*$ conditions over $F(\overline{\rho})$, while the others are $\mathrm{Ad}^0 \overline{\rho}$ conditions over $F(\overline{\rho})$, so we only need to check conditions (1), (3), (4) are compatible.

We first show that (3) and (4) can be satisfied simultaneously. Indeed, choose integer $x \not\equiv \pm 1 \bmod p$. By raising it to a sufficiently large power of p, we may assume that the order of x in B is the same as that in $\mathbf{k}$. Using the fullness of ρ_A and the fact that ρ_A has determinant χ, one easily sees that $\begin{pmatrix} x(1+F_i) & 0 \\ 0 & (1+F_i)^{-1} \end{pmatrix} \in \mathrm{Im}(\rho_A)$. Let w be a prime of F unramified in $F(\rho_A)$ with Frobenius in the conjugacy class of $\begin{pmatrix} x(1+F_i) & 0 \\ 0 & (1+F_i)^{-1} \end{pmatrix} \in \mathrm{Gal}(F(\rho_A)/F)$. Then necessarily $\chi(\sigma_w) = x$ and $\rho_A(\sigma_w) = \begin{pmatrix} \chi(\sigma_w)(1+F_i) & 0 \\ 0 & (1+F_i)^{-1} \end{pmatrix}$. It follows that $\rho_B(\sigma_w) = \begin{pmatrix} \chi(\sigma_w) & 0 \\ 0 & 1 \end{pmatrix}$ because $F_i = 0$ in B. By our assumption on the order of x, w is ρ_B-nice.

Lastly, we show that the fourth condition entails the first. Indeed, suppose (4) holds. Then we have $\rho_{A/(pA+\mathfrak{m}_A^2)}(\sigma_w) = \begin{pmatrix} \chi(\sigma_w) & 0 \\ 0 & 1 \end{pmatrix} = \overline{\rho}(\sigma_w)$. In view of the correspondence described in the proof of Proposition 3.3.6, in particular, equation

(3.3) in that proof, (Note that A and the universal deformation ring R^S have the same "pre-cotangent": $A/(pA+\mathfrak{m}_A^2) = R^S/(pR^S+\mathfrak{m}_{R^S}^2)$.) we see that $f_i(\sigma_w)=0$ for any basis element $f_i \in H^1_{\mathcal{L}}(G_{F,S}, Ad^0\overline{\rho}) = 0$. □

Pick $w_i \in Q_i$, and let $Q = \{w_1, ..., w_n\}$. Let $R^{S\cup Q}$, $\rho_{R^{S\cup Q}}$ be the universal deformation ring and universal deformation associated to the set $S \cup Q$. Finally, we prove the main theorem:

Theorem 3.3.9. $R^{S\cup Q} \simeq \mathcal{R}$

Proof. Using part (3) of Proposition 3.3.3, we see that $\dim H^1_{\mathcal{L}}(G_{F,S\cup Q}, \mathrm{Ad}^0\,\overline{\rho}) = \dim H^1_{\mathcal{L}}(G_{F,S}, \mathrm{Ad}^0\,\overline{\rho}) = n$. Therefore, $R^{S\cup Q}$ is a quotient of $W(\mathbf{k})[[X_1, ..., X_n]]$ by an ideal generated by at most $\dim H^1_{\mathcal{L}}(G_{F,S\cup Q}, \mathrm{Ad}^0\,\overline{\rho}) = n$ power series by Theorem 1.2.6. Moreover, since the primes in Q are ρ_B-nice, there's a surjection $R^{S\cup Q} \twoheadrightarrow B$ by universality. (Indeed, it can be shown that fullness of $\rho_{B/(pB+\mathfrak{m}_B^2)}$ implies the map $R^{S\cup Q}/(pR^{S\cup Q}+\mathfrak{m}_{R^{S\cup Q}}^2) \to B/(pB+\mathfrak{m}_B^2)$ is surjective, which in turns implies that $R^{S\cup Q} \to B$ is surjective by Nakayama.) By definition of B, there's a surjection $B \twoheadrightarrow \mathcal{R}/p^N\mathcal{R}$, which induces $R^{S\cup Q} \twoheadrightarrow \mathcal{R}/p^N\mathcal{R}$. By Proposition 2.2.5, it suffices to show that the induced map $R^{S\cup Q}/pR^{S\cup Q} \to \mathcal{R}/p\mathcal{R}$ is an isomorphism.

Suppose this is not true, then $R^{S\cup Q}/pR^{S\cup Q}$ surjects onto one of the small, index-$\#\mathbf{k}$ extensions $D = W(k)[[X_1, ..., X_n]]/J$ of $\mathcal{R}/p\mathcal{R} = W(k)[[X_1, ..., X_n]]/(F_1, ..., F_n, p)$. An easy application of Nakayama's lemma gives $J \supseteq (F_1, ..., F_n, p)(p, X_1, ..., X_n)$. Recall that the integer M is chosen to satisfy $(p, X_1, ..., X_n)^M \subset (F_1, ..., F_n, p)(p, X_1, ..., X_n)$, so A surjects onto D.

