GALOIS DEFORMATIONS

GAL PORAT

ABSTRACT. These notes are my attempt to understand basic aspects of the theory of Galois deformations, with emphasis on examples.

CONTENTS

1.	Generalities	1
2.	Tangent Spaces	3
3.	Mazur's theorem on H^2	5
4.	Functorial properties	7
4.1.	Conjugation	7
4.2.	Duality	7
4.3.	Determinant	7
4.4.	Tensor product	8
4.5.	Change of group	8
5.	Rigid Analytic Fibers	8
6.	Dimension Formulas	9
6.1.	The case where $G = G_{\mathbb{Q}_p}$	9
6.2.	The case where $G = G_{\mathbb{Q},S}$	10
7.	Examples	10
7.1.	Deformations in dimension 1	10
7.2.	G prime to p	10
7.3.	Deformations of finite cyclic groups	11
7.4.	Other explicit examples	13

1. GENERALITIES

Choose a prime p and an n such that $p \nmid n$. Given a profinite group G, we say it satisfies Mazur's condition Φ_p if for any $\Delta < G$ of finite index, the quotient $\Delta/[\Delta, \Delta]\Delta^p$ is finite. In practice, this assumption will hold for any group we consider.

From now on, fix a group G satisfying Mazur's condition Φ_p. For simplicity, in this note we will work only with the residue field $\mathbb{F}_p$. Thus, let $\mathcal{C}$ be the category of complete noetherian local $\mathbb{Z}_p$-algebras with residue field $\mathbb{F}_p$, with local morphisms. We have a functor

$$\mathcal{D}^\square : \mathcal{C} \to \mathrm{Sets},$$
$$\mathcal{D}^\square(A) = \{\rho : G \to \mathrm{GL}_n(A), \rho \mod \mathrm{m}_A = \overline{\rho}\} = \{\text{lifts of } \overline{\rho} \text{ to } \mathrm{GL}_n(A)\},$$

and the functor

$$\mathcal{D} : \mathcal{C} \to \mathrm{Sets},$$
$$\mathcal{D}(A) = \{\rho : G \to \mathrm{GL}_n(A), \rho \mod \mathrm{m}_A = \overline{\rho}\} / \{\text{conjugation}\} = \{\text{lifts of } \overline{\rho} \text{ to } \mathrm{GL}_n(A)\} / \{\text{conjugation}\}.$$

In order to state the following result, we need a to give two reminder regarding representations. We say $\overline{\rho}$ is *absolutely irreducible* if it remains irreducible after any finite extension of $\mathbb{F}_p$. We say $\overline{\rho}$ is *Schur* if $\mathrm{End}_{\mathbb{F}_p[G]}\overline{\rho} = \mathbb{F}_p$; note that if $\overline{\rho}$ is absolutely irreducible, it is also Schur.

Theorem 1.1. *1. The functor $\mathcal{D}^\square$ is representable by a representation $\rho^\square : G \to R^\square_{\overline{\rho}}$.*
2. If $\overline{\rho}$ is Schur, the functor $\mathcal{D}$ is representable by a representation $\rho^{\mathrm{univ}} : G \to R^{\mathrm{univ}}_{\overline{\rho}}$.

We call $R^\square_{\overline{\rho}}$ the *universal lifting ring* and $R^{\mathrm{univ}}_{\overline{\rho}}$ the *univesal deformation ring.*
Proof sketch of 1. Take

$$R = \mathbb{Z}_p[[X^g_{ij}]]_{1\leq i,j\leq n}/I,$$

where I is the ideal generated by the following relations: for each relation $r(g_1, ..., g_k) = 1$ in G, we have the relations which are the entries in the equality $\left(X^{g_1}_{ij}\right) \cdot ... \cdot \left(X^{g_k}_{ij}\right) = I$.
Now let J be the ideal in R which is the kernel of $R \to \mathbb{F}_p$ sending $\left(X^g_{ij}\right)$ to $\overline{p}(g)$. Then take $R^\square_{\overline{\rho}}$ to be the completion $R^\wedge_J$. ∎

In the case where $\overline{\rho}$ is absolutely irreducible, its liftings and deformations can be studied via its traces, according to the following lemma of Carayol.

Lemma 1.1. *Let $\overline{\rho}$ be absolutely irreducible, let $A \in \mathcal{C}$ and let $\rho \in \mathcal{D}^\square(A)$.*
1. If $a \in \mathrm{GL}_n(A)$ and $a\rho a^{-1} = \rho$ then $a \in A^\times$. In other words, the centraliser of ρ is as small as possible.
2. If $\rho' \in \mathcal{D}^\square(A)$ and $\mathrm{Tr}(\rho') = \mathrm{Tr}(\rho)$ then ρ and ρ' are equal in $\mathcal{D}(A)$.

In the case where $\overline{\rho}$ is absolutely irreducible, we can use the previous lemma to relate $R^\square_{\overline{\rho}}$ and $R^{\mathrm{univ}}_{\overline{\rho}}$.

Theorem 1.2. *If $\overline{\rho}$ is absolutely irreducible then $R^\square_{\overline{\rho}}$ is a power series over $R^{\mathrm{univ}}_{\overline{\rho}}$ in $n^2 - 1$ variables.*

Proof. We shall show

$$\rho^\square : G \to \mathrm{GL}_n(R^{\mathrm{univ}}_{\overline{\rho}}[[X_{i,j}]]_{i,j=1...,n}/X_{1,1}),$$

given by sending g to $(I + X_{i,j})\rho_{\mathrm{univ}}(I + X_{i,j})^{-1}$ in the universal lifting.
Indeed, let $A \in \mathcal{C}$. Then we must show that there is a natural isomorphism

$$\mathrm{Hom}(R^{\mathrm{univ}}_{\overline{\rho}}[[X_{i,j}]]_{i,j=1...,n}/X_{1,1}, A) \cong \mathcal{D}^\square(A).$$

Well, we have

$$\mathrm{Hom}(R^{\mathrm{univ}}_{\overline{\rho}}[[X_{i,j}]]_{i,j=1\ldots,n}/X_{1,1}, A) = \mathrm{Hom}(R^{\mathrm{univ}}_{\overline{\rho}}, A) \times \mathcal{M}(A)$$
$$= \{\text{lifts of } \overline{\rho} \text{ to } \mathrm{GL}_n(A)\} \,/\, \{\text{conjugation}\} \times (I + \mathcal{M}(A)),$$

where $\mathcal{M}(A)$ is the set of matrices in A which are of the form (X_{ij}) with $X_{11} = 0$ and $X_{ij} \in \mathrm{m}_A$. Finally, we have

$$\{\text{lifts of } \overline{\rho} \text{ to } \mathrm{GL}_n(A)\} \,/\, \{\text{conjugation}\} \times (I + \mathcal{M}(A)) \to \mathcal{D}^{\square}(A),$$
$$(A, B) \mapsto BAB^{-1},$$

and we wish to show this is a bijection. This amounts to the claim that any representation ρ' conjugate to ρ and reducing to $\overline{\rho}$ will be conjugate to it by a unique matrix in $I + \mathcal{M}(A)$. However it is clear that ρ' will be conjugate to ρ by a matrix in $I + M_n(\mathrm{m}_A)$, by part 2 of the previous lemma, and the amibguity in the choice is precisely given by those matrices commuting with ρ. By the previous lemma, these are just the scalar matrices. Thus each ρ' is conjugate to ρ by a matrix in $I + M_n(\mathrm{m}_A)$ which is unique up to scaling. But $I + \mathcal{M}(A)$ precisely gives a choice of represenatives for this equivalence relation. □

