NOTES FROM MODULARITY LIFTING SEMINAR AT STANFORD, 2009-2010

SAM LICHTENSTEIN

Lecture 1: Overview by Brian

0. Why Study Galois Representations? Here we discuss the link between analytic L-functions and L-functions attached to varieties.

Let F be a number field and X a smooth projective variety over F.

Define the **partial Euler product**

$$\zeta_X^*(s) = \prod_{v \text{ good place of } F} \zeta(X \bmod v, q_v^{-s}), \qquad \operatorname{Re} s \gg_{\dim X} 0.$$

Here $X \bmod v$ denotes the smooth projective variety over $k(v) \simeq \mathbb{F}_{q_v}$ obtained by reduction of a smooth proper model of X over the valuation ring of F_v.

Example. Let X be an elliptic curve over F. Then

$$\zeta_E^*(s) = \prod_{E \text{ has good reduction at } v} \frac{1 - a_v q_v^{-s} + q_v^{1-2s}}{(1-q_v^{-s})(1-q_v^{1-s})} = \zeta^* F(s) \zeta_F^*(s-1) L^*(E,s)^{-1}, \qquad a_v = q_v + 1 - \#E(k(v)).$$

We would like to do the following.

(1) Fill in the "bad" factors to obtain an L-function with a good functional equation, analytic continuation, etc.
(2) Relate ζ_X^* to arithmetic properties of X. (E.g., Birch-Swinnerton-Dyer conjecture, etc.)

A clue for (1) comes from **Artin representations**:

$$\begin{array}{ccc} G_F = \operatorname{Gal}(\overline{F}/F) & \xrightarrow{\quad\rho\quad} & \operatorname{GL}(W) = \text{f.d. v.s.}/\mathbb{C} \\ & \searrow \qquad \nearrow & \\ & \operatorname{Gal}(F'/F) = \text{Gal. gp. of finite Gal. extn.} & \end{array}$$

Note that F'/F is unramified at all but finitely many places. We define the **Artin L-function** of ρ to be

$$L(s,\rho) = \prod_v \det([1 - \rho(\mathrm{Frob}_v) q_v^{-s}]|_{W^{I_v}})^{-1}, \qquad W^{I_v} = \text{subspace of } W \text{ fixed by inertia at } v.$$

Grothendieck gave a related description of ζ_X^* using *continuous* p-adic representations

$$G_F \to \operatorname{GL}(\mathrm{H}^i_{\text{ét},c}(X_{\overline{F}}, \mathbb{Q}_p)) =: \operatorname{GL}(W^i).$$

These are unramified almost everywhere, including at all good places away from p. Here the ith cohomology group W^i above vanishes for $i > 2\dim X$. Grothendieck proved that if we remove the contribution of p-adic places to $\zeta_X^*(s)$ then

$$\zeta_X^*(s) = \prod_i L^*(s, W^i)^{(-1)^i},$$

where $L^*(s,W^i)$ is like the Artin L-function without the "bad" factors and the p-adic places:

$$L^*(s, W^i) = \prod_{\text{good } v \nmid p} \det([1 - \mathrm{Frob}_v\, q_v^{-s}]|_{W^i})^{-1}.$$

Note: The expression for $L^*(s,W^i)$ requires some care, since q_v^{-s} is a *complex number* acting on a *p-adic* vector space. What has to be proved is that the characteristic polynomial for the action of Frob_v on W^i has rational coefficients (and is independent of p), so evaluation using q_v^{-s} makes sense (and the Riemann

Hypothesis ensures absolute convergence of the product in a suitable right half-plane depending only in $\dim X$).

We conclude from all this that it is a good idea to study L-functions of reasonable p-adic representations. Representation theory can often be used to fill in the bad factors later.

Eternal dangerous bend: The case of $v|p$ is tricky! The complication is that "unramifiedness" is not the right notion corresponding to "good reduction" for p-adic representations of Galois groups of p-adic fields.

