Galois Deformation Notes

Niven Achenjang

Fall 2023

These are notes on Galois deformation rings and the statement of "$R = T$" theorems, written for the MF learning seminar. They reflect my understanding (or lack thereof) of the material, so are far from perfect. They are likely to contain some typos and/or mistakes, but ideally none serious enough to distract from the mathematics. With that said, enjoy and happy mathing.

As with my last talk for this seminar, much of what is written in these notes can be ignored (this is even more true this time than last time). The most important bits are definitions and statements of theorems and whatnot.

These notes were written somewhat hurriedly/haphazardly (and are still unfinished). Let me know what mistakes you find.

Contents

Introduction

This talk marks the beginning of a shift in the topics of this seminar. From now until the end of the semester, we will focus our efforts on gaining some understanding of Galois deformations. Before diving into this material, let's give a quick recap of where we are.

Recall 1. Suppose (a,b,c) is a non-trivial solution to $a^p + b^p = c^p$.[1] Attached to this is the remarkable Frey curve $E : y^2 = x(x-a^p)(x+b^p)$.

- In the first lecture we discussed this curve. In particular, we showed that its mod p representation $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ is absolutely irreducible, odd, unramified outside $2p$, and flat at p. In particular, it has surprisingly little ramification; so little ramification, in fact, that modularity predicts that E cannot exist.

- In the third and fourth lectures, we discussed the Langlands-Tunnell [CSS97, Chapter VI, Theorem 1.3] result on modularity of odd, solvable Artin representations. We have also seen (e.g. in notes for the first lecture) that this implies the modularity of $\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ (when this representation is irreducible).

- In the fifth lecture, we discussed Serre's conjecture. Because $\overline{\rho}_{E,p}$ has so little ramification, the full strength of this conjecture would predict that it is the representation attached to a modular form of weight 2 and level $\Gamma_0(2)$, but no such form exists, a contradiction. Serre's full conjecture was not known at the time FLT was proven, but his simpler 'epsilon conjecture' (on level lowering for modular representations) was known. This is enough to show that *if* $\overline{\rho}_{E,p}$ *is modular* (of weight 2 and some level), then it must be so of weight 2 and level 2. Thus, weight 2 modularity of $\overline{\rho}_{E,p}$ would prove FLT.

- This brings us to now. We know $\overline{\rho}_{E,3}$ is modular (when its irreducible). If we knew that E itself was modular, e.g. that $\rho_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_3)$ was modular, then we could conclude that $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ (and so also $\overline{\rho}_{E,p}$) is modular too, and so arrive at a contradiction via Serre's epsilon conjecture. $\odot$

To finish this story, Wiles and Taylor-Wiles proved

Theorem 2. *Let E be as above. For any prime ℓ, if $\overline{\rho}_{E,\ell}$ is modular (and irreducible), then $\rho_{E,\ell}$ is modular as well.*

The rough strategy for proving this theorem is to study all the ways of deforming/lifting $\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ to Galois representations over larger (complete and/or artinian) rings A (e.g. $A = \mathbb{Z}_\ell$), and then to show that all such deformations satisfying appropriate local conditions (modelled e.g. on properties of $\rho_{E,\ell}$, our main representation of interest) must in fact be modular.

In this talk, we want to set the stage for carrying out such an argument. We will introduce the basic objects and definitions that come into play and hopefully get a sense for what work needs to

[1] For technical reasons, one should assume that $p \geq 5$, that $a \equiv -1 \mod 4$, and that $2 \mid b$. See the first lecture in this seminar for why.

be done in order to prove such a modularity lifting result. These notes are mostly based on [Gee22] (supplemented by [Zho]) and [BÏ3]. The paper [CHT08] (especially section 2) has also been helpful.

By the end (of this semester), we will *not* prove Theorem 2.[2] Instead, we will largely follow [Gee22] and so prove something like the following:

Theorem 3 ([Gee22, Theorem 5.2])**.** *Fix a prime $p > 3$. Let F be a totally real number field, and choose some $L/\mathbb{Q}_p$ large enough that L contains the images of all embeddings $F \hookrightarrow \overline{\mathbb{Q}}_p$. Let $\mathcal{O} = \mathcal{O}_L$. Suppose that $\rho : G_F \to \mathrm{GL}_2(\mathcal{O})$ is a continuous, `geometric`[3] representation such that $\overline{\rho}$ is modular, say $\overline{\rho} \cong \overline{\rho}_{f,\lambda}$ for some modular form f. Further suppose that*

(1) For all $\sigma : F \hookrightarrow L$, $\mathrm{HT}_\sigma(\rho) = \mathrm{HT}_\sigma(\rho_{f,\lambda})$ (i.e. $\rho, \rho_{f,\lambda}$ have the same Hodge-Tate weights)

(2) For all $v \mid p$, $\rho|_{G_{F_v}}$ and $\rho_{f,\lambda}|_{G_{F_v}}$ are crystalline.

(3) p is unramified in F

(4) For all $\sigma : F \hookrightarrow L$, the elements $\mathrm{HT}_\sigma(\rho)$ differ by at most $p - 2$.

(5) $\mathrm{Im}\,\overline{\rho} \supset \mathrm{SL}_2(\mathbb{F}_p)$.

Then, ρ is modular.

Remark 4. In [Gee22, Section 6], Gee discusses what sort of work would be needed to relax the hypotheses in Theorem 3. At the very least, I think it will be reasonable for us to aim to prove (something like) this for $p \geq 3$ instead of at least 5. Certainly, in order to have the theorem apply to *some* Frey curves (even if it still doesn't apply to enough of them to deduce FLT), we'll want to allow $p = 3$. In Appendix A, I'll say more about (my understanding of) which (semistable) elliptic curves Theorem 3 applies to. ◦

With all that out of the way, it's probably about time we get into the actual material that will be present in the talk.

1 Universal Deformation Rings (start of actual material)

We want to study ways of lifting a mod p representation $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{F}_p)$ to one valued in $\mathrm{GL}_n(A)$ where, for example A is a finite extension of $\mathbb{Z}_p$ (or even something more exotic like some version of a Hecke algebra). As it turns out, there is often a universal such lifting $G_{\mathbb{Q}} \to \mathrm{GL}_n(A^{\mathrm{univ}})$ from which all others are pushed forward. Our first task is to make this precise.

Notation 1.1. We fix the following notation throughout:

- p is a rational prime

[2] This is mostly because this whole area is new to me, so what I can plan for us to do is limited by a combination of my naivety and what approachable-seeming notes I can find.

[3] i.e. unramified almost everywhere and de Rham at all places above p

- $\mathbb{F}$ is a finite field of characteristic p, and $W(\mathbb{F})$ is the ring of integers in the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}$.

  Note 1. Witt was a nazi, so I'm gonna try to not call $W(\mathbb{F})$ by its usual name.

  Note 2. After finishing these notes, I realized I never actually use the notation $W(\mathbb{F})$ for anything, so I guess the above is just a public service announcement.

- $\mathscr{O} = \mathscr{O}_L$ denotes the ring of integers in some local field $L/\mathbb{Q}_p$ with residue field $\mathbb{F}$ (so $W(\mathbb{F})[1/p] \subset L$).

- $\mathcal{C}_{\mathscr{O}}$ will denote the category of local *artinian* $\mathscr{O}$-algebras with residue field $\mathbb{F}$.

- $\widehat{\mathcal{C}}_{\mathscr{O}}$ will denote the category of complete local *noetherian* $\mathscr{O}$-algebras with residue field $\mathbb{F}$.

  Warning 1.2. The adjective 'noetherian' appearing above stops $\widehat{\mathcal{C}}_{\mathscr{O}}$ from literally being pro–$\mathcal{C}_{\mathscr{O}}$, the pro-category on $\mathcal{C}_{\mathscr{O}}$. •

  Remark 1.3. Given $A \in \widehat{\mathcal{C}}_{\mathscr{O}}$, we let $\mathfrak{m}_A \subset A$ denote its maximal ideal. Note that the structure map $\mathscr{O} \to A$ gives a canonical identification $\mathbb{F} \xrightarrow{\sim} A/\mathfrak{m}_A$. ○

  Note 3. After finishing these notes, I realized I don't really ever use $\mathcal{C}_{\mathscr{O}}$, so I guess I didn't need to define it.