2. Tangent Spaces

The most simple geometric property of $R^{\square}_{\overline{\rho}}$ and $R^{\mathrm{univ}}_{\overline{\rho}}$ is its dimension. It is useful to study it by studying instead the tangent space at the origin. Recall however that the dimension of the tangent space only counts in some sense the minimal number of generators in any presentation, and not necessarily the actual Krull dimension. The situation when these are the same (up to reducing mod p) is the case where our rings are regular. But the rings we are considering here are not necessarily regular, which as we shall see will be related to the nonvanishing of H^2.

Theorem 2.1. *The following are in natural bijection. We think of each of them as the tangent space at the origin of* $R^{\square}_{\overline{\rho}}$.

1. $\mathrm{Hom}_{\mathbb{F}_p}\left(\left(\mathrm{m}_{R^{\square}_{\overline{\rho}}}/\mathrm{m}^2_{R^{\square}_{\overline{\rho}}}\right) \otimes \mathbb{F}_p, \mathbb{F}_p\right)$.

2. $\mathrm{Hom}_{\mathbb{Z}_p}(R^{\square}_{\overline{\rho}}, \mathbb{F}_p[\varepsilon]/\varepsilon^2)$.

3. $\mathcal{D}^{\square}(\mathbb{F}_p[\varepsilon]/\varepsilon^2)$.

4.$\mathrm{Z}^1(G, \mathrm{ad}\overline{\rho})$ *(action given by conjugation).*

Moreover, if $\overline{\rho}$ *is absolutely irreducible, there are induced bijections between*

$$\mathrm{Hom}_{\mathbb{F}_p}\left(\left(\mathrm{m}_{R^{\mathrm{univ}}_{\overline{\rho}}}/\mathrm{m}^2_{R^{\mathrm{univ}}_{\overline{\rho}}}\right) \otimes \mathbb{F}_p, \mathbb{F}_p\right)$$

and $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$.

Proof. The bijection between $\mathrm{Hom}_{\mathbb{Z}_p}(R^{\square}_{\overline{\rho}}, \mathbb{F}_p[\varepsilon]/\varepsilon^2)$ and $\mathcal{D}^{\square}(\mathbb{F}_p[\varepsilon]/\varepsilon^2)$ is clear because of the condition defining $R^{\square}_{\overline{\rho}}$, once we explain why any $\mathbb{Z}_p$-algebra homomorphism $\varphi : R^{\square}_{\overline{\rho}} \to \mathbb{F}_p[\varepsilon]/\varepsilon^2$ is local. For this, it suffices to show that if $\varphi(x)$ is a unit then x is a unit. Replacing x by x^p, we may assume $\varphi(x) \in \mathbb{F}_p^{\times}$. Then since it's a $\mathbb{Z}_p$-algebra homomorphism, we may find

$a \in \mathbb{Z}_p^\times$ reducing to $\varphi(x)$, and $\varphi(x-a) = \varphi(x) - \overline{a} = 0$. Thus $x \in a + \ker\varphi$. But as $R_{\overline{\rho}}^\square$ is local, we have $a + \ker\varphi \subset a + \mathrm{m}_{R_{\overline{\rho}}^\square}$, so x is a unit.

Next, we have $\mathrm{Hom}_{\mathbb{Z}_p}(R_{\overline{\rho}}^\square, \mathbb{F}_p[\varepsilon]/\varepsilon^2) = \mathrm{Hom}_{\mathbb{F}_p}(R_{\overline{\rho}}^\square \otimes \mathbb{F}_p, \mathbb{F}_p[\varepsilon]/\varepsilon^2)$, and $\mathrm{Hom}_{\mathbb{F}_p}(R_{\overline{\rho}}^\square \otimes \mathbb{F}_p, \mathbb{F}_p[\varepsilon]/\varepsilon^2) = \mathrm{Hom}_{\mathbb{F}_p}\left(\left(\mathrm{m}_{R_{\overline{\rho}}^\square}/\mathrm{m}_{R_{\overline{\rho}}^\square}^2\right) \otimes \mathbb{F}_p, \mathbb{F}_p\right)$ is standard, by checking what $\mathrm{m}_{R_{\overline{\rho}}^\square}$ maps to.

Finally, we must show $\mathcal{D}^\square(\mathbb{F}_p[\varepsilon]/\varepsilon^2)$ and $\mathrm{Z}^1(G, \mathrm{ad}\overline{\rho})$ are in bijection. Given a cocycle ξ of G with values in $\mathrm{ad}\overline{\rho}$, consider the lifting $\rho : G \to \mathrm{GL}_n\left(\mathbb{F}_p[\varepsilon]/\varepsilon^2\right)$ given by $\rho(g) = (1+\xi(g)\varepsilon)\overline{\rho}(g)$. To check this is a homomorphism, we compute:

$$\rho(g)\rho(h) = (1+\xi(g)\varepsilon)\overline{\rho}(g)(1+\xi(h)\varepsilon)\overline{\rho}(h) = (1+[\xi(g)+\overline{\rho}(g)\xi(h)\overline{\rho}(g^{-1})]\varepsilon)\overline{\rho}(gh) = (1+\xi(gh))\overline{\rho}(gh).$$

Conversely, suppose ρ is a lifting, and write $\rho(g) = \overline{\rho}(g) + \varepsilon\overline{\eta}(g)$. Then reversing the above computation shows that $\xi(g) = \overline{\eta}(g)\overline{\rho}(g)^{-1}$ is a cocycle. The assignments $\rho \mapsto \xi$ and $\xi \mapsto \rho$ are clearly inverses, and this establishes the bijection between 3 and 4.

Finally, the bijection between $\mathrm{Hom}_{\mathbb{F}_p}\left(\left(\mathrm{m}_{R_{\overline{\rho}}^{\mathrm{univ}}}/\mathrm{m}_{R_{\overline{\rho}}^{\mathrm{univ}}}^2\right) \otimes \mathbb{F}_p, \mathbb{F}_p\right)$ and $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$ is established by checking that coboundaries induce conjugations in the bijection between 3 and 4.