1. Modular Galois representations and modularity lifting theorems.

Definitions.

Definition. A ***p*-adic representation** of G_F is a continuous linear representation $\rho : G_F \to \mathrm{GL}(W)$, where W is a finite dimensional vector space over a p-adic field K (i.e. a finite extension $K/\mathbb{Q}_p$) and ρ is unramified at almost all places v of F.

Example. The repsentation $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ arising from the Tate module of an elliptic curve E over F is historically the first really interesting example.

Example. Étale cohomology, with compact support: $W^i = \mathrm{H}^i_{\text{ét},c}(X_{\overline{F}}, \mathbb{Q}_p)$ for any separated F-scheme X of finite type. (Note that this is unramified at all but finitely many places, even if X is not smooth. The proof rests on properties of constructible ℓ-adic sheaves.)

Remark. In the definition of a p-adic representation it is *equivalent* to take the coefficient field to be $\overline{\mathbb{Q}}_p$, because of the following fact: any compact subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ is contained in $\mathrm{GL}_n(K)$ for a finite extension $K/\mathbb{Q}_p$. The proof of this uses the Baire Category Theorem. [Warning! It is *false* if we consider $\mathbb{C}_p$ instead of $\overline{\mathbb{Q}}_p$!] So we *could* do everything over $\overline{\mathbb{Q}}_p$, but we will find it more convenient to take the coefficient field K to be locally compact.

Definition. A $\bmod p$ **representation** of G_F is a continuous representation $\overline{\rho} : G_F \to \mathrm{GL}(\overline{W})$, where $\overline{W}$ is a finite dimensional vector space over a finite extension $k/\mathbb{F}_p$. Note that $\mathrm{GL}(\overline{W})$ is thus a discrete topological group, so the continuity condition entails that $\overline{\rho}$ factors through a finite Galois group $\mathrm{Gal}(F'/F)$.

Example. The p-torsion of an elliptic curve: $E[p](\overline{F}) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^r}$.

Example. Étale cohomology: $\mathrm{H}^i_{\text{ét},c}(X_{\overline{F}}, \mathbb{Z}/p\mathbb{Z})$.

Remark. It is "equivalent" to take the coefficient field to be $\overline{\mathbb{F}}_p$.

Reduction of Galois representations.

Proposition. Any p-adic representation $\rho : G_F \to \mathrm{GL}_K(W)$ has a G_F-stable $\mathcal{O}_K$-lattice $\Lambda \subset W$; i.e. ρ induces a map $\overline{\rho} : G_F \to \mathrm{GL}_{\mathcal{O}_K} \Lambda \approx \mathrm{GL}_n(\mathcal{O}_K) \twoheadrightarrow \mathrm{GL}_n(k)$ where $k = \mathcal{O}_K/\mathfrak{m}$. □

(Here by a **lattice** we mean a finitely generated $\mathcal{O}_K$-submodule of W such that $K \otimes_{\mathcal{O}_K} \Lambda = W$.) It is not hard to see that the characteristic polynomial of $\overline{\rho}$ is independent of the choice of lattice Λ.

Theorem (Cor. of Brauer-Nesbit Theorem). *Let $\overline{\rho}^{ss} = \bigoplus\{\text{Jordan-Holder factors of } \overline{\rho}\}$. Then $\overline{\rho}^{ss}$ has the same characteristic polynomial as $\overline{\rho}$, and is determined up to isomorphism by its characteristic polynomial, and is therefore independent of the choice of Λ.*

In light of the theorem, we shall henceforce call $\overline{\rho}^{ss}$ "the" reduction of ρ. Here are a bunch of things to watch out for:

1. $\overline{\rho}^{ss}$ is often denoted $\overline{\rho}$, even though it is certainly not just the "reduction mod p" of ρ in general.
2. $\overline{\rho}^{ss}$ may be unramified at some places where ρ is ramifield. For example, if $\rho(I_v) \subset 1 + \mathfrak{m} \cdot \mathrm{Mat}_n \mathcal{O}_K$, then the inertia at v simply "disappears" mod v.
3. If $\overline{\rho}^{ss}$ is irreducible, then in fact the only stable lattices in W were of the form $\pi^i \Lambda$, where π is a uniformizer for K and $i \in \mathbb{Z}$.
4. Irreducibility is *not* the same as *absolute* irreducibility = irreducibility over $\overline{k}$.
5. ρ might be absolutely irreducible over K, yet $\overline{\rho}^{ss}$ could be not only reducible, but even completely trivial! (Hence completely reducible...)

Exercise: If ρ is reducible then any Jordan-Holder filtration of ρ induces a similar filtration for $\overline{\rho}^{ss}$. So the last warning above is "one-directional".

Modular Galois representations. Let $f \in S_k(\Gamma_1(N), \chi)$ be a Hecke eigenform of weight $k \geq 1$. Let $K_f \subset \mathbb{C}$ be the field generated over $\mathbb{Q}$ by all the Fourier coefficients $a_\ell(f)$ of f for primes $\ell \nmid N$. Then K_f is a number field containing the values of the Nebentypus χ. Let λ be a place of K_f lying over p.

Theorem (Deligne, Deligne-Serre, Ribet)**.** *There exists a unique continuous irreducible p-adic representaion*

$$\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(K_{f,\lambda})$$

unramified at all $\ell \nmid Np$, such that for all such ℓ we have

$$\textit{sum of eigenvalues of } \mathrm{Frob}_\ell = \mathrm{Tr}(\rho_{f,\lambda}\,\mathrm{Frob}_\ell) = a_\ell(f)[= T(\ell)\textit{-eigenvalue of } f]$$

and

$$\det \circ \rho_{f,\lambda} = \chi \cdot \epsilon_p^{k-1}$$

where $\epsilon_p : G_\mathbb{Q} \to \mathbb{Z}_p^\times \subset \mathcal{O}_{K_f,\lambda}^\times$ is the p-adic cyclotomic character.

In particular, for $\ell \nmid Np$, the characteristic polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_\ell)$ is

$$t^2 - a_\ell(f)t + \chi(\ell)\ell^{k-1} \in K_f[t] \subset K_{f,\lambda}[t],$$

a non-obvious integrality property. Note that this polynomial is independent of λ.

Remark. The independence of λ and the precise control on the unramified primes implies that the collection $\{\rho_{f,\lambda}\}_\lambda$ is a "compatible" family of of representations, with respect to K_f-characteristic polynomials, just like $\{V_pE\}_p$ is a "compatible" family of represention with respect to $\mathbb{Q}$-characteristic polynomials. Cf. Serre's book *Abelian ℓ-adic representations.*

Let us look at the partial Artin L-functions

$$L^*(s, \rho_{f,\lambda}) = \prod_{\ell \nmid Np} \det\left(1 - \rho_{f,\lambda}(\mathrm{Frob}_\ell) \cdot \ell^{-s}\right)^{-1} = \prod_{\ell \nmid Np} \frac{1}{1 - a_\ell(f)\ell^{-s} + \chi(\ell)\ell^{k-1-2s}} =: L^*(s, f).$$

Remark. Note that for a complex conjugation c, $\det \rho_{f,\lambda}(c) = \chi(-1)\epsilon_p^{k-1} = (-1)^k(-1)^{k-1} = -1$, so all the representations produced by the theorem above are *odd*!

Now consider the (semisimplified) reduction $\overline{\rho}_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(k_{f,\lambda})$, which is continuous and semisimple, but might be reducible. In general, we say a mod-p representation $\overline{\rho}$ **is modular** if it is isomorphic over $\overline{\mathbb{F}}_p$ to some $\overline{\rho}_{f,\lambda}$.

Just *suppose* $\overline{\rho}_{f,\lambda}$ happens to be absolutely irreducible. By the last remark, it, too, is odd. Serre's conjecture is concerned with when mod-p representations with such properties are in fact modular.