- G will denote a profinite group.

- $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a fixed continuous representation.

Definition 1.4. Choose $A \in \widehat{\mathcal{C}}_{\mathscr{O}}$. A `lift` (or `framed deformation`) of $\overline{\rho}$ to A is a continuous representation $\rho : G \to \mathrm{GL}_n(A)$ such that $\rho \mod \mathfrak{m}_A = \overline{\rho}$. On the other hand, a `deformation` of $\overline{\rho}$ to A is an equivalence class of lifts, where $\rho \sim \rho' \iff \rho' = a\rho a^{-1}$ for some $a \in \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$. ◇

Remark 1.5. Let $V = \mathbb{F}^{\oplus n}$, equipped with G-action specified by ρ, and let $\beta = (e_1, \dots, e_n)$ denote the canonical (ordered) $\mathbb{F}$-basis on V. Then, a deformation of V is equivalently a finite free A-module V_A w/ continuous G-action equipped with an isomorphism $V_A \otimes_A \mathbb{F} \xrightarrow{\sim} V$. A framed deformation is such a V_A along with a(n ordered) basis β_A which becomes identified with β upon passing from A to $\mathbb{F}$. ○

Notation 1.6. We consider the two functors $D_{\overline{\rho}}, D_{\overline{\rho}}^{\square} : \widehat{\mathcal{C}}_{\mathscr{O}} \to \mathrm{Set}$ given by

$$\begin{aligned} D_{\overline{\rho}}(A) &= \{\text{deformations of } \overline{\rho} \text{ to } A\} \\ D_{\overline{\rho}}^{\square}(A) &= \{\text{framed deformations of } \overline{\rho} \text{ to } A\}. \end{aligned}$$

The first basic result in the theory is that $D_{\overline{\rho}}^{\square}$ is always representable.

Warning 1.7. $D_{\overline{\rho}}$ is *not* always representable. As is often the case when one encounters non-representable functors, the issue is lies in the objects being parameterized having too many automorphisms. When $\mathrm{End}_{\mathbb{F}[G]}(\overline{\rho}) = \mathbb{F}$ (i.e. $\overline{\rho}$ is Schur), then there is no issue and $D_{\overline{\rho}}$ is representable. If more automorphisms exist though, one is better served by replacing $D_{\overline{\rho}}$ with the corresponding category cofibered in groupoids, see e.g. [BÏ3, Section 1.6]. •

1.1 Constructing the universal framed deformation

Let's prove representability of $D_{\overline{\rho}}^{\square}$ in a few steps.

(1) First suppose that G is finite.

Write $G = \langle g_1, \ldots, g_s \mid r_1(g_1, \ldots, g_s), \ldots, r_t(g_1, \ldots, g_s) \rangle$. Consider the ring (remember $n = \dim \overline{\rho}$)

$$\mathcal{R} = \mathscr{O}\left[X_{i,j}^k \mid i, j = 1, \ldots, n; k = 1, \ldots, s\right]/\mathcal{I},$$

where $\mathcal{I}$ is the ideal generated by the coefficients of the matrices

$$r_\ell(X^1, \ldots, X^s) - I_n \text{ where } X^k = \left(X_{i,j}^k\right)_{i,j=1}^n .$$

Thus, $\mathcal{R}$ is cooked up exactly so that it admits a representation $\rho : G \to \mathrm{GL}_n(\mathcal{R})$ sending $g_k \mapsto X^k$. This $\mathcal{R}$ is not necessarily complete, so let $\mathcal{J} \subset \mathcal{R}$ be the kernel of the map $\mathcal{R} \to \mathbb{F}$ which sends $X^k \mapsto \overline{\rho}(g_k)$, and set $R_{\overline{\rho}}^{\square} := \varprojlim_n \mathcal{R}/\mathcal{J}^n$. Then, ρ naturally extends to a representation $\rho^{\square} : G \to \mathrm{GL}_n(R_{\overline{\rho}}^{\square})$ and one can check that $(R_{\overline{\rho}}^{\square}, \rho^{\square})$ "represents" $D_{\overline{\rho}}^{\square}$.

Warning 1.8. The scare quotes are there because while $R_{\overline{\rho}}^{\square}$ is certainly a complete, local $\mathscr{O}$-algebra w/ residue field $\mathbb{F}$ such that

$$D_{\overline{\rho}}^{\square}(A) = \mathrm{Hom}(R_{\overline{\rho}}^{\square}, A)$$

for any $A \in \widehat{\mathcal{C}}_{\mathscr{O}}$, we still have not shown that $R_{\overline{\rho}}^{\square}$ is noetherian. •

(2) Now say that G is an arbitrary profinite group.

Write $G = \varprojlim_i G/H_i$ with i ranging over some directed poset I of open, normal subgroups $H_i \triangleleft G$ which are contained in $\ker(\overline{\rho})$. For each i, **(1)** above yields a universal pair $(R_i^{\square}, \rho_i^{\square})$, and now one defines

$$\left(R_{\overline{\rho}}^{\square}, \rho^{\square}\right) := \varprojlim_i \left(R_i^{\square}, \rho_i^{\square}\right).$$

(3) Show that $R = R_{\overline{\rho}}^{\square}$ is noetherian.

This will not be the case for arbitrary G, but we will see exactly the condition we need for this to hold.

Exercise. Choose $\{\alpha_i\}_{i\in I} \subset \mathfrak{m}_R$ whose images generate $\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathscr{O}})$, the "relative cotangent space of $\mathscr{O} \to R$". Then, the map

$$\begin{array}{rccc} \varphi : & \mathscr{O}[\![x_i : i \in I]\!] & \longrightarrow & R \\ & x_i & \longmapsto & \alpha_i \end{array}$$

is surjective.

By the above exercise, to show that the above constructed $R = R_{\overline{\rho}}^{\square}$ is noetherian, it will suffice to show that $\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathscr{O}})$ is finite dimensional. We now take a detour to do this...

Definition 1.9. Let $D : \widehat{\mathcal{C}}_{\mathscr{O}} \to \mathrm{Set}$ be a functor such that $D(\mathbb{F})$ consists of a single point. Its `Zariski tangent space` is $t_D := D(\mathbb{F}[\varepsilon])$, where $\mathbb{F}[\varepsilon] := \mathbb{F}[\varepsilon]/\varepsilon^2$. ◇

Remark 1.10. t_D always has a natural $\mathbb{F}$-action of "scalar multiplication." If D satisfies $D(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) \xrightarrow{\sim} D(\mathbb{F}[\varepsilon]) \times D(\mathbb{F}[\varepsilon])$ (e.g. if D is representable), then t_D supports an addition law as well. In this case, it is naturally an $\mathbb{F}$-vector space. ○

Exercise. Suppose $D : \widehat{\mathcal{C}}_{\mathscr{O}} \to \mathrm{Set}$ is representable, say by A. Then, there is a natural $\mathbb{F}$-linear isomorphism

$$t_A := \mathrm{Hom}_{\mathbb{F}}\big(\mathfrak{m}_A/(\mathfrak{m}_A^2, \mathfrak{m}_{\mathscr{O}}), \mathbb{F}\big) \xrightarrow{\sim} \mathrm{Hom}_{\mathscr{O}}(A, \mathbb{F}[\varepsilon]) \simeq D(\mathbb{F}[\varepsilon]) = t_D.$$

The above shows that A has the same tangent space as the functor it represents.