If ξ_1 is cohomologous to ξ_2, then there exists $\alpha \in \mathrm{ad}\overline{\rho}$ such that $\xi_1(g) - \xi_2(g) = \overline{\rho}(g)\alpha\overline{\rho}(g)^{-1} - \alpha$. Letting $\overline{\eta}_i(g) = \xi_i(g)\overline{\rho}_i(g)$, we have $\rho_1(g) - \rho_2(g) = \varepsilon\overline{\eta}_1(g) - \varepsilon\overline{\eta}_2(g) = \overline{\rho}(g)\alpha - \alpha\overline{\rho}(g)$. So

$$\rho_2(g) = \rho_1(g) - \overline{\rho}(g)\alpha + \alpha\overline{\rho}(g) = (1+\varepsilon\alpha)\rho_1(g)(1-\varepsilon\alpha),$$

so ρ_1 and ρ_2 are cohomologous. Conversely, if ρ_1 is conjugate to ρ_2, our assumption that $\overline{\rho}$ is absolutely irreducible implies by part 2 of the lemma that there exists some $1+\varepsilon\alpha \in \mathrm{GL}_n\left(\mathbb{F}_p[\varepsilon]/\varepsilon^2\right)$ with $\rho_2 = (1+\varepsilon\alpha)\rho_1(1-\varepsilon\alpha)$. Then one can check that $\xi_1(g) - \xi_2(g) = \overline{\rho}(g)\alpha\overline{\rho}(g)^{-1} - \alpha$, by reversing the above calculation. □

This allows us to give a simple expression for the dimension of the tangent space.

Corollary 2.1. *1.* $\dim_{\mathbb{F}_p}\mathrm{Hom}_{\mathbb{F}_p}\left(\left(\mathrm{m}_{R_{\overline{\rho}}^\square}/\mathrm{m}_{R_{\overline{\rho}}^\square}^2\right) \otimes \mathbb{F}_p, \mathbb{F}_p\right) = n^2 + \dim_{\mathbb{F}_p}\mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) - \dim_{\mathbb{F}_p}\mathrm{H}^0(G, \mathrm{ad}\overline{\rho})$.

2. If $\overline{\rho}$ is absolutely irreducible then $\dim_{\mathbb{F}_p}\mathrm{Hom}_{\mathbb{F}_p}\left(\left(\mathrm{m}_{R_{\overline{\rho}}^{\mathrm{univ}}}/\mathrm{m}_{R_{\overline{\rho}}^{\mathrm{univ}}}^2\right) \otimes \mathbb{F}_p, \mathbb{F}_p\right) = \dim_{\mathbb{F}_p}\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$.

Proof. Part 1 follows from the exact sequence

$$0 \to \mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) \to \mathrm{ad}\overline{\rho} \to \mathrm{Z}^1(G, \mathrm{ad}\overline{\rho}) \to \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) \to 0,$$

and part 2 follows from Theorem 1.2, together with $\mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) = \mathbb{F}_p$. □

Now let $d = \dim_{\mathbb{F}_p}\mathrm{Z}^1(G, \mathrm{ad}\overline{\rho})$, which is the dimension of the tangent space of $R_{\overline{\rho}}^\square \otimes \mathbb{F}_p$. We can therefore choose a surjection

$$\phi : \mathbb{Z}_p[[X_1, ..., X_d]] \to R_{\overline{\rho}}^\square,$$

and we have an induced map $\phi \otimes 1 : \mathbb{F}_p[[X_1, ..., X_d]] \to R_{\overline{\rho}}^\square/p$. The following theorem is due to Mazur.

Theorem 2.2. *Let $I = \ker\phi\otimes 1$. Then there is an injection* $(I/(X_1, ..., X_d)I)^\vee \hookrightarrow \mathrm{H}^2(G, \mathrm{ad}\overline{\rho})$.

We shall give the proof of this theorem in the next section. Note that a similar theorem (and its proof) holds true for $R_{\overline{\rho}}^{\mathrm{univ}}$ if $\overline{\rho}$ is absolutely irreducible.

Corollary 2.2. *The Krull dimension of $R_{\overline{\rho}}^{\square} \otimes \mathbb{F}_p$ is at least*

$$n^2 - \log \chi(\mathrm{ad}\overline{\rho}) = n^2 - \dim_{\mathbb{F}_p} \mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) + \dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) - \dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}).$$

If $\overline{\rho}$ is absolutely irreducible, the Krull dimension of $R_{\overline{\rho}}^{\mathrm{univ}} \otimes \mathbb{F}_p$ is at least

$$1 - \log \chi(\mathrm{ad}\overline{\rho}) = \dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) - \dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}).$$

In particular, if $\mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) = 0$, then $R_{\overline{\rho}}^{\square}$ is formally smooth over $\mathbb{Z}_p$, of dimension $Z^1(G, \mathrm{ad}\overline{\rho})$; and $R_{\overline{\rho}}^{\mathrm{univ}}$ is formally smooth over $\mathbb{Z}_p$, of dimension $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$.

Remark 2.1. Mazur conjectures that if $\overline{\rho}$ is absolutely irreducible then there is an equality. It seems that Boeckle provides counterexamples when $\overline{\rho}$ is only assumed to be Schur.

3. Mazur's theorem on H^2

The purpose of this subsection is to prove Theorem 2.2.

We start with a slightly more general discussion of liftings of homomorphisms to try and clear the assumptions and role of cohomology we are actually using.

Let P be a group which is not necessarily abelian, and let M be a normal abelian subgroup. We wish to discuss when a homomorphism $G \to P/M$ can be lifted to a homomorphism $G \to P$. If M is central, this question can be treated nicely using group cohomology. Namely, let G act trivially on M, P and P/M. Then according to the appendix in Serre's Local Fields, a long exact sequence of non abelian cohomology is induced:

$$0 \to M \to P \to P/M \to \mathrm{Hom}(G, M) \to \mathrm{Hom}(G, P) \to \mathrm{Hom}(G, P/M) \to \mathrm{H}^2(G, M).$$

In particular, a homomorphism $\varphi : G \to P/M$ lifts to $\mathrm{Hom}(G, P)$ if and only if it is mapped to zero under the map $\mathrm{Hom}(G, P/M) \to \mathrm{H}^2(G, M)$.

However, if M is not central this argument does not literally works. However, any homomorphism $\varphi \in \mathrm{Hom}(G, P/M)$ induces by functoriality a map $\mathrm{H}^2(P/M, M) \to \mathrm{H}^2(G, M)$; here the cohomology is taken with respect to the conjugation action of P/M on M (resp. the conjugation action of G on M induced by φ). In other words, we have a map

$$(,) : \mathrm{Hom}(G, P/M) \times \mathrm{H}^2(P/M, M) \to \mathrm{H}^2(G, M).$$

An extension $0 \to M \to P \to P/M \to 0$ gives rise to a cocycle $\xi_P \in \mathrm{H}^2(P/M, M)$, and this defines a cocycle $(\varphi, \xi) \in \mathrm{H}^2(G, M)$. Then one has the following theorem.