Note that $\overline{\rho}_{f,\lambda}$ does not determine k or N. There could be congruences "$g \equiv f$" modulo λ for some eigenform $g \in S_{k'}(\Gamma_1(N'), \chi')$ (with the congruence taken in the sense of Fourier coefficients, say, relative to a p-adic place of $\overline{\mathbb{Q}}$ over λ on K_f and some chosen p-adic place of K_g). This would imply that $\overline{\rho}_{f,\lambda} = \overline{\rho}_{g,\lambda}$. This is actually abusive notation, since to obtain such a comparison, we might need to extend scalars on the residue fields of these reductions.

Wiles's insight. The prototype of a **modularity lifting theorem** is the following.

Theorem (Not really a theorem)**.** *Given any p-adic representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ such that $\overline{\rho}$ is irreducible and modular over $\overline{\mathbb{F}}_p$, and ρ is "nice" (at p, in the sense of p-adic Hodge theory!) then ρ is modular.*

In this seminar, we'll focus on those ρ such that

$$\rho|_{D_p} \approx \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$$

where D_p is the decomposition group at p, ψ_2 is an unramified character, and ψ_1 is ϵ_p^{k-1} times an unramified character. These representations are "essentially like the ones that come from elliptic curves with good ordinary reduction at p".

3. Applications of the method.

- Serre's conjecture.
- Sato-Tate.
- Gross-Zagier, Heegner points, Kolyvagin (need to provide a finite map $X_0(N_E) \to E$ over $\mathbb{Q}$, which is done via Faltings' theorem and the "modularity" of $V_\ell(E)$).
- FLT. (Modularity of the Galois rep. attached to the Frey curve.)

Lecture 2: Akshay on Serre's Conjecture, Etc.

Fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, and let k denote a finite subfield of the residue field of $\overline{\mathbb{Q}}_p$.

1. Serre's conjecture. Here's the conjecture:

Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be irreducible and odd. Then there exists a newform f whose Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ satisfies $\overline{\rho}_f \cong \overline{\rho}$. (Here $\overline{\rho}_f$ always means semisimplication!) Moreover f is of level $N(\overline{\rho})$ and weight $k(\overline{\rho})$ to be discussed below.

Remark. Apropos of reduction mod p: If V is a $\mathbb{Q}_p$-vector space and $G \subset \mathrm{GL}(V)$ is a compact subgroup, then there exists a G-fixed lattice in V for the following reason. Pick any lattice $L \subset V$. Then the G-stabilizer of L is open and of finite index. So $\Lambda = \sum_{g \in G} gL \subset V$ is also a lattice, and it is definitely G-stable. The same works with coefficients in any finite extension of $\mathbb{Q}_p$, or even in $\overline{\mathbb{Q}}_p$ (since we saw last time that in this latter case the image is contained in $\mathrm{GL}_n(K)$ for some subfield K of finite degree over $\mathbb{Q}_p$.

The level $N(\overline{\rho})$. Serre conjectured that $N(\overline{\rho}) =$ Artin conductor of $\overline{\rho}$, which has the following properties.

- $(p, N(\overline{\rho})) = 1$.
- For $\ell \neq p$, the ℓ-adic valuation $\mathrm{ord}_\ell N(\overline{\rho})$ depends only on $\overline{\rho}|_{I_\ell}$, and is given by
$$\mathrm{ord}_\ell N(\overline{\rho}) = \sum_{j \geq 0} \frac{1}{[G_0 : G_j]} \dim(V/V^{G_j})$$
Here, we set $K = \overline{\mathbb{Q}}^{\ker \overline{\rho}}$ to be the the field cut out by $\overline{\rho}$, and G_j to be image under $\overline{\rho}$ of the lower-numbered ramification filtration at ℓ of $\mathrm{Gal}(K/\mathbb{Q})$. In other words, if w is a place of K over ℓ, then
$$G_j = \overline{\rho}\{\sigma \in I_\ell \mid \mathrm{ord}_w(\sigma x - x) > j, \forall x \in \mathcal{O}_{K,w}\}.$$
The filtration goes
$$G_0 = \overline{\rho}(I_\ell) \supset G_1 \supset G_2 \supset \cdots$$
The first step is of index prime to ℓ, while the latter groups are all ℓ-groups. If K is tamely ramified or unramified at ℓ, then $\mathrm{ord}_\ell N(\overline{\rho}) = \dim(V/V^{I_\ell})$. The Hasse–Arf theorem ensures that the proposed formula for the ℓ-adic ordinal above is actually an integer.