Lemma 1.11. *Let $R = R_{\overline{\rho}}^{\square}$ be the* `universal lifting ring` *constructed earlier. Then, the following are in bijection*

(1) $t_R = \mathrm{Hom}_{\mathbb{F}}\big(\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathscr{O}}), \mathbb{F}\big)$

(2) $t_{D_{\overline{\rho}}^{\square}}$

(3) *liftings of $\overline{\rho}$ to $\mathbb{F}[\varepsilon]$*

(4) *the set of cocycles $Z^1(G, \mathrm{ad}\overline{\rho})$, where $\mathrm{ad}\overline{\rho} : G \to \mathrm{Aut}(M_n(\mathbb{F})) \cong \mathrm{GL}_{n^2}(\mathbb{F})$ is the conjugation action of G (in other words, $\mathrm{ad}\overline{\rho} \cong \overline{\rho} \otimes \overline{\rho}^{\vee}$).*

Proof Sketch. That **(1)**,**(2)**,**(3)** are in bijection follows from the most recent exercise and expanding definitions. Let's show that **(3)** is in bijection with **(4)**. Given a cocycle $\varphi \in Z^1(G, \mathrm{ad}\overline{\rho})$, the corresponding lifting $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\varepsilon])$ is given by

$$\rho(g) := (1 + \varphi(g)\varepsilon)\,\overline{\rho}(g).$$

Conversely, given $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\varepsilon])$ lifting $\overline{\rho}$, one first defines $\theta : G \to M_n(\mathbb{F})$ via $\rho(g) = \overline{\rho}(g) + \theta(g)\varepsilon$ and then checks that $g \mapsto \theta(g)\overline{\rho}(g)^{-1}$ is a 1-cocycle in $Z^1(G, \mathrm{ad}\overline{\rho})$. ■

Corollary 1.12. *With R as above,*

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

Proof. This follows from the exact sequence

$$0 \longrightarrow \mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) \longrightarrow \mathrm{ad}\overline{\rho} \longrightarrow Z^1(G, \mathrm{ad}\overline{\rho}) \longrightarrow \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) \longrightarrow 0. \qquad \blacksquare$$

Corollary 1.13. *$R = R^{\square}_{\overline{\rho}}$ is noetherian (and so an element of $\widetilde{\mathcal{C}}_{\mathscr{O}}$) if*[4] *$\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$ is finite-dimensional.*

To understand the size of $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$, one can use inflation-restriction. Let $G' := \ker \overline{\rho}$. Then, we have a left exact sequence

$$0 \longrightarrow \mathrm{H}^1(G/G', \mathrm{ad}\overline{\rho}) \longrightarrow \mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) \longrightarrow \mathrm{H}^1(G', \mathrm{ad}\overline{\rho})^{G/G'}.$$

Note that G/G' and (the vector space underlying) $\mathrm{ad}\overline{\rho}$ are both finite, so $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$ is finite-dimensional if and only if $\mathrm{H}^1(G', \mathrm{ad}\overline{\rho})^{G/G'}$ is. Since G' acts trivially on $\mathrm{ad}\overline{\rho}$, we have

$$\mathrm{H}^1(G', \mathrm{ad}\overline{\rho}) = \mathrm{Hom}_{\mathrm{cts}}(G', \mathrm{ad}\overline{\rho}) = \mathrm{Hom}_{\mathrm{cts}}(G', \mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathrm{ad}\overline{\rho},$$

which is finite-dimensional if and only if $\mathrm{Hom}(G', \mathbb{F}_p)$ is.

Definition 1.14. We say G satisfies `Mazur's condition` Φ_p if $\mathrm{Hom}(G', \mathbb{F}_p)$ is finite for every open subgroup $G' \subset G$. ◇

Thus, the discussion so far has proven the following.

Theorem 1.15. *The framed deformation functor $D^{\square}_{\overline{\rho}} : \widehat{\mathcal{C}}_{\mathscr{O}} \to \mathrm{Set}$ is always pro-representable*[5] *by some $(R^{\square}_{\overline{\rho}}, \rho^{\square})$. If, furthermore, G satisfies Mazur's condition Φ_p, then $D_{\overline{\rho}}$ is representable, i.e. $R^{\square}_{\overline{\rho}}$ is noetherian.*

As a consequence of Corollary 1.12, we can write $R^{\square}_{\overline{\rho}}$ as a quotient

$$\pi : \mathscr{O}[\![x_1, \dots, x_d]\!] \twoheadrightarrow R^{\square}_{\overline{\rho}}, \text{ where } d := h^1(G, \mathrm{ad}\overline{\rho}) - h^0(G, \mathrm{ad}\overline{\rho}) + n^2$$

(send the x_i's to lifts of a basis for $t^{\vee}_{R^{\square}_{\overline{\rho}}}$). This tells us that $R^{\square}_{\overline{\rho}}$ has a presentation with d generators. How many relations does it require? Let $J = \ker \varphi$.

Proposition 1.16. *Let $\mathfrak{m} = (\mathfrak{m}_{\mathscr{O}}, x_1, \dots, x_d)$ be the maximal ideal of $\mathscr{O}[\![x_1, \dots, x_d]\!]$. There exists an injection $\mathrm{Hom}_{\mathbb{F}}(J/\mathfrak{m}J, \mathbb{F}) \hookrightarrow \mathrm{H}^2(G, \mathrm{ad}\overline{\rho})$.*

This is proved, for example, in [Zho, Lecture 7]. Thus, the presentation π has at most $\dim \mathrm{H}^2(G, \mathrm{ad}\overline{\rho})$ many relations.

[4] I'm pretty sure this is secretly an if and only if, but I didn't think too deeply about this

[5] i.e. represented by a ring which is an inverse limit of objects in $\mathcal{C}_{\mathscr{O}}$

Corollary 1.17. *Assume G satisfies Mazur's condition Φ_p.*

(1) *Then,*

$$\dim R_{\overline{\rho}}^{\square} \geq d+1-\dim_{\mathbb{F}} \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) = n^2+1-\dim \mathrm{H}^0(G, \mathrm{ad}\overline{\rho})+\dim \mathrm{H}^1(G, \mathrm{ad}\overline{\rho})-\dim \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}).$$

(2) *If* $\dim \mathrm{H}^2(G, \mathrm{ad}\overline{\rho}) = 0$*, then*
$$\mathscr{O}[\![x_1, \dots, x_d]\!] \xrightarrow{\sim} R_{\overline{\rho}}^{\square}$$

1.2 Brief discussion of the universal deformation

What about the deformation functor $D_{\overline{\rho}}$ without framings?

Theorem 1.18. *If $\overline{\rho}$ is Schur, then $D_{\overline{\rho}}$ is representable, say by $(R_{\overline{\rho}}^{univ}, \rho^{univ})$. We call $R_{\overline{\rho}}^{univ}$ the* `universal deformation ring`*.*

Proof Sketch. Let $\widehat{\mathrm{PGL}}_n$ denote the formal completion of $\mathrm{PGL}_{n,\mathscr{O}}$ along its identity section.[6] Then, $\widehat{\mathrm{PGL}}_n$ acts on $X = \mathrm{Spf}\, R_{\overline{\rho}}^{\square}$ via conjugating liftings and the Schur condition ensures that this action is free. One can then construct $R_{\overline{\rho}}^{\mathrm{univ}}$ as (the $\mathscr{O}$-algebra whose Spf is the formal scheme) $X/\widehat{\mathrm{PGL}}_n$. See [BÏ3, Theorem 2.1.1] for details. ■

(Alternatively, one can argue as in [DDT07, Thereom 2.36].)

We have already gotten a hint that tangent spaces are important, so we record the following

Lemma 1.19. *Let $R = R_{\overline{\rho}}^{univ}$ be the universal deformation ring constructed earlier. Then, the following are in bijection*

(1) $t_R = \mathrm{Hom}_{\mathbb{F}}\big(\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathscr{O}}), \mathbb{F}\big)$

(2) $t_{D_{\overline{\rho}}}$

(3) *deformations of $\overline{\rho}$ to $\mathbb{F}[\varepsilon]$*

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

(5) $\mathrm{Ext}^1(\overline{\rho}, \overline{\rho})$

Proof Sketch. If you view a deformation of $\overline{\rho}$ to $\mathbb{F}[\varepsilon]$ as a finite free $\mathbb{F}[\varepsilon]$-module V whose reduction mod ε is $V_{\mathbb{F}}$ (the module underlying $\overline{\rho}$), then it becomes clear that V sits in an extension

$$0 \longrightarrow \varepsilon V_{\mathbb{F}} \longrightarrow V \longrightarrow V_{\mathbb{F}} \longrightarrow 0,$$

and this assignment gives the bijection **(3)**→**(5)**. To connect everything else to **(4)**, one could either

[6] This has functor of points $\widehat{\mathrm{PGL}}_n(A) = \ker(\mathrm{PGL}_n(A) \to \mathrm{PGL}_n(\mathbb{F}))$, see [BÏ3, Exercise 2.8.1].