Theorem 3.1. *Given an extension given by $\xi \in \mathrm{H}^2(P/M, M)$ and $\varphi \in \mathrm{Hom}(G, P/M)$, the map φ lifts to a map in $\mathrm{Hom}(G, P)$ if and only if (φ, ξ) is trivial.*

Proof. The induced map on H^2 is given by the pullback diagram

$$\begin{array}{ccccccccc} 0 & \to & M & \to & P & \to & P/M & \to & 0 \\ & & =\uparrow & & \uparrow & & \varphi\uparrow & & \\ 0 & \to & M & \to & E & \to & G & \to & 0 \end{array},$$

and (φ, ξ) is trivial if and only if the map $E \to G$ admits a section, which happens if and only if φ lifts to a map in $\mathrm{Hom}(G, P)$. $\square$

Remark 3.1. 1. The point is that even though there is a cocycle in $\mathrm{H}^2(G, M)$ which determines whether or not φ lifts, in general it will not be given as the image of a coboundary map unless M is central.
2. One can also write this coboundary explicilty by taking any set theoretic lifting of P/M to M, getting a map $L : G \to P$. Then $\eta(g, h) := L(g)L(h)L(gh)^{-1}$ is valued in M, and it is the 2-cocycle which vanishes if and only if the map admits a lifting.
3. I am quite sure that when M is central both constructions are the same.

Now fix notations as in the statement of Theorem 2.2. Thus, $R^{\square}_{\overline{\rho}}$ is the universal lifting ring of $\overline{\rho}$, and $\mathbb{F}_p[[X_1, ..., X_d]] \to R^{\square}_{\overline{\rho}}/p$ induces an isomorphism on tangent spaces, and has kernel I. We wish to show that $(I/mI)^{\vee} \hookrightarrow \mathrm{H}^2(G, \mathrm{ad}\overline{\rho})$.
Proof of Theorem 2.2. Consider the exact sequence (of $\phi \otimes 1$),

$$0 \to I \to \mathbb{F}_p[[X_1, ..., X_d]] \to R^{\square}_{\overline{\rho}}/p \to 0.$$

There is an induced sequence,

$$0 \to I/(X_1, ..., X_d)I \to \mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I \to R^{\square}_{\overline{\rho}}/p \to 0.$$

The map $\mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I \to R^{\square}_{\overline{\rho}}/p$ still induces an isomorphism on tangent spaces (as $(X_1, ..., X_d)I \subset (X_1, ..., X_d)^2$, because $(X_1, ..., X_d)$ is the maximal ideal of $\mathbb{F}_p[[X_1, ..., X_d]]$). The point of our construction is that we are replacing $\mathbb{F}_p[[X_1, ..., X_d]]$ by the smallest algebra which still has this property in some sense.
According to the universal property of $R^{\square}_{\overline{\rho}}$, the ring $R^{\square}_{\overline{\rho}}/p$ is the mod p universal lifting ring of $\overline{\rho}$. Let $\rho^{\square}_p : G \to \mathrm{GL}_n(R^{\square}_{\overline{\rho}}/p)$ be the corresponding representation. Consider the question of lifting $\rho^{\square}_p$ to $\mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I$; we have the following exact sequence

$$1 \to 1 + M_n(I/(X_1, ..., X_d)I) \to \mathrm{GL}_n(\mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I) \to \mathrm{GL}_n\left(R^{\square}_{\overline{\rho}}/p\right) \to 1.$$

By Theorem 3.1, the obstruction to lifting $\rho^{\square}_p$ is given by an element in $\mathrm{H}^2(G, 1+M_n(I/(X_1, ..., X_d)I))$. On the other hand, we have

$$1 + M_n(I/(X_1, ..., X_d)I) \cong M_n(I/(X_1, ..., X_d)I) \cong \mathrm{ad}\overline{\rho} \otimes I/(X_1, ..., X_d)I,$$

as G representations. The reason is that $(I/(X_1, ..., X_d)I)^2 = 0$, so multiplying in $1 + M_n(J/(X_1, ..., X_d)I)$ is the same as adding in $M_n(I/(X_1, ..., X_d)I)$.
Hence, the obstrucion is an element ξ of $\mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) \otimes I/(X_1, ..., X_d)I$.
We now obtain a map

$$(I/(X_1, ..., X_d)I)^{\vee} \to \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}),$$

by evaluating ξ at the functional.
Finally, we show that this map is injective. Suppose f is a nonzero element of its kernel. We have that $I(X_1, ..., X_d) \subset \ker f \subset I$, and it follows that $\ker f$ is an ideal of $\mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I$. Let A be the quotient of $\mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I$ by $\ker f$, and let J be the image of $I/(X_1, ..., X_d)I$ in the quotient. We have

$$J = I/\left((X_1, ..., X_d)I, \ker(f)\right) \cong \mathbb{F}_p.$$

Thus, we have an exact sequence

$$0 \to \mathbb{F}_p \to A \to R^{\square}_{\overline{\rho}}/p \to 0,$$

and $A \to R^{\square}_{\overline{\rho}}/p$ still induces an isomorphism on tangent spaces. The point is that since $\ker f \subset I$, and I is the kernel of $\mathbb{F}_p[[X_1, ..., X_d]] \to R^{\square}_{\overline{\rho}}/p$, there is no harm in modding out by it already in the middle stage, thus bringing A as close as possible to $R^{\square}_{\overline{\rho}}/p$.

However now the obstruction to lifting $\rho_p^{\square}$ to A vanishes, precisely because it is given by an element of $\mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) \otimes J$, and the "$J$-coefficient" is 0 by the assumption that f is mapped to 0.

By the universal property, we must have an induced homomorphism $R^{\square}_{\overline{\rho}}/p \to A$, such that the composition $R^{\square}_{\overline{\rho}}/p \to A \to R^{\square}_{\overline{\rho}}/p$ is the identity. Thus the sequence

$$0 \to \mathbb{F}_p \to A \to R^{\square}_{\overline{\rho}}/p \to 0$$

splits, which is a contradiction to the assumption that $A \to R^{\square}_{\overline{\rho}}/p$ induces an isomorphism on tangent spaces. □