The weight $k(\overline{\rho})$.

Theorem (Deligne)**.** *Suppose f is a newform of weight $< p$ and level prime to p (so χ_f is unramified at p). Suppose f is **ordinary** at p, meaning $a_p(f) \in \overline{\mathbb{Z}}_p^\times$. Then $\overline{\rho}_f$ has a unique 1-dimensional **unramified** quotient; i.e.*
$$\overline{\rho}_f|_{D_p} \sim \begin{pmatrix} \alpha\omega^{k-1} & * \\ 0 & \beta \end{pmatrix}$$
*for **unramified** characters $\alpha, \beta : D_p \to \overline{\mathbb{F}}_p^\times$ and ω the mod-p cyclotomic character.*

It follows that
$$\overline{\rho}_f|_{I_p} \sim \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$
This can be seen concretely in the case of elliptic curves E with ordinary reduction: for $\rho_f = V_\ell(E)$ the "connected-étale sequence"
$$\mathcal{E}[p^n]^0 \to \mathcal{E}[p^n] \to \mathcal{E}[p^n]/\mathcal{E}[p^n]^0$$
associated to the p^n-torsion on the Néron model $\mathcal{E}$ has last quotient is unramified. Now take limits on generic fibers to deduce the theorem in this case.

Serre conjectured that
$$k(\overline{\rho}) := \begin{cases} 1 + pa + b & \text{"most of the time"} \\ 1 + pa + b + p - 1 & \ldots \end{cases}$$
is the minimal weight at prime-to-p level. Here $a \leq b$ are integers to be defined below. In the ordinary, low ($< p$) weight case, $a = 0, b = k - 1$.

We need to detour into the structure of $I = I_p \subset G_{\mathbb{Q}}$. By definition $I_w \lhd I \twoheadrightarrow I_t$, where I_w, the wild ramification group, is the largest pro-p subgroup.

Proposition. $I_t \cong \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \overline{\mathbb{F}}_p^{\times}) = \varprojlim_r \mathbb{F}_{p^r}^{\times} = \prod_{\ell \neq p} \mathbb{Z}_\ell(1)$. □

Think: $\widehat{\mathbb{Z}}$ minus the p-part. The Tate-twisting notation records how the canonical Frobenius element in D_p/I_p acts on the abelian quotient I_t of I_p. The map from left to right is $g \mapsto g(\theta_r)/\theta_r$ where $\theta_r^{p-1} = p$. The action of $\mathrm{Frob}_p \in D_p/I_p$ is by raising to the pth power on the right side. The composite quotient map

$$\psi_r : I_t \twoheadrightarrow \mathbb{F}_{p^r}^{\times}$$

is called the *level-r fundamental character*, though the more canonical collection is its p-powers (thereby being "independent of the choice of $\overline{\mathbb{F}}_p$").

We can deduce that

$$(\overline{\rho}|_{I_p})^{\mathrm{ss}} \cong \left(\begin{smallmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{smallmatrix}\right).$$

To see this, note that $\overline{\rho}$ is assumed irreducible. On one hand I_w is pro-p, so by a counting argument it must fix a nontrivial subspace when acting on a vector space over a finite field of characeristic p. On the other hand I_p/I_w is abelian, so it has no irreducible 2-dimensional representations. Hence $\overline{\rho}_{I_p}$ is not itself irreducible; i.e. it is upper triangular, so its semisimplification splits as a direct sum of characters.