- Show that the construction in Lemma 1.11 assigns two liftings to $\mathbb{F}[\varepsilon]$ to cohomologous cocycles exactly when they are conjugate; or
- consider the following construction: given an extension $0 \to V_{\mathbb{F}} \to V \to V_{\mathbb{F}} \to 0$ with $V_{\mathbb{F}}$ the $\mathbb{F}[G]$-module underlying $\overline{\rho}$, one can tensor with $V_{\mathbb{F}}^{\vee}$ to get an extension $0 \to \mathrm{ad}\overline{\rho} \to V \otimes V_{\mathbb{F}}^{\vee} \to \mathrm{ad}\overline{\rho} \to 0$, and then consider the image of $\mathrm{id} \in \mathrm{H}^0(G, \mathrm{ad}\overline{\rho})$ under the coboundary map $\mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) \to \mathrm{H}^1(G, \mathrm{ad}\overline{\rho})$ of this extension; or
- argue that $M \rightsquigarrow \mathrm{Ext}^i_G(\mathbb{F}, (-) \otimes \overline{\rho}^{\vee})$ and $M \rightsquigarrow \mathrm{Ext}^i_G(\overline{\rho}, -)$ are (co)effacable δ-functors (on the category of continuous, discrete $\mathbb{F}[G]$-modules) which agree with $i = 0$ and so must agree for higher i (and also note that $\mathrm{H}^1(G, \mathrm{ad}\overline{\rho}) = \mathrm{Ext}^1_G(\mathbb{F}, \mathrm{ad}\overline{\rho})$). ■

Definition 1.20. Let $\varphi : D' \to D$ be a natural transformation of functors $\widehat{\mathcal{C}}_{\mathscr{O}} \to \mathrm{Set}$. We say φ is `formally smooth` if for any surjection $A \to A'$ in $\mathcal{C}_{\mathscr{O}}$ (i.e. A, A' both artinian), the induced map

$$D'(A) \longrightarrow D'(A') \times_{D(A')} D(A)$$

is surjective. ◇

Proposition 1.21. *The natural transformation $D^{\square}_{\overline{\rho}} \to D_{\overline{\rho}}$ sending a lifting of $\overline{\rho}$ to its deformation class is formally smooth. Thus, if $D_{\overline{\rho}}$ is representable, then*

$$R^{\square}_{\overline{\rho}} \cong R^{univ}_{\overline{\rho}}[\![x_1, \ldots, x_r]\!] \quad \textit{where } r := n^2 - h^0(G, \mathrm{ad}\overline{\rho}).$$

Proof. That this map is formally smooth follows from simply expanding definitions; it is the tautological statement that, given $A \to A'$, if you have a lifting of $\overline{\rho}$ to A' which is conjugate to some lifting to A, then it is isomorphic to some lifting to A.

Suppose that $D_{\overline{\rho}}$ is representable, so we have $R^{\square}_{\overline{\rho}} \to R^{\mathrm{univ}}_{\overline{\rho}}$. Let $\mathfrak{m}_{\square} := \mathfrak{m}_{R^{\square}_{\overline{\rho}}}$ and $\mathfrak{m} := \mathfrak{m}_{R^{\mathrm{univ}}_{\overline{\rho}}}$. Considering the surjection $\mathbb{F}[\varepsilon] \xrightarrow{\varepsilon=0} \mathbb{F}$, we in particular see that

$$\mathrm{Hom}_{\mathbb{F}}\big(\mathfrak{m}_{\square}/(\mathfrak{m}_{\square}^2, \mathfrak{m}_{\mathscr{O}}), \mathbb{F}\big) \longrightarrow \mathrm{Hom}_{\mathbb{F}}\big(\mathfrak{m}/(\mathfrak{m}^2, \mathfrak{m}_{\mathscr{O}}), \mathbb{F}\big)$$

is surjective, so $\mathfrak{m}/(\mathfrak{m}^2, \mathfrak{m}_{\mathscr{O}}) \hookrightarrow \mathfrak{m}_{\square}/(\mathfrak{m}_{\square}^2, \mathfrak{m}_{\mathscr{O}})$ is injective. Choosing r generators for the cokernel (possibly by Corollary 1.12 + Lemma 1.19) and lifting them to $\mathfrak{m}_{\square}$, we obtain a surjection

$$R^{\mathrm{univ}}_{\overline{\rho}}[\![x_1, \ldots, x_r]\!] \twoheadrightarrow R^{\square}_{\overline{\rho}}.$$

Formally smoothness in fact implies that this is an isomorphism. It's an isomorphism on tangent spaces (i.e. on $\mathbb{F}[\varepsilon]$-points) by construction. One can then induct on the length of an artinian $\mathscr{O}$-algebra A to show that it's an isomorphism on A-points in general. ■

Remark 1.22. When $\overline{\rho}$ is Schur, one has $h^0(G, \mathrm{ad}\overline{\rho}) = 1$ (since $\mathrm{H}^0(G, \mathrm{ad}\overline{\rho}) = \mathrm{End}_{\mathbb{F}[G]}\,\overline{\rho} = \mathbb{F}$ by assumption), so $R^{\square}_{\overline{\rho}}$ is (ismorphic to) a power series ring in $n^2 - 1$ variables over $R^{\mathrm{univ}}_{\overline{\rho}}$. According to [Gee22, Exercise 3.9], the universal lifting

$$\rho^{\square} : G \longrightarrow \mathrm{GL}_n\left(R_{\overline{\rho}}^{\mathrm{univ}}[\![X_{i,j}]\!]_{i,j=1}^{n} / (X_{1,1})\right)$$

is $\rho^{\square} = (I_n + (X_{i,j}))\, \rho^{\mathrm{univ}} (I_n + (X_{i,j}))^{-1}$. ◦

Slogan. $R_{\overline{\rho}}^{\square}$ and $R_{\overline{\rho}}$ have equivalent singularities.

2 Deformation Problems and Galois Deformations

Continue to use the notation from Notation 1.1. We will soon specialize to the case that our profinite group G is (a quotient of) the Galois group of some p-adic or number field.

Exercise. Prove that both of the following groups satisfy Mazur's condition Φ_p:

- The absolute Galois group G_L for $L/\mathbb{Q}_p$ a finite extension.
- The maximal quotient $G_{K,S}$ of G_K (for $K/\mathbb{Q}$ a number field) which is unramified outside a specified finite set S of places of K.

Before specializing to one of the above cases, we introduce the notion of a *deformation problem*. The universal lifting ring $R_{\overline{\rho}}^{\square}$ is generally too big; in practice, one is not interested in *all* liftings of a given residual representation, but only those which are "nice enough". For example, if $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a modular representation, and we want to show some lifting $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ is also modular, then we better hope at the very least that ρ has the right determinant and is geometric; if we want ρ to be modular of a specified level N, then we'd also want it to be unramified away from N.

Thus, the deformation rings one works with in practice are certain quotients of $R_{\overline{\rho}}^{\square}$ which classify liftings satisfying specified desirable conditions.

Definition 2.1. A `deformation problem` $\mathcal{D}$ is a collection of liftings (R, ρ) of $(\mathbb{F}, \overline{\rho})$ (with $R \in \mathrm{ob}\,\widehat{\mathcal{C}}_{\mathscr{O}}$) satisfying the following

(1) $(\mathbb{F}, \overline{\rho}) \in \mathcal{D}$

(2) If $f : R \to S$ is a morphism in $\widehat{\mathcal{C}}_{\mathscr{O}}$ and $(R, \rho) \in \mathcal{D}$, then $(S, f \circ \rho) \in \mathcal{D}$.

(3) If $f : R \hookrightarrow S$ is an injective morphism in $\widehat{\mathcal{C}}_{\mathscr{O}}$, then $(R, \rho) \in \mathcal{D}$ if and only if $(S, f \circ \rho) \in \mathcal{D}$

(4) Suppose that $R_1, R_2 \in \mathrm{ob}\,\widehat{\mathcal{C}}_{\mathscr{O}}$ and I_1, I_2 are closed ideals of R_1, R_2, respectively, equipped with an isomorphism $f : R_1/I_1 \xrightarrow{\sim} R_2/I_2$.

If $(R_1, \rho_1), (R_2, \rho_2) \in \mathcal{D}$ and $f(\rho_1 \bmod I_1) = \rho_2 \bmod I_2$, then their fiber product

$$R := R_1 \times_{R_1/I_2} R_2 := \{(r_1, r_2) \in R_1 \oplus R_2 : f(r_1 \mod I_1) = r_2 \mod I_2\},$$

equipped with $\rho := \rho_1 \oplus \rho_2$ is in $\mathcal{D}$ as well.