Remark 3.2. Geometrically, I think we can understand this proof as follows. The scheme $\mathrm{Spec} R^{\square}_{\overline{\rho}}/p$ is sitting inside $\mathrm{Spec}\mathbb{F}_p[[X_1, ..., X_d]]$ and it is an isomorphism on tangent spaces in the unique closed point. Thus the situation is something like $\mathrm{Spec}\mathbb{F}_p[[X_1, ..., X_d]]$ is the completed local ring of 0 in A^d, and $\mathrm{Spec} R^{\square}_{\overline{\rho}}/p$ is something potentially smaller which sees the whole tangent space; for instance it could be the union of two lines passing through the origin in the completed local ring of A^2 at the origin. Now $\mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I$ is the thickening of $R^{\square}_{\overline{\rho}}/p = \mathbb{F}_p[[X_1, ..., X_d]]/I$ in all directions simultaneously; and the lifting problem is to extend the "familiy" $\rho_p^{\square}$ in all directions simultaneously. Now $I/(X_1, ..., X_d)I = \ker \mathbb{F}_p[[X_1, ..., X_d]]/(X_1, ..., X_d)I \to R^{\square}_{\overline{\rho}}/p$ is the closed subscheme corresponding to $\mathrm{Spec} R^{\square}_{\overline{\rho}}/p$ in the thickening $\mathbb{F}_p[[X_1, ..., X_d]]/I$; the space $(I/(X_1, ..., X_d)I)^{\vee}$ is the space of direction in which we can try to extend the family. Each such direction gives rise to such an obstruction via the map $(I/(X_1, ..., X_d)I)^{\vee} \to \mathrm{H}^2(G, \mathrm{ad}\overline{\rho})$; and the calculation shows that any nontrivial direction gives rise to a nontrivial obstruction, because otherwise $\mathrm{Spec} R^{\square}_{\overline{\rho}}/p$ which is universal by definition could be thickened a bit more.

4. Functorial properties

See section 1.3 of Mazur's 89 paper for more details.

4.1. **Conjugation.** Suppose that $\overline{\rho}$ is absolutely irreducible, and fix a matrix $a \in \mathrm{GL}_n(\mathbb{F}_p)$. Conjugation by a gives an automorphism of $\mathrm{GL}_n(\mathbb{F}_p)$, and composing in this way gives a representation $a\overline{\rho}a^{-1}$. Lift a arbitrarily to an element of A for a complete noetherian algebra A; by Lemma 1.1, the effect of conjugating by this element does not depend on the choice of lifting. So conjugating by a defines an isomorphism of functors between $\mathcal{D}^{\square}_{\overline{\rho}}$ and $\mathcal{D}^{\square}_{a\overline{\rho}a^{-1}}$. Consequentley by the Yonda Lemma, $R^{\square}_{\overline{\rho}} \cong R^{\square}_{a\overline{\rho}a^{-1}}$. One can argue similarly for $\overline{\rho}^{\mathrm{univ}}$.

4.2. **Duality.** The natural contragredient morphism on GL_n extends to lifting and defines a natural isomorphism between $\mathcal{D}^{\square}_{\overline{\rho}}$ and $\mathcal{D}^{\square}_{\overline{\rho}^{\vee}}$, and thus $R^{\square}_{\overline{\rho}} \cong R^{\square}_{\overline{\rho}^{\vee}}$.

4.3. **Determinant.** The determinant gives rise to a natural morphism $R^{\square}_{\det\overline{\rho}} \to R^{\square}_{\overline{\rho}}$.

4.4. **Tensor product.** Given two reps $\overline{\rho}_1 : G \to \mathrm{GL}_n(\mathbb{F}_p), \overline{\rho}_2 : G \to \mathrm{GL}_m(\mathbb{F}_p)$, we can form the tensor product $\overline{\rho}_1 \otimes \overline{\rho}_2 : G \to \mathrm{GL}_{nm}(\mathbb{F}_p)$. On the other hand to any two deformations A_1, A_2 of them we can form the tensor product $A_1 \widehat{\otimes}_{\mathbb{Z}_p} A_2$. This gives rise to a morphism $R^{\square}_{\overline{\rho}_1 \otimes \overline{\rho}_2} \to R^{\square}_{\overline{\rho}_1} \widehat{\otimes}_{\mathbb{Z}_p} R^{\square}_{\overline{\rho}_2}$.
For example, this allows us to twist by a character, which induces an isomorphism by functoriality.

4.5. **Change of group.** Given a homomorphism $\varphi : G_1 \to G_2$ such that $\overline{\rho}_2 \circ \varphi = \overline{\rho}_1$, there is an induced homomorphism $R^{\square}_{\overline{\rho}_1} \to R^{\square}_{\overline{\rho}_2}$ of local noetherian complete $\mathbb{Z}_p$-algebras.

5. Rigid Analytic Fibers

For simplicity let's focus on the cases $n = 1$ or $n = 2$, though it probably does not matter too much. We let $\overline{\rho}$ be a representation of G. Under the assumption that $R^{\square}_{\overline{\rho}}$ or $R^{\mathrm{univ}}_{\overline{\rho}}$ exists, we can construct an associated rigid analytic space. For instance, let's work with $R^{\mathrm{univ}}_{\overline{\rho}}$. Then it is isomorphic to a ring of the form $\mathbb{Z}_p[[X_1, ..., X_n]]/(f_1, ..., f_m)$. The construction of Berthelot (as described in de Jong 1995 and Berthelot 1991) attaches to the generic fiber $R^{\mathrm{univ}}_{\overline{\rho}}[1/p] = R^{\mathrm{univ}}_{\overline{\rho}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ a rigid analytic space $X_{\overline{\rho}}$. One should think of it as (the vanishing locus of $f_1, ..., f_m$ in) the open unit n-polydisc. Formally, the construction proceeds by constructing the appropiate closed polydiscs and letting the radius go to 1. In particular, the construction is slightly indirect. Note also this construction really receives a formal scheme, so the data of the topology on this ring is also required.

Warning 1. This construction does not make $R^{\mathrm{univ}}_{\overline{\rho}}[1/p]$ into the ring of global functions of $X_{\overline{\rho}}$. For instance, on the open unit disc there should be functions such as $\log(1 + X)$ which converge everywhere but are not bounded. Rather, it seems that according to Theorem 7.4.1 of de Jong's paper, these are the *bounded global functions,* and $R^{\mathrm{univ}}_{\overline{\rho}}$ is the subring of *power-bounded global functions,* at least if $R^{\mathrm{univ}}_{\overline{\rho}}$ is flat over $\mathbb{Z}_p$. My guess is that the only issue for this flatness is p-torsion, which does not change the generic fiber according to Lemma 7.1.4, so that it should always be true that $R^{\mathrm{univ}}_{\overline{\rho}}[1/p]$ is the ring of bounded functions.

Warning 2. It is not true that for A for which this construction is defined, $\mathrm{Spf}(A) \mapsto \mathrm{Spf}(A)^{\mathrm{rig}}$ is something like an equivalence of categories. First, because there could be something like p-torsion as we mentioned before. But also because there seems to be no way in general to actually recover A, only something like $A[1/p]$.