Now since $\overline{\rho}|_{I_p}$ extends to a representation of D_p, the pair $\{\chi_1, \chi_2\}$ must be preserved under the Frobenius action of D_p/I_p. In other words, we have

$$\begin{cases} \chi_1^p = \chi_1 \\ \chi_2^p = \chi_2 \end{cases} \qquad \text{or} \qquad \begin{cases} \chi_1^p = \chi_2 & \chi_1^{p^2} = \chi_1 \\ \chi_2^p = \chi_1 & \chi_2^{p^2} = \chi_1 \end{cases}$$

In the first case, each, χ_i factors through $I_t \to \mathbb{F}_p^{\times}$. In the second case, each χ_i factors through $I_t \to \mathbb{F}_{p^2}^{\times}$.

So in the first case we can write $\chi_1 = \omega^a, \chi_2 = \omega^b$ for $0 \le a \le b$, where $\omega : I_t \to \varprojlim \mathbb{F}_{p^r}^{\times} \twoheadrightarrow \mathbb{F}_p^{\times}$ is the mod-p cyclotomic character. In the second case we can likewise write $\chi_1 = \psi^{a+pb}$, $\chi_2 = \psi^{pa+b}$ where $\psi : I_t \to \mathbb{F}_{p^2}^{\times}$ is the level-2 fundamental character. These are the a, b in Serre's conjecture.

The exceptional case $k(\overline{\rho}) = 1 + pa + b + p - 1$. Now we address where this case comes from (but without precisely defining it). Consider the special cases

$$\overline{\rho}|_{I_p} \sim \left(\begin{smallmatrix} \omega^2 & * \\ 0 & 1 \end{smallmatrix}\right)$$

and

$$\overline{\rho}|_{I_p} \sim \left(\begin{smallmatrix} \omega & * \\ 0 & 1 \end{smallmatrix}\right).$$

In the first case the guess is $k(\overline{\rho}) = 3$. In the second case the "standard" guess $(a = 0, b = 1)$ is $k(\overline{\rho}) = 2$. But a naive combinatorial estimate says that the number of representations of the second type is roughly twice as much as the number of the first type. On the other hand these are certainly fewer modular forms of weight 2 than of weight 3. The "corrected" guess of $p+1$ for the second case when $a = 0$ and $b = 1$ could provide the necessary extra modular representations.

Note: $\overline{\rho}|_{D_p}$ "comes from" a finite flat group scheme over $\mathbb{Z}_p$ if it arises in weight 2; this property depends only on the restriction to inertia, and it can be characterized in purely Galois-theoretic terms. This leads to a special case in Serre's conjecture related to the case $k(\overline{\rho}) = 2$.

Emerton on Serre's conjecture. Matt Emerton has a version of "mod p local Langlands" which gives the following picture. There is a natural action of $\mathrm{GL}_2(\mathbb{A}_f)$ (with $\mathbb{A}_f$ the finite adeles) on

$$\mathrm{Hom}_{G_{\mathbb{Q}}}(\overline{\rho}, \varinjlim_N \mathrm{H}^1(X(N), \overline{\mathbb{F}}_p)) \cong {\bigotimes_q}' \pi_q(\overline{\rho}),$$

where the right side is a "factorization" into local "mod p automorphic" representations. Here $\pi_q(\overline{\rho})$ is finite length but not necessarily irreducible, and depends only on $\overline{\rho}|_{D_q}$. Supose $\overline{\rho} = \overline{\rho}_f$ for $f \in S_k^{\mathrm{new}}(N)$. Then in fact

$$\overline{\rho} \hookrightarrow \mathrm{H}^1(X(N), \mathrm{Sym}^{k-2}\, \overline{\mathbb{F}}_p^2).$$