(5) If (R, ρ) is a lifting of $(\mathbb{F}, \overline{\rho})$ and $I_1 \supset I_2 \supset \dots$ is a sequence of ideals of R with $\bigcap_j I_j = 0$ such that $(R/I_j, \rho \mod I_j) \in \mathcal{D}$ for all j, then $(R, \rho) \in \mathcal{D}$.

(6) If $(R, \rho) \in \mathcal{D}$ and $a \in \ker(\mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbb{F}))$, then $(R, a\rho a^{-1}) \in \mathcal{D}$. ◇

Remark 2.2. Let $K := \ker\big(\mathrm{GL}_n(R^\square_{\overline{\rho}}) \to \mathrm{GL}_n(\mathbb{F})\big)$. Then, $K \curvearrowright R^\square_{\overline{\rho}}$ as follows. Each $a \in K$ acts via the homomorphism $R^\square_{\overline{\rho}} \to R^\square_{\overline{\rho}}$ corresponding to the lifting

$$a^{-1}\rho^\square a : G \to \mathrm{GL}_n(R^\square_{\overline{\rho}})$$

of $\overline{\rho}$ (recall $\mathrm{End}(R^\square_{\overline{\rho}}) = D^\square_{\overline{\rho}}(R^\square_{\overline{\rho}})$). ○

Proposition 2.3. *Let $\mathcal{D}$ be a deformation problem. Then, there exists a K-invariant ideal $I(\mathcal{D}) \subset R^\square_{\overline{\rho}}$ such that a lifting $\rho : G \to \mathrm{GL}_n(R)$ of $\overline{\rho}$ lies in $\mathcal{D}$ if and only if the kernel of the induced map $R^\square_{\overline{\rho}} \to R$ contains $I(\mathcal{D})$, i.e. if and only if $R^\square_{\overline{\rho}} \to R$ factors through $R^\square_{\overline{\rho}}/I(\mathcal{D})$.*

(See [Gee22, Lemma 3.17] for more on the connection between deformation problems and K-invariant ideals)

Proof. Let $\mathcal{J}$ denote the set of ideals I of $R^\square_{\overline{\rho}}$ such that $(R^\square_{\overline{\rho}}/I, \rho^\square) \in \mathcal{D}$. By property **(3)** of Definition 2.1, $(R, \rho) \in \mathcal{D}$ if and only if the kernel of the induced map $f_\rho : R^\square_{\overline{\rho}} \to R$ is in $\mathcal{J}$. We claim that $\mathcal{J}$ has a minimal element, which we'll call $I(\mathcal{D})$, that is contained in all other elements. First note that $\mathcal{J}$ is non-empty by property **(1)** of Definition 2.1. Furthermore, properties **(4)** and **(5)** tell us that $\mathcal{J}$ is closed under (arbitrary) finite intersections and nested countable intersections. Taken together, this means that $\mathcal{J}$ is closed under (arbitrary) countable intersections.[7] Thus, it suffices to show that $\mathcal{J}$ is countable (and then $I(\mathcal{D}) = \bigcap_{I \in \mathcal{J}} I$). This is true simply because every $R \in \widehat{\mathfrak{C}}_{\mathscr{O}}$ has only countably many ideals.[8] ■

Remark 2.4. Given a deformation problem $\mathcal{D}$, let $\mathcal{D}^\square_{\overline{\rho}} : \widehat{\mathfrak{C}}_{\mathscr{O}} \to \mathrm{Set}$ (not to be confused with $D^\square_{\overline{\rho}}$) denote the functor sending A to the set $\mathcal{D}^\square_{\overline{\rho}}(A)$ of framed deformations $\rho : G \to \mathrm{GL}_n(A)$ of $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ such that $(A, \rho) \in \mathcal{D}$. Then, Proposition 2.3 tells us that $\mathcal{D}^\square_{\overline{\rho}}$ is represented by the ring $R^\square_{\overline{\rho}}/I(\mathcal{D}) =: R^{\square,\mathcal{D}}_{\overline{\rho}}$. ○

The above notion of deformation problem (seemingly) says nothing about determinants. However, these are easy to handle/fix.

Construction 2.5. Fix a character $\chi : G \to \mathscr{O}^\times$ such that $\chi \otimes_{\mathscr{O}} \mathbb{F} = \det \overline{\rho}$. Let $\mathcal{D}$ be a deformation problem. Then, the functor

$$\mathcal{D}^\square_{\overline{\rho},\chi}(A) := \{\rho : G \to \mathrm{GL}_n(A) \mid \det \rho = \chi \text{ and } (A, \rho) \in \mathcal{D}\}$$

is represented by "the quotient of $R^{\square,\mathcal{D}}_{\overline{\rho}}$ by $\det \rho - \chi$" (where $\rho : G \to \mathrm{GL}_n(R^{\square,\mathcal{D}}_{\overline{\rho}})$ is the universal object). Here's one way to make this precise. First realize that we have a ring $R^\square_{\det \overline{\rho}}$ representing

[7]Given, $I_1, I_2, \dots, \in \mathcal{J}$, notice that $\bigcap_{n \ge 1} I_n = \bigcap_{n \ge 1} (\bigcap_{k=1}^n I_k)$

[8]Hint: every ideal of R contains $\mathfrak{m}_R^n$ for some n, and every quotient $R/\mathfrak{m}_R^n$ is artinian (so only has finitely many ideals)

liftings of $\det\overline{\rho}$. Thus, we get two maps $R^{\square}_{\det\overline{\rho}} \rightrightarrows R^{\square,\mathcal{D}}_{\overline{\rho}}$ representing the two choices of liftings $\det\rho : G \to \left(R^{\square,\mathcal{D}}_{\overline{\rho}}\right)^{\times}$ and $\chi : G \to \mathscr{O}^{\times} \to \left(R^{\square,\mathcal{D}}_{\overline{\rho}}\right)^{\times}$. The functor $\mathcal{D}^{\square}_{\overline{\rho},\chi}$ is represented by the coequalizer

$$R^{\square,\mathcal{D}}_{\overline{\rho},\chi} := \mathrm{CoEq}\left(R^{\square}_{\det\overline{\rho}} \rightrightarrows \left(R^{\square,\mathcal{D}}_{\overline{\rho}}\right)^{\times}\right). \qquad \bigcirc$$

Remark 2.6. Alternatively, we can construct $R^{\square,\mathcal{D}}_{\overline{\rho},\chi}$ above as the quotient of $R^{\square,\mathcal{D}}_{\chi}$ by the ideal generated by the elements $\det\rho(g) - \chi(g) \in R^{\square,\mathcal{D}}_{\chi}$. $\circ$

Exercise. Prove or disprove the following

- For fixed $\chi : G \to \mathscr{O}^{\times}$ lifting $\det\overline{\rho}$, the collection $\mathcal{D}_{\chi}$ of (A,ρ) such that $\det\rho = \chi$ is a deformation problem.
- For deformation problems $\mathcal{D}_1, \mathcal{D}_2$, the collections $\mathcal{D}_1 \cup \mathcal{D}_2$ and $\mathcal{D}_1 \cap \mathcal{D}_2$ are deformation problems.

2.1 Galois Deformations with Local Conditions

We've finally done enough setup to start talking about the specific sort of deformation rings we actually care about. Continue to use Notation 1.1.

Setup 2.7. Fix a number field $F/\mathbb{Q}$ and choose embeddings $\overline{F} \hookrightarrow \overline{F}_v$ for all places v of F. Fix a finite set S of places of F, let F_S/F be the maximal extension unramified outside S, and set $G := G_{F,S} := \mathrm{Gal}(F_S/F)$.