Something that is true is proposition 7.1.7 of de Jong's paper. For *affinoids* Y, there is an isomorphism

$$\lim_{\mathfrak{Y} \text{model of } Y} \mathrm{Hom}_{\text{Formal schemes}/\mathbb{Z}_p}(\mathfrak{Y}, \mathfrak{X}) \to \mathrm{Hom}_{\text{Rigid Spaces}/\mathbb{Q}_p}\left(Y, \mathfrak{X}^{\mathrm{rig}}\right).$$

In the special case where $E/\mathbb{Q}_p$ is a field extension, there is acutally an isomorphism $\mathfrak{X}(E^{\circ}) = \mathfrak{X}^{\mathrm{rig}}(\mathrm{Sp}(E))$. See for example lecture 2 of the Berkeley Lectures of Scholze. So in this case *we can* think of the homomorphism between rings as being equivalent to the data of a morphism between the rigid spaces, although this is not equivalent in general.

Thus on $R^{\mathrm{univ}}_{\overline{\rho}}$, every point $x \in X_{\overline{\rho}}$ gives rise to a morphism $\mathrm{Sp}(E) \to X_{\overline{\rho}}$ for $E = k(x)$ (which is automatically a finite extension of $\mathbb{Q}_p$), and this is equivalent to a morphism $R^{\mathrm{univ}}_{\overline{\rho}} \to \mathcal{O}_E$.

(I am suddenly a bit skeptical about this if $R_{\overline{\rho}}^{\mathrm{univ}}$ is not flat becuase it could have perhaps p-torsion, and then such elements will automatically be sent to 0. Is that a problem? Maybe not, because probably in the flat model such elements are automatically zero anyway). Thus we see that "points of $X_{\overline{\rho}}$ parametrise lifts of $\overline{\rho}$ to $\overline{\mathbb{Z}}_p$".

Some caveats are that

1. if we are taking E whose residue field is an extension of $\mathbb{F}_p$ then probably this is really a lifting of the extension of $\overline{\rho}$ to that residue field (so it is not per se a lifting of $\overline{\rho}$), and

2. Because of the preceding discussions it is not as simple to discuss actual families of representations in this way because in general $\mathrm{Sp}(R)$-valued points for $R = A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ an algebra will likely not be given simply by a homomorphism from $R_{\overline{\rho}}^{\mathrm{univ}}$ to A as it is in the case of a point. de Jong's proposition 7.1.7 above does shows that if R is affinoid then there exists a homomorphism from some model which induces this, but it seems to be a priori unclear which model it is, and it has no reason to be our specific choice of A.

3. Because of the previous point it really does not enable us to work integrally, i.e. as there is no canonical choice of such A they do not glue a priori, so we also cannot reduce in families, only in points. So this is why Kisin says he does "rational p adic Hodge Theory" instead of "integral p adic Hodge theory". According to a mathoverflow question of David Loeffler, the existence of Kisin's O_X-sheaf on the rigid analyic space X really should not be possible to do before passing to the generic fiber as in Berthelot's construction.

6. Dimension Formulas

6.1. **The case where $G = G_{\mathbb{Q}_p}$.** Recall we have the local Euler characteristic, for a mod l representation $\overline{V}$ of $G_{\mathbb{Q}_p}$:

$$\dim_{\mathbb{F}_l} \mathrm{H}^0\left(\overline{V}\right) - \dim_{\mathbb{F}_l} \mathrm{H}^1\left(\overline{V}\right) + \dim_{\mathbb{F}_l} \mathrm{H}^2\left(\overline{V}\right) = \log_l \chi(\overline{V}).$$

If p does not divide n, the local Euler characteristic formula gives

$$\log_l \chi(\overline{V}) = \begin{cases} 0 & p \neq l \\ -\dim_{\mathbb{F}_l} \overline{V} & p = l \end{cases}.$$

Thus the formulas of section 2 give

Corollary 6.1. *Let $\overline{\rho} : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{F}_l)$ be a representation, and suppose p does not divide n. Then we have the following table:*

$$\begin{array}{ccc} & \mathrm{Kdim}\left(R_{\overline{\rho}}^{\square} \otimes \mathbb{F}_P\right) & \mathrm{Kdim}\left(R_{\overline{\rho}}^{\mathrm{univ}} \otimes \mathbb{F}_p\right) \\ p \neq l & \geq n^2 & \geq 1 \\ p = l & \geq 2n^2 & \geq n^2+1 \end{array},$$

where the right column assumes $\overline{\rho}$ is absolutely irreducible.

6.2. **The case where $G = G_{\mathbb{Q},S}$.** Recall we have the global Euler characteristic formula, for a mod l representation $\overline{V}$ of $G_{F,S}$:

$$\log_l \chi(\overline{V}) = \sum_{v \in S_\infty} \dim_{\mathbb{F}_l} \mathrm{H}^0(G_{F_v}, \overline{V}) - [F:\mathbb{Q}] \dim_{\mathbb{F}_l} \overline{V}.$$

In particular for $F = \mathbb{Q}$, $\overline{V} = \mathrm{ad}\overline{\rho}$, and $\overline{\rho}$ absolutely irreducible, where $\overline{\rho}$ has dimension 2,

$$\log_l \chi(\mathrm{ad}\overline{\rho}) = \dim_{\mathbb{F}_l} \mathrm{H}^0(G_{\mathbb{R}}, \mathrm{ad}\overline{\rho}) - 4 = \begin{cases} -2 & \overline{\rho} \text{ odd} \\ 0 & \overline{\rho} \text{ even} \end{cases}.$$

Thus the formulas of section 2 give

Corollary 6.2. *Let $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_l)$ be a representation, and suppose p does not divide n. Then we have the following table:*

$\overline{\rho}$	$\mathrm{Kdim}\left(R^{\square}_{\overline{\rho}} \otimes \mathbb{F}_P\right)$	$\mathrm{Kdim}\left(R^{\mathrm{univ}}_{\overline{\rho}} \otimes \mathbb{F}_p\right)$
odd	≥ 6	≥ 3
even	≥ 4	≥ 1

,

where the right column assumes $\overline{\rho}$ is absolutely irreducible.

7. Examples

7.1. **Deformations in dimension 1.** Twisting allows us to assume $\overline{\rho}$ is trivial. In this case we have $R^{\square}_{\overline{\rho}} = \mathbb{Z}_p[[G^{\mathrm{ab},p}]]$, with the homomorphism $\rho^{\square} : G \to \mathbb{Z}_p[[G^{\mathrm{ab},p}]]^{\times}$ given by mapping g to $\overline{g}$, and reducing $\overline{g} - 1$ to 0.

To see this, note that for a complete noetherian local $\mathbb{Z}_p$-algebra A with residue field $\mathbb{F}_p$, we have

$$\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[[G^{\mathrm{ab},p}]], A\right) \cong \mathrm{Hom}_{\mathrm{Grp}}(G^{\mathrm{ab},p}, A^{\times}) = \mathrm{Hom}_{\mathrm{Grp}}(G^{\mathrm{ab},p}, 1 + \mathrm{m}_A) =$$
$$\mathrm{Hom}_{\mathrm{Grp}}(G, 1 + \mathrm{m}_A) = \mathcal{D}^{\square}(A).$$

Note that this agrees with the calculations done in the previous section. If $l \neq p$, then $G^{\mathrm{ab},p}_{\mathbb{Q}_l} \cong \mathbb{Z}_p \times$ cyclic, so see that indeed $\mathbb{F}_p[[G^{\mathrm{ab},p}]]$ has Krull dimension 1. If $l = 0$ then $G^{\mathrm{ab},p}_{\mathbb{Q}_l} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{F}_p[[G^{\mathrm{ab},p}]]$ really has dimension 2.