Denote the composition $G_{F,S\cup Q} \xrightarrow{\rho_{R^{S\cup Q}}} \mathrm{GL}_2(R^{S\cup Q}) \to \mathrm{GL}_2(D)$ by $\rho_D^{(1)}$, and the composition $G_{F,S\cup Q} \to G_{F,S} \xrightarrow{\rho_A} \mathrm{GL}_2(A) \to \mathrm{GL}_2(D)$ by $\rho_D^{(2)}$. Since $(p) \subset J \subsetneq (p, F_1, ..., F_n)$, $F_i \notin J$ for some i. But then $\rho_D^{(2)}(\sigma_{w_i}) = \rho_A(\sigma_{w_i}) \bmod J =$

$\begin{pmatrix} \chi(\sigma_{w_i})(1+F_i) & 0 \\ 0 & (1+F_i)^{-1} \end{pmatrix} \bmod J \neq \begin{pmatrix} \chi(\sigma_{w_i}) & 0 \\ 0 & 1 \end{pmatrix} \bmod J$. In other words, $\rho_D^{(2)}|_{G_{w_i}} \notin \mathcal{D}_{w_i}$. On the other hand, being induced from the universal deformation $G_{F,S\cup Q} \to GL_2(R^{S\cup Q}), \rho_D^{(1)}|_{G_{w_i}} \in \mathcal{D}_{w_i}$. Note that composing $\rho_D^{(1)}$ or $\rho_D^{(2)}$ with $\mathrm{GL}_2(D) \to \mathrm{GL}_2(\mathcal{R}/p\mathcal{R})$ gives the same map because both compositions factor through $\mathrm{GL}_2(B)$. Therefore, $\rho_D^{(1)}$ and $\rho_D^{(2)}$ differ by a class $z \in H^1(G_{S\cup Q}, Ad^0\overline{\rho}\otimes I) \simeq H^1(G_{S\cup Q}, Ad^0\overline{\rho})$, where I is the kernel of the small extension $D \twoheadrightarrow \mathcal{R}/p\mathcal{R}$. That is, $\rho_D^{(1)} = (I+z)\rho_D^{(2)}$. We know that $\rho_D^{(1)}, \rho_D^{(2)} \in \mathcal{D}_v$ for all $v \in S$, so $z|_{G_v} \in \mathcal{L}_v$ for all $v \in S$. But then since the maps

$$H^1(G_{F,S\cup Q}, Ad^0\overline{\rho}) \to \oplus_{v\in S}\frac{H^1(G_v, Ad^0\overline{\rho})}{\mathcal{L}_v} \quad \text{and}$$
$$H^1(G_{F,S}, Ad^0\overline{\rho}) \to \oplus_{v\in S}\frac{H^1(G_v, Ad^0\overline{\rho})}{\mathcal{L}_v}$$

have the same kernel by part 1 of Proposition 3.3.3, we have $z \in H^1_{\mathcal{L}}(G_{F,S}, Ad^0\overline{\rho})$. Recall that w_i is chosen to satisfy $H^1_{\mathcal{L}}(G_{F,S}, Ad^0\overline{\rho})|_{G_{w_i}} = 0$, so $z|_{G_{w_i}} = 0$. This is impossible as $\rho_D^{(1)}|_{G_{w_i}} \in \mathcal{D}_v$ while $\rho_D^{(2)}|_{G_{w_i}} \notin \mathcal{D}_v$. □

BIBLIOGRAPHY

[1] D. A. Bayer. *THE DIVISION ALGORITHM AND THE HILBERT SCHEME*. ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)–Harvard University.

[2] G. Böckle. A local-to-global principle for deformations of Galois representations. *J. Reine Angew. Math.*, 509:199–236, 1999.

[3] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[4] T. Gee. Companion forms over totally real fields. II. *Duke Math. J.*, 136(2):275–284, 2007.

[5] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II. *Ann. of Math. (2)* **79** *(1964), 109–203; ibid. (2)*, 79:205–326, 1964.

[6] C. Khare, M. Larsen, and R. Ramakrishna. Constructing semisimple p-adic Galois representations with prescribed properties. *Amer. J. Math.*, 127(4):709–734, 2005.

[7] C. Khare and R. Ramakrishna. Lifting torsion Galois representations. *Forum Math. Sigma*, 3:e14, 37, 2015.

[8] B. Lundell. *Selmer groups and ranks of Hecke rings*. ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–Cornell University.

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

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

[11] B. Mazur and A. Wiles. On p-adic analytic families of Galois representations. *Compositio Math.*, 59(2):231–264, 1986.

[12] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006.

[13] A. Pande. Deformations of Galois representations and the theorems of Sato-Tate and Lang-Trotter. *Int. J. Number Theory*, 7(8):2065–2079, 2011.

[14] S. Patrikis. Deformations of Galois representations and exceptional monodromy. *Invent. Math.*, 205(2):269–336, 2016.

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

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

[17] R. Ramakrishna. Constructing Galois representations with very large image. *Canad. J. Math.*, 60(1):208–221, 2008.

[18] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, second edition, 1989. With the collaboration of Willem Kuyk and John Labute.

[19] M. Talpo and A. Vistoli. Deformation theory from the point of view of fibered categories. In *Handbook of moduli. Vol. III*, volume 26 of *Adv. Lect. Math. (ALM)*, pages 281–397. Int. Press, Somerville, MA, 2013.

[20] R. Taylor. On icosahedral Artin representations. II. *Amer. J. Math.*, 125(3):549–566, 2003.

[21] L. C. Washington. Galois cohomology. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 101–120. Springer, New York, 1997.

[22] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[23] O. Zariski and P. Samuel. *Commutative algebra. Vol. II.* Springer-Verlag, New York-Heidelberg, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.