Definition 2.8. A `global Galois deformation problem` $\mathcal{S} = (F, S, \mathscr{O}, \overline{\rho}, \chi, \{\mathcal{D}_v\}_{v\in S})$ is a tuple consisting of

- $F, S, \mathscr{O}$ as before
- $\overline{\rho} : G_{F,S} \to \mathrm{GL}_n(\mathbb{F})$ a continuous representation, which we'll assume to be Schur
- $\chi : G_{F,S} \to \mathscr{O}^{\times}$ continuous such that $\chi \mod \mathfrak{m}_{\mathscr{O}} = \det\overline{\rho}$
- $\mathcal{D}_v$ a deformation problem for $\overline{\rho}|_{G_v}$. $\diamond$

Remark 2.9. As suggested by [Gee22, Section 3.20], one could make this definition in a more general context, e.g. G a profinite group equipped with maps $G_v \to G$ from some collection of other profinite groups (w/ no relation to Galois theory). $\circ$

Definition 2.10. Choose a subset $T \subset S$ (possibly $T = \emptyset$), and let $\mathcal{S}$ be a global Galois deformation problem. Let $D^{\square,T}_{\mathcal{S}} : \widehat{\mathfrak{C}}_{\mathscr{O}} \to \mathrm{Set}$ be the functor

$$D^{\square,T}_{\mathcal{S}}(A) := \left\{\left(\rho, \{\alpha_v\}_{v\in T}\right)\right\} / \sim,$$

where

- $\rho : G \to \mathrm{GL}_n(A)$ is a lift of $\overline{\rho}$
- $\alpha_v \in \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$ for all $v \in T$
- $\det \rho = \chi$
- $\rho|_{G_v} \in \mathcal{D}_v$ for all $v \in S$,

and the relation $\sim$ is generated by

$$(\rho, \{\alpha_v\}) \sim \left(\beta\rho\beta^{-1}, \{\beta\alpha_v\}\right) \text{ for all } \beta \in \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))\,.$$

An element of $D_{\mathcal{D}}^{\square,T}$ is called a `$T$-framed deformation` of $\overline{\rho}$ of type $\mathcal{S}$. $\diamond$

Remark 2.11. A T-framed deformation of $\overline{\rho}$ is a deformation (not lifting!) of $\overline{\rho}$ with specified local behavior at S (and with fixed determinant) in addition to framings at T. In particular, given $(\rho, \{\alpha_v\}_{v\in T})$, $\rho|_{G_v}$ is not a well-defined element of $\mathcal{D}_v$ (it's not $\sim$-invariant), but $\alpha_v^{-1}\rho|_{G_v}\alpha_v$ is (when $v \in T$).

Recall that the universal deformation ring $R^{\mathrm{univ}}_{\overline{\rho}|_{G_v}}$ may not exist if $\overline{\rho}|_{G_v}$ is reducible, while the universal framed deformation ring $R^{\square}_{\overline{\rho}|_{G_v}}$ always exists. Considering T-framed deformations allows one to better study deformations of $\overline{\rho}$ which become reducible when restricted to some G_v's. $\circ$

Theorem 2.12. *Choose a subset $T \subset S$, and let $\mathcal{S}$ be a global Galois deformation problem. Then, $D_{\mathcal{S}}^{\square,T}$ is representable by some $R_{\mathcal{S}}^{\square,T} \in \widehat{\mathcal{C}}_{\mathcal{O}}$.*

Notation 2.13. If $T = \emptyset$, we set $R^{\mathrm{univ}}_{\mathcal{S}} := R^{\square,\emptyset}_{\mathcal{S}}$. If $T = S$, we set $R^{\square}_{\mathcal{S}} := R^{\square,S}_{\mathcal{S}}$.

(The below is my best attempt at making sense of how one constructs this)

Proof Sketch. Convince yourself that the functor $A \rightsquigarrow \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$ is representable, say by B. Now, it's not too hard to show that the functor sending A to the set of all T-*framed liftings* of $\overline{\rho}$ of type $\mathcal{S}$ is represented by a suitable quotient of $R^{\square,\mathcal{D}}_{\overline{\rho},\chi} \oplus B^{\oplus\#T}$, where $\mathcal{D}$ is the deformation problem consisting of reps which are locally in $\mathcal{D}_v$ for all v. Call this quotient R. Now, one can construct $R^{\square,T}_{\mathcal{S}}$ as the quotient of R by its natural $\widehat{\mathrm{PGL}_n}$-action. ■

Thus, we finally have rings $R^{\square,T}_{\mathcal{S}}$ which control deformations of $\overline{\rho}$ with specified determinant and local behavior. The ultimate goal is to understand these rings well enough to say that every such deformation of $\overline{\rho}$ must be modular (this will amount to showing that $R^{\square,T}_{\mathcal{S}}$ is essentially some Hecke algebra). Understanding $R^{\square,T}_{\mathcal{S}}$ in particular means controlling its Krull dimension. The utility of this is seen in statements like the following.

Lemma 2.14. *Let A be a complete noetherian local domain. If $A[\![x_1, \ldots, x_n]\!] \twoheadrightarrow R$ is a surjection onto a complete local ring of dimension $n + \dim A$, then it is an isomorphism.*

Proof. Let $\mathfrak{p} \subset R$ be a minimal prime (so $\dim R = \dim(R/\mathfrak{p})$). Then, the composition $A[\![x_1, \ldots, x_n]\!] \twoheadrightarrow R \twoheadrightarrow R/\mathfrak{p}$ is an isomorphism (the kernel must be a height 0 prime), so $A[\![x_1, \ldots, x_n]\!] \twoheadrightarrow R$ must be an isomorphism as well. ■

Remark 2.15. To see the actual sort of statements one uses in the end, check out these notes on patching. ◦

Thus, if we eventually construct some surjection $R_{\mathcal{S}}^{\square,T} \twoheadrightarrow \mathbb{T}$ that we hope to be an isomorphism, it could be useful to know things like the dimensions of these rings and the number of generators/relations needed to write down presentations for them.

With that said, we end this section by noting that $R_{\mathcal{S}}^{\square,T}$ is naturally an algebra over

$$R_{\mathcal{S},T}^{\mathrm{loc}} := \widehat{\bigotimes}_{v\in T} R_{\overline{\rho}|_{G_v},\mathcal{X}}^{\square,\mathcal{D}_v}$$

(need $v \in T$ in order to have a well-defined element $\alpha_v^{-1}\rho^{\square,T}\alpha_v$ of $\mathcal{D}_v$ over $R_{\mathcal{S}}^{\square,T}$). In a later talk, we will discuss the number of generators/relations needed to present $R_{\mathcal{S}}^{\square,T}$ over $R_{\mathcal{S},T}^{\mathrm{loc}}$, akin to observations made in and above Corollary 1.17 (see [Gee22, 3.23]).

3 Intro to Hecke Algebras and $R = \mathbb{T}$?

Our eventual goal, as has maybe been alluded to a few times now, is to show that some suitable universal deformation ring R is in fact a Hecke algebra (and then use this to deduce that all deformations represented by R are modular). In order to make sense of this, we at least need to produce a map from R to some Hecke algebra $\mathbb{T}$, i.e. we need to construct some $\mathbb{T}$-valued Galois representation. We (hopefully briefly) explain how in the current section.

Remark 3.1. The below (Section 3.1) is my preferred way of thinking of modular forms and Hecke operators. I feel empowered to present them this way because I'm assuming the audience already has some familiarity with these objects. For other perspectives on this material, you can see e.g. [DDT07, Section 3.3] or [The, Lecture 8] (for sources concerned w/ modularity lifting), [DS05] (for a introduction to modular forms/Hecke operators), and/or [Gro90] (for more info on the perspective adopted below). If you really want lots for relevant information, check out this book. ◦

I'm gonna try to be somewhat quick in this section.

3.1 Defining Modular Forms and Hecke Algebras

I'm not 100% sure I have all my definitions correct yet, so take this section w/ a grain of salt.

Notation 3.2. Fix some integer $N \geq 1$. Let $\mathcal{X}_1(N)/\mathbb{Z}[1/N]$ denote the moduli stack parameterizing triples $(S, E/S, \alpha : \mu_{N,S} \hookrightarrow E)$ where S is a $\mathbb{Z}[1/N]$-scheme, E is a generalized elliptic scheme over S, and α is an embedding of S-group schemes. Write $X_1(N)$ for the coarse space of $\mathcal{X}_1(N)$, so this is always a scheme.