7.2. G **prime to** p**.** In this case we have (regardless of $\overline{\rho}$) an equality $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) = \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) = 0$. Therefore according to Theorem 2.2, the map $\mathbb{Z}_p \to R^{\square}_{\overline{\rho}}$ is an isomorphism.

(Actually, it seems like one has to explain why there is a lifting to $\mathbb{Z}_p$ at all. Other proofs I have seen do not seem to address this issue. Here is a sketch of such an argument, which is possibly not wrong. Any representation $G \to \mathrm{GL}_n(\mathbb{F}_p)$ factors through a finite quotient, which is in this case prime to l. We can work with this quotient instead of l, and replace it by a constant group scheme of order prime to l. Then the morphism from $\mathrm{Spec}\mathrm{GL}_n(\mathbb{F}_p)$ to $\mathrm{Spec}G$ is formally etale, because G is prime to p and $\mathrm{Spec}\mathrm{GL}_n(\mathbb{F}_p)$ is defined over $\mathbb{F}_p$ (any group scheme over $\mathbb{F}_p$ of order prime to p is etale over $\mathbb{F}_p$, I think). So a morphism from G lifts across nilpotnent thickenings).

7.3. **Deformations of finite cyclic groups.** In this case, the theory of the Herbrand quotient implies that $\dim \mathrm{H}^1(\mathrm{ad}\overline{\rho}) = \dim \mathrm{H}^2(\mathrm{ad}\overline{\rho})$; in particular, the Krull bound on the dimension of $R^{\square}_{\overline{\rho}} \otimes \mathbb{F}_p$ is $n^2 - \dim_{\mathbb{F}_p} \mathrm{H}^0(G, \mathrm{ad}\overline{\rho})$. (There is also a nice bound on $R^{\mathrm{univ}}_{\overline{\rho}} \otimes \mathbb{F}_p$, but it is basically never the case the representation is absolutely irreducible unless $n = 1$).

7.3.1. *Case where G is cyclic and $\overline{\rho} = \overline{\rho}_{\mathrm{triv}}$.* In this case we can calculate the cohomology of $\mathrm{ad}\overline{\rho}$ using Tate cohomology. We have the generator σ acting trivially, and the norm acts by multiplying with $\#G$. We have

$$\begin{cases} \mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) = \mathrm{ad}\overline{\rho} \\ \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) = \mathrm{ad}\overline{\rho}[\#G] \\ \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) = \frac{\mathrm{ad}\overline{\rho}}{\#G} \end{cases} .$$

In the interesting case, where $\#G$ is divisible by p, we can rewrite this as

$$\begin{cases} \mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) = \mathrm{ad}\overline{\rho} \\ \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) = \mathrm{ad}\overline{\rho} \\ \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) = \mathrm{ad}\overline{\rho} \end{cases} .$$

So $R^{\square}_{\overline{\rho}} \otimes \mathbb{F}_p$ has Krull dimension 0, but there as many as $\dim_{\mathbb{F}_p} \mathrm{ad}\overline{\rho}$ generators and relations. For instance, let's inspect with some more detail the case of the trivial representation for $G = \mathbb{Z}/p$, $n = 2$. According to (the proof of) proposition 1.3.1 in Boeckle's notes, the ring $R^{\square}_{\overline{\rho}}$ is the ring $\mathbb{Z}_p[X_{11}, X_{12}, X_{21}, X_{22}]/(X_{ij}^p - 1)$, completed at the ideal generated by $(p, X_{11} - 1, X_{12}, X_{21}, X_{22} - 1)$. I think this shows that the ring is

$$R^{\square}_{\overline{\rho}} = \mathbb{Z}_p[[X_{11}-1, X_{12}, X_{21}, X_{22}-1]]/(X_{ij}^p-1) = \mathbb{Z}_p[[X, Y, Z, W]]/\left(\left(I + \begin{pmatrix} X & Y \\ Z & W \end{pmatrix}\right)^p - I\right),$$

which is quite visibly of dimension 0 (when reducing mod p), but with tangent space of dimension $n^2 = n^2 + \dim \mathrm{H}^1 - \dim \mathrm{H}^0$, in agreement with section 2.

7.3.2. *Case where G is cyclic, $\overline{\rho} \neq \overline{\rho}_{\mathrm{triv}}$, $n = 2$.* Again in the interesting case $G = \mathbb{Z}/p^d$ is divisible by p. It is probably easy to reduce to the case where G is of order a power of p, so I will assume this here, and prove the required descent result elsewhere. Since we are assuming that $\overline{\rho} \neq \overline{\rho}_{\mathrm{triv}}$, we have $\overline{\rho}(\sigma) \neq I$. On the other hand $\overline{\rho}(\sigma)^{p^d} = I$. Therefore all the eigenvalues of $\overline{\rho}(\sigma)$ are 1, which means it is conjugate to a matrix of the form

$$I + N = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

proving in fact that there is a factorisation through a group of order p (and, moreover, $N^2 = 0$). Now acting with σ on $\mathrm{ad}\overline{\rho}$ has the same effect as conjugating by $I + N$. We easliy compute that

$$(I + N)\begin{pmatrix} a & b \\ c & d \end{pmatrix}(I - N) = \begin{pmatrix} a + c & -a - c + b + d \\ c & d - c \end{pmatrix},$$

so

$$(\sigma - 1)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & -a - c + d \\ 0 & -c \end{pmatrix}$$

$$\ker(\sigma-1)=\mathrm{ad}\overline{\rho}^G=\left\{\begin{pmatrix} a & * \\ 0 & a \end{pmatrix}\right\}$$

and

$$\mathrm{Im}(\sigma-1)=\left\{\begin{pmatrix} a & * \\ 0 & -a \end{pmatrix}\right\}.$$

On the other hand, noticing again that $\overline{\rho}(\sigma)^p=I$, the norm $(1+\sigma+...+\sigma^{p^d-1})=(1+\sigma+...+\sigma^{p-1})(1+\sigma^p+...+\sigma^{p^{d-1}})$ has the same action as $d(1+\sigma+...+\sigma^{p-1})$.