Here $\mathrm{Sym}^{k-2}\, \overline{\mathbb{F}}_p^2$ is viewed as a local system on $X(N)$ as the Tate module of the "universal elliptic curve" (up to some subtleties at the cusps). The right side is almost the same as [*need to clarify appearance of*

$\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$*-invariants below*]

$$(\mathrm{H}^1(X(N(\rho)), \overline{\mathbb{F}}_p) \otimes \mathrm{Sym}^{k-2}\, \overline{\mathbb{F}}_p^2)^{\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})} = ((\bigotimes{}' \pi_q(\overline{\rho}))^{k(Np)} \otimes \mathrm{Sym}^{k-2}\, \overline{\mathbb{F}}_p^2)^{\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})} \neq 0$$

[*This needs to be extended a bit more to explain the relation with "independence" of the N and the k in Serre's conjecture.*]

2. Hecke algebras. Let $V = S_2(\Gamma_0(N))$ for N squarefree. Let $\mathbb{T} \subset \mathrm{End}(V)$ be the $\mathbb{Z}$-subalgebra generated by all Hecke operators $T(p), p \nmid N$ and $U_p, p|N$. (Recall that $U_p : \sum a_n q^n \mapsto \sum a_{np} q^n$.)

Fact: $\mathbb{T}$ is finite over $\mathbb{Z}$.

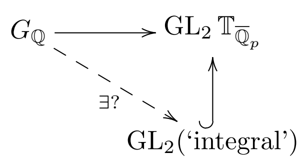
Proof. One approach is to show that $\mathbb{T}$ preserves a lattice in V, by using the arithmetic theory of modular curves (with models over $\mathbb{Z}$). An alternative which is easier to carry out rigorously and involves just topological/analytic tools is to embed V into $\mathrm{H}^1(X_0(N), \mathbb{C})$ and extend the $\mathbb{T}$-action to this space and prove it preserves the lattice of integral cohomology (which can also be studied in terms of group cohomology). This will be addressed in all weights ≥ 2 in Baran's later lecture. □

Fact: The natural map from $\mathbb{T}_{\mathbb{C}} := \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}$ onto the subalgebra $\mathbb{C}[T(p), U_p \mid p \in \mathbb{Z}] \subset \mathrm{End}(V)$ is an isomorphism; that is, $\mathbb{T}_{\mathbb{C}}$ acts faithfully on V. This will also be proved in Baran's lecture (in any weight at least 2).

Fact: V is a free $\mathbb{T}_{\mathbb{C}}$ module of rank 1.

Proof. It is enough to construct a cyclic vector f; i.e., $T \mapsto Tf$ gives a surjection $\mathbb{T}_{\mathbb{C}} \twoheadrightarrow V$. (It is automatically then injective since $\mathbb{T}$ acts faithfully on V.) By multiplicity 1, we have $V = \bigoplus_{\text{newforms } f_i} V_i$ where V_i is the generalized Hecke eigenspace corresponding to f_i. It suffices to check the existence of a cyclic vector for each V_i, due to the Chinese Remainder Theorem for coprime maximal ideals of $\mathbb{T}_{\mathbb{C}}$ (which corresponding to eigenforms). The existence of a cyclic vector for each V_i can be done explicitly. □

By the last fact, $\mathrm{H}^1(X_0(N), \mathbb{C}) \cong V \oplus \overline{V}$ is free of rank 2 over $\mathbb{T}_{\mathbb{C}}$. Consequently $\mathrm{H}^1(X_0(N), \overline{\mathbb{Q}}_p)$ is free of rank 2 over $\mathbb{T}_{\overline{\mathbb{Q}}_p}$. The latter is $\mathbb{T}_{\overline{\mathbb{Q}}_p}$-linearly isomorphic to $\mathrm{H}^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_p)$, which also has a $G_{\mathbb{Q}}$-action (that is Hecke equivariant, due to an alternative way to define the Hecke action via correspondences between modular curves over $\mathbb{Q}$). So we obtain a "modular" Galois representation:



We'd like to produce a $G_{\mathbb{Q}}$-stable $\mathbb{T}_{\overline{\mathbb{Z}}_p}$-lattice inside our rank 2 $\mathbb{T}_{\overline{\mathbb{Q}}_p}$ module. This approach gets involved with delicate commutative algebra properties of integral Hecke algebras (Gorenstein condition, etc.), and in more general settings it is simpler to bypass such subtleties at the outset. So we will use a slicker method with wider applicability which avoids making such a Hecke lattice.