($\mathcal{X}_1(N)$ is a scheme if $N \geq 5$. Even if N is small, you won't lose much if you pretend in your head that this is a scheme)

Warning 3.3. Some others prefer to use $\underline{\mathbb{Z}/N\mathbb{Z}}$ in place of μ_N above. This has the disadvantage that the Tate curve $\mathbb{G}_m/q^{\mathbb{Z}}$ naturally has μ_N as a subscheme instead of $\underline{\mathbb{Z}/N\mathbb{Z}}$. So, using $\underline{\mathbb{Z}/N\mathbb{Z}}$, you can only define q-expansions of modular forms over $\mathbb{Z}[1/N, \zeta_N]$-algebras, but I'm getting ahead of myself... $\bullet$

Over $\mathcal{X}_1(N)$ there is a universal generalized elliptic curve $\pi : \mathcal{E} \to \mathcal{X}_1(N)$ equipped with a canonical embedding of μ_N.

Definition 3.4. The Hodge bundle on $\mathcal{X}_1(N)$ is the line bundle $\omega := \pi_*\omega_{\mathcal{E}/\mathcal{X}_1(N)}$, where $\omega_{\mathcal{E}/\mathcal{X}_1(N)}$ is the relative dualizing sheaf. A little less scary sounding, this is equivalently the pullback $\sigma^*\Omega^1_{\mathcal{E}/\mathcal{X}_1(N)}$ of the sheaf of relative differentials along the identity section $\sigma : \mathcal{X}_1(N) \to \mathcal{E}$. $\diamond$

Definition 3.5. Consider any $\mathbb{Z}[1/N]$-algebra R. The space of modular forms of weight k and level $\Gamma_1(N)$ over R is

$$M_k(N, R) := \mathrm{H}^0(\mathcal{X}_1(N)_R, \omega^{\otimes k}).$$

Similarly, a cusp form is a section of $\omega^{\otimes k}(-\text{cusps})$. $\diamond$

Remark 3.6. Aren't modular forms supposed to be fancy functions on the upper half place? Say $R = \mathbb{C}$. Given any $\tau \in \mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$, consider the elliptic curve

$$E_\tau := \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau) \xrightarrow[\exp(2\pi i z)]{\sim} \mathbb{C}^\times/q^{\mathbb{Z}} \text{ where } q = e^{2\pi i \tau}.$$

Let α be the natural embedding $\mu_N(\mathbb{C}) \hookrightarrow \mathbb{C}^\times/q^{\mathbb{Z}} = E_\tau$, and let $\varphi = (E_\tau, \alpha) \in \mathcal{X}_1(N)(\mathbb{C})$.

Now, let $f \in M_k(N, \mathbb{C})$ be a modular form over $\mathbb{C}$. Note that $\varphi^*\omega$ is simply the 1-dimensional $\mathbb{C}$-vector space $\mathrm{H}^0(E_\tau, (\Omega^1_{E_\tau})^{\otimes k}) \cong \mathrm{H}^0(E_\tau, \mathscr{O})$ of kth tensor powers of invariant differentials on E_τ. Thus, it has a basis given by $(\frac{\mathrm{d}z}{z})^{\otimes k}$, where z is the parameter on $\mathbb{C}$.[9] Then, we may define $f(\tau) \in \mathbb{C}$ via

$$\varphi^* f = f(\tau)\left(\frac{\mathrm{d}z}{z}\right)^{\otimes k} \in \mathrm{H}^0(E_\tau, (\Omega^1_{E_\tau})^{\otimes k}).$$

This is how you recover the usual definition of modular forms from this one. $\circ$

Remark 3.7. You can also think of a modular form as a (sensible) rule which assigns to any pair (E, α) defined over (some scheme S defined over) R, an element $f(E, \alpha) \in \mathrm{H}^0(S, \omega^{\otimes k})$, where ω is the Hodge bundle on S. $\circ$

Let's define the Hecke operators.

Definition 3.8. For each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have the diamond operator $\langle d\rangle$, which we'll think of as the automorphism of $X_1(N)$ given by

$$\langle d\rangle\,(E, \alpha) = (E, d\alpha). \quad \diamond$$

Definition 3.9. For each prime $p \nmid N$, we consider the moduli stack $\mathcal{X}_1(N; p)/\mathbb{Z}[1/N]$ parameterizing tuples $(S, E/S, \alpha, \beta)$ where $(S, E/S, \alpha) \in \mathcal{X}_1(N)(S)$ and $\beta : E \to E'$ is an isogeny of degree

[9]The differntial $\mathrm{d}z$ on $\mathbb{C}$ is invariant under translation $z \mapsto z + c$ (for any $c \in \mathbb{C}$) and so descends to a(n invariant) differential on $E_\tau = \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$. Under the isomorphism $E_\tau \simeq \mathbb{C}^\times/q^{\mathbb{Z}}$, $\mathrm{d}z \leftarrow\!\shortmid \mathrm{d}(\log(z)/(2\pi i)) = \mathrm{d}z/(2\pi i z)$. Thus, $\mathrm{d}z/z$ is an invariant differential on E_τ and so generates $\mathrm{H}^0(E_\tau, \Omega^1)$.

p. This has two maps $\mathcal{X}_1(N;p) \rightrightarrows \mathcal{X}_1(N)$ given by $(E,\alpha,\beta) \mapsto (E,\alpha)$ and $(E,\alpha,\beta) \mapsto (E', \beta\circ\alpha)$. We'll think of the `Hecke correspondence` T_p as the correspondence

$$\begin{tikzcd} & \mathcal{X}_1(N;p) \arrow[dl] \arrow[dr] & \\ \mathcal{X}_1(N) & & \mathcal{X}_1(N) \end{tikzcd}$$ ◇

(there are $p+1$ isogenies $E \to E'$ of degree p; think about order p subgroups of $(\mathbb{Z}/p\mathbb{Z})^2$)

Warning 3.10. In the above (and below) examples, I've really only properly defined $\mathcal{X}_1(N;p)$ away from the cusps. For a reference that's a bit more careful, see e.g. [Gro90, Section 3]. •

Definition 3.11. For each prime $p \mid N$, we let $\mathcal{X}_1(N;p)/\mathbb{Z}[1/N]$ be the moduli stack parametrizing tuples $(S, E/S, \alpha, \beta)$ where $(S, E/S, \alpha) \in \mathcal{X}_1(N)(S)$ and $\beta : E \to E'$ is a degree p isogeny *such that* $\operatorname{im}\alpha \cap \ker\beta = 0$. As before, we'll think of the `Hecke correspondence` U_p as the correspondence

$$\begin{tikzcd} & \mathcal{X}_1(N;p) \arrow[dl] \arrow[dr] & \\ \mathcal{X}_1(N) & & \mathcal{X}_1(N) \end{tikzcd}$$

In fact, we'll often write T_p in place of U_p even when $p \mid N$. ◇

Remark 3.12. The diamond operator and Hecke correspondences all act on the space of modular forms. For example, T_p sends a modular form f to the modular form $f|T_p$ (when $p \nmid N$) corresponding to the rule (see Remark 3.7)[10]

$$f|T_p(E,\alpha) = \frac{1}{p}\sum_{\beta:E\to E'} \beta^*(f(E',\beta\alpha))$$

(If $p \mid N$, only sum over isogenies for which $\ker\beta \cap \operatorname{im}\alpha = 0$). More simply, $\langle d\rangle$ acts via $f|\langle d\rangle(E,\alpha) = f(E, d\alpha)$. ○

Warning 3.13. Shouldn't we worry about the division by p above, at least if $p \nmid N$? No, it all works out. $f|T_p$ is still defined over R instead of over $R[1/p]$. The easiest way to see this is to just work out the effect on q-expansions.[11] •

Remark 3.14. $\langle d\rangle$ and T_p induce analogous correspondences on the coarse space $X_1(N)$, and hence also act on the Jacobian $J_1(N) := \operatorname{Jac} X_1(N)$ (since correspondences naturally act on divisors). We define the `Hecke algebra` $\mathbb{T}(N)$ `of level` N to be the subring $\mathbb{T}(N) \subset \operatorname{End}(J_1(N)_{\mathbb{Q}})$ generated

[10] Note that T_p acts on modular forms via $\frac{1}{p}$ times the usual action of a correspondence of sections of a line bundle.

[11] The Tate curve gives a $\mathbb{Z}[\![q]\!]$ point of $\mathcal{X}_1(N)$ w/ a canonical basis for (sections of) its Hodge bundle. Evaluating a modular form on this Tate curve and then expression it as some $(R \otimes \mathbb{Z}[\![q]\!])$-multiple of the canonical basis element let's you define q-expansions over R.