The action of $1+\sigma+...+\sigma^{p-1}$ on $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{ad}\overline{\rho}$ is given by

$$A+(I+N)A(I-N)+(I+N)^2A(I-N)^2+...+(I+N)^{p-1}A(I-N)^{p-1}.$$

As $N^2=0$, this simplifies to

$$\begin{aligned}&A+(I+N)A(I-N)+(I+2N)A(I-2N)+...+(I+(p-1)N)A(I-(p-1)N)\\&=pA+\binom{p}{2}NA-\binom{p}{2}AN-\frac{(p-1)p(2p-1)}{6}NAN.\\&=-\frac{(p-1)p(2p-1)}{6}NAN.\end{aligned}$$

If $p\geq 5$, this is 0. Otherwise, this is $NAN=\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$.

Summarising this, if either $p\geq 5$ or d is divisible by 3, we have

$$\begin{cases}\mathrm{H}^0(G,\mathrm{ad}\overline{\rho})=\ker(\sigma-1)=\left\{\begin{pmatrix} a & * \\ 0 & a \end{pmatrix}\right\}\\ \mathrm{H}^1(G,\mathrm{ad}\overline{\rho})=\ker(\mathrm{Norm})/\mathrm{Im}(\sigma-1)=\mathrm{ad}\overline{\rho}/\left\{\begin{pmatrix} a & * \\ 0 & -a \end{pmatrix}\right\}\\ \mathrm{H}^2(G,\mathrm{ad}\overline{\rho})=\ker(\sigma-1)/\mathrm{Im}(\mathrm{Norm})=\left\{\begin{pmatrix} a & * \\ 0 & a \end{pmatrix}\right\}\end{cases}.$$

Thus in this case the universal lifting ring has $4-2+2=4$ generators and 2 relations.

On the other hand, in the exceptional case $p=3$, d is not divisible by 3, we have that $\mathrm{Norm}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$, and

$$\begin{cases}\mathrm{H}^0(G,\mathrm{ad}\overline{\rho})=\ker(\sigma-1)=\left\{\begin{pmatrix} a & * \\ 0 & a \end{pmatrix}\right\}\\ \mathrm{H}^1(G,\mathrm{ad}\overline{\rho})=\ker(\mathrm{Norm})/\mathrm{Im}(\sigma-1)=\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}/\left\{\begin{pmatrix} a & * \\ 0 & -a \end{pmatrix}\right\}\\ \mathrm{H}^2(G,\mathrm{ad}\overline{\rho})=\ker(\sigma-1)/\mathrm{Im}(\mathrm{Norm})=\left\{\begin{pmatrix} a & * \\ 0 & a \end{pmatrix}\right\}/\left\{\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}\right\}\end{cases}.$$

For example, we now know that for the nontrivial representation $\mathbb{Z}/9\mathbb{Z} \to \mathrm{GL}_2(\mathbb{F}_3)$, the universal lifting ring actually has $4-2+1=3$ generators and 1 relation.

7.4. **Other explicit examples.**

7.4.1. *Mazur's example 1.* The following is an example of Mazur. Let $g(X) = X^3 + aX + 1$ such that $27 + 4a^3 = p$ is a prime. Then $\mathrm{disc}(f(X)) = -p$, and the splitting field K of $g(X)$ is thus an S_3 extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{-p})$. Let $\overline{\rho} : \mathrm{Gal}(\mathbb{Q}_{\{p,\infty\}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_l)$ be the representation factoring through $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, mapping σ to $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ and τ to $\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$. This representation is irreducible, and Mazur is able to compute (although I am unable to understand his calculation, in section 1.13 of his first paper) that $\mathrm{H}^2(\mathrm{Gal}(\mathbb{Q}_{\{p,\infty\}}/\mathbb{Q}), \mathrm{ad}\overline{\rho}) = 0$. Therefore the universal deformation ring is $R_{\overline{\rho}}^{\mathrm{univ}} \cong \mathbb{Z}_l[[X_1, X_2, X_3]$.

On the other hand, it seems like all these representations are known to modular. As these reprsentation factor through a finite group, their Hodge-Tate weights are both 0 (if lifted to $\mathrm{GL}_2(\mathbb{Z}_p)$, and we expect them to rise from a modular form of weight 1. For instance, if $p = 23$, so that $g(X) = X^3 - X + 1$, the representation $\rho_f : \mathrm{Gal}(\mathbb{Q}_{\{p,\infty\}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l)$ defined by the same formulas as above arises from the eigenform $f(q) = q\prod(1-q^n)(1-q^{23n})$, which is of level 23 and weight 1. Probably there should be some $R = T$ theorem, and more modular points above, so that there would be some congruent eigenforms which also give the same residual representation.

Let's specializse further in this example to the case where $l = 2$. Then something interesting happens. We can also consider the elliptic curve

$$E : y^2 = X^3 - X + 1,$$

and the associated representation $\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_2)$ for the action on 2-power torsion. Then the roots of order 2 in E are just given by $(0, x_i)$ where the x_i are the roots, and the action on $\mathrm{GL}_2(\mathbb{F}_2)$ is just given by factoring through S_3 as above. In other words, the represntations ρ_E and ρ_f are congruent mod 2. On the other hand we know by Taylor Wiles that ρ_E also arises from a weight 2 modular form. In this case one sees the conductor of E is $92 = 2^2 \cdot 11$, and indeed such a mod form $h(q) \in S_2(\Gamma_0(92))$ is given in the LMFDB by

$$h(q) = q - 3q^3 - 2q^5 - 4q^7 + 6q^9 + 2q^{11} - 5q^{13} + 6q^{15} + ...$$

On the other hand

$$f(q) = q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} + ...$$

and we indeed see that the a_n are congruent mod 2 away from 2 and 11. This is especially nice because the mod forms have different weights. Thus these are two points in the universal deformation space $R_{\overline{\rho}}$, which might be isomorphic to $\mathbb{Z}_2[[X_1, X_2, X_3]]$ (alas this is the case of $p = 2$ so it might be more tricky).

7.4.2. *Mazur's example 2.* The following example is from the yellow book. Consider the representation

$$\overline{\rho} : G_{\mathbb{Q},\{3,7,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_3),$$

obtained from the 3-torsion points of the elliptic curve $X_0(49)$. Then the universal deformation ring is isomorphic to

$$\mathbb{Z}_3[[t_1,t_2,t_3,t_4]] / \left((1+t_4)^3 - 1\right).$$

Here of course this is not smooth, which is the same as saying that $\mathrm{H}^2 \neq 0$ for $\mathrm{ad}\overline{\rho}$. A few interesting things to notice are:

1. The universal deformation ring, although not smooth, is smooth at the generic fiber (after inverting 3).

2. After reducing mod 3, one stays with $\mathbb{F}_3[[t_1,t_2,t_3,t_4]] / (t_4)^3$, which clearly has tangent space of dimension 4 and has Krull dimension 3. On the other hand, before reducing mod 3 one has something which geometrically has 3 components (indeed, specializing $1+t_4$ are cube roots of unity gives the 3 components). Thus after adding a cube root of unity one is left with 3 components and the dimension of the tangent space rises significantly; however when we reduce mod 3 these 3 components become 1 component.