(over $\mathbb{Z}$) by the actions of the diamond operators $\langle d\rangle$ and the Hecke correspondences T_p (for all p). Similarly, we define the `anemic Hecke algebra` $\mathbb{T}'(N)$ `of level` N as the subring $\mathbb{T}_0(N) \subset \mathbb{T}(N)$ generated by the diamond operators $\langle d\rangle$ and the Hecke operators T_p for $p \nmid N$. ◦

Warning 3.15. Since I'm realizing $\mathbb{T}(N)$ inside the endomorphism ring of the Jacobian, I guess this is really (a quotient of) the "weight 2" Hecke algebra. In general, you get a "weight k" Hecke algebra inside $\mathrm{End}(S_k(N,R))$; this weight will be reflected e.g. in the determinant of the Galois representation attached to characters of $\mathbb{T}(N)$. •

3.2 $R = \mathbb{T}$?

For my talk, I'll probably skip the above and jump straight to here after defining the various universal deformation/lifting rings

Fix some integer $N \geq 1$.

Remark 3.16. $\mathbb{T}(N)$ is a finite, free $\mathbb{Z}$-algebra, e.g. since it's contained in $\mathrm{End}_{\mathbb{Q}}(J_1(N))$. In particular, it is integral over $\mathbb{Z}$ so it has (finitely many) minimal primes which are exactly the ones living over $(0) \subset \mathbb{Z}$ and every nonminimal prime is maximal (and lives over some $(p) \subset \mathbb{Z}$). ◦

Remark 3.17. The above remark holds also for the anemic Hecke algebra $\mathbb{T}_0(N)$. Furthermore, this $\mathbb{T}_0(N)$ is reduced.[12] Hence, there is an embedding

$$\mathbb{T}_0(N) \hookrightarrow \prod_{\min\ \mathfrak{p} \subset \mathbb{T}_0(N)} \mathbb{T}_0(N)/\mathfrak{p},$$

where each $\mathbb{T}_0(N)/\mathfrak{p}$ above is a characteristic zero domain which is finite over $\mathbb{Z}$ (so an order in some number field). ◦

Fix a prime ℓ, and let $\mathbb{T}_\ell := \mathbb{T}_0(N) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$, so $\mathbb{T}_\ell$ is a finite, free reduced $\mathbb{Q}_\ell$-algebra.

Fact (Compare [The, Proposition 2.5, Lecture 8])**.** Prime ideals of $\mathbb{T}_\ell$ are in bijection with Galois orbits of normalized newforms in $S_2(N, \overline{\mathbb{Q}}_\ell)$.

Thus, to each prime $\mathfrak{p} \subset \mathbb{T}_\ell$, one can associate a modular representation (the one associated to any of the corresponding newforms)

$$\rho_{\mathfrak{p}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{T}_\ell/\mathfrak{p}).$$

Taking a product over all such $\mathfrak{p}$ gives a representation landing $\prod_{\mathfrak{p}} \mathrm{GL}_2(\mathbb{T}_\ell/\mathfrak{p})$. One can show (See e.g. [The, Theorem 3.1, Lecture 8]) that this representation really lands in $\mathrm{GL}_2(\mathbb{T}_\ell)$ (note that $\mathbb{T}_\ell \hookrightarrow \prod \mathbb{T}_\ell/\mathfrak{p}$ since it is reduced), and so it produces our desired representation

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{T}_\ell).$$

[12] Pretend I realized $\mathbb{T}_0(N)$ as a ring of endomorphisms for $S_2(N, \mathbb{Z}[1/N])$ instead. For the usual Petersson inner product, it acts by normal [DS05, Theorem 5.5.3] and commuting operators, so $S_2(N, \mathbb{C})$ has a basis of simultaneous eigenvectors for $\mathbb{T}_0(N)$ (some elements of this basis will be oldforms, and so won't be eigenvectors for $\mathbb{T}(N)$. This is why this argument won't proved reducedness for $\mathbb{T}(N)$, but I'm getting ahead of myself...). Any $T \in \mathbb{T}_0(N)$ is trivial iff it acts trivially on this basis, so one gets an injection $\mathbb{T}_0(N) \hookrightarrow \prod \mathbb{C}$ by taking the eigenvalue of $T \in \mathbb{T}_0(N)$ on each element of this basis.

Remark 3.18. I believe (but am not sure I could actually prove) that the above representation is really the action of $G_{\mathbb{Q}}$ on the ℓ-adic Tate module $V_\ell(J_1(N)) = T_\ell(J_1(N)) \otimes \mathbb{Q}$ (note that $\mathbb{T}_\ell$ acts Galois-equivariantly on $V_\ell(J_1(N))$ since its action on $J_1(N)$ is defined over $\mathbb{Q}$). This is why I chose to realize these Hecke algebras in the endomorphism ring of $J_1(N)$ instead of in the endomorphism ring of $S_2(N, \mathbb{Z}[1/N])$. $\circ$

I'll leave elucidating the relevant properties of this representation for another talk, but suffice it to say that if one sets up an appropriate global Galois deformation problem $\mathcal{S}$, then this representations produces a map

$$R_{\mathcal{S}}^{\text{univ}} \longrightarrow \mathbb{T}_\ell$$

from the corresponding universal lifting ring. It seems it is usually not supposed to be too hard to check that this map is a surjection. The goal of an $(R = \mathbb{T})$-theorem is to show that it is an isomorphism.

Warning 3.19. Really, $\mathbb{T}_\ell$ is the wrong ring to consider. The deformation ring $R_{\mathcal{S}}^{\text{univ}}$ one sets up will be deformations of some fixed modular representation. This modular representation comes some eigenform over $\overline{\mathbb{F}}_\ell$ (i.e. some map $\mathbb{T}_0(N) \to \overline{\mathbb{F}}_\ell$, i.e. some maximal ideal of $\mathbb{T}_0(N)$ over $(\ell) \subset \mathbb{Z}$, i.e. some maximal ideal of $\mathbb{T}_0(N) \otimes \mathbb{Z}_\ell$). Thus, the correct ring to consider is really $\mathbb{T}_{\mathfrak{m}} :=$ the completion of the localization of $\mathbb{T}_0(N) \otimes \mathbb{Z}_\ell$ at the maximal ideal $\mathfrak{m}$ corresponding to the residual representation under consideration. You end up building $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_{\mathfrak{m}})$ not from all (Galois orbits of) normalized newforms, but only from those whose associated residual representation is isomorphic to the one you care about (the one attached to $\mathfrak{m}$). $\bullet$

Appendices

A Applicability of Theorem 3 to elliptic curves

TODO: Write this section

In brief,

- The condition that $p > 3$ is sad for us. We want $p = 3$ so we can apply the theorem to $\overline{\rho}_{E,3}$ (which is known to be modular by Langlands-Tunnell)
- Condition **(2)** is essentially asking for good reduction at all places above p. In the setting of Frey curves, these means it'd mainly be applicable to Fermat triples (a, b, c) such that $3 \nmid abc$.
- Condition **(3)** is no big deal; for Fermat, we only care about $F = \mathbb{Q}$ anyways.
- Say something about Hodge-Tate weights....

References

[BÏ3] Gebhard Böckle. Deformations of Galois representations. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 21–115. Birkhäuser/Springer, Basel, 2013. 3, 5, 8

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. *Publ. Math. Inst. Hautes Études Sci.*, (108):1–181, 2008. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras. 3

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem*. Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995. 2

[DDT07] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. `https://www.math.mcgill.ca/darmon/pub/Articles/Expository/05.DDT/paper.pdf`, Sept 2007. 8, 14

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. 14, 17

[Gee22] Toby Gee. Modularity lifting theorems. *Essential Number Theory*, 1(1):73–126, oct 2022. 3, 10, 11, 12, 14

[Gro90] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990. 14, 16

[The] Stanford Number Theorists. Stanford modularity lifting seminar. `http://virtualmath1.stanford.edu/~conrad/modseminar/`. 14, 17

[Zho] Rong Zhou. Modularity lifting theorems. `https://users.math.yale.edu/~rz289/Galois_reps.pdf`. 3, 7

Index