Example. Consider level $N = 33$. Then $\dim(S_2) = 3$. The cusp forms in question come from two elliptic curves. The first $y^2 + y = x^3 \pm x^2$ has conductor 11, giving rise to

$$f = q \prod_n (1 - q^n)^2 (1 - q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 \pm 2q^6$$

of level 11, hence $f'(z) := f(3z)$ is level 33. The second $y^2 + xy = x^3 + x^2 - 11x$ gives rise to $g = q + q^2 + q^3 - q^4 - 2q^5 \pm 2q^6$ in level 33. Observe that $f \equiv g \bmod 3$, which is no accident. Indeed, the Hecke algebra $\mathbb{T}$ acting on the lattice $\mathbb{Z}f \oplus \mathbb{Z}f' \oplus \mathbb{Z}g$ in S_2 is generated over $\mathbb{Z}$ by U_3, which acts by

$$g \mapsto -g, f' \mapsto f, f \mapsto -f - 3f'.$$

From this we can find

$$\mathbb{T} \cong \mathbb{Z}[x]/(x+1)(x^2 + x + 3).$$

So $\mathrm{Spec}\, \mathbb{T}$ lying over $\mathrm{Spec}\, \mathbb{Z}$ has two irreducible components,

$$\mathrm{Spec}\, \mathbb{Z} = \mathrm{Spec}\, \mathbb{Z}[x]/(x+1), \ \ \mathrm{Spec}\, \mathbb{Z}[x]/(x^2 + x + 3),$$

which happen to meet at the fiber over $(3) \in \operatorname{Spec} \mathbb{Z}$. (This is precisely the reason for the congruence observed earlier, as we will see in a moment.) The fiber in question consists of a single maximal ideal $\mathfrak{m} \in \operatorname{Spec} \mathbb{T}$, the kernel of

$$\mathbb{T} \overset{\text{act on } \mathbb{Z}f}{\to} \mathbb{Z} \twoheadrightarrow \mathbb{F}_3.$$

If we consider the completed localization $\mathbb{T}_{\mathfrak{m}}$ then we claim that after a suitable conjugation, $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_{\overline{\mathbb{Q}}_3})$ factors through $\mathrm{GL}_2(\mathbb{T}_{\mathfrak{m}})$. Once this is done, then using the two specializations $\mathbb{T}_{\mathfrak{m}} \to \mathbb{Z}_3$ corresponding to the two elliptic curves then recovers the 3-adic Tate modules of these elliptic curves as deformations of a common mod-3 residual representation.

But how to make the representation land in $\mathrm{GL}_2(\mathbb{T}_{\mathfrak{m}})$? Consider the 3-adic eigenforms associated to minimal primes of $\mathbb{T}$ below $\mathfrak{m}$, of which there are 2 and so actually the ones from the elliptic curves above (for a unique prime over 3 in the quadratic field associated to the second component of $\mathbb{T}$). This gives representations from $G_{\mathbb{Q}}$ into $\mathrm{GL}_2(\mathbb{Z}_3)$ which are conjugate modulo 3. One checks that these mod-3 representations are irreducible, and hence absolutely irreducible (due to oddness). Thus, the *local* fiber product ring

$$R = \mathbb{Z}_3 \times_{\mathbb{F}_3} \mathbb{Z}_3 = \{(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \mid a \equiv b \bmod 3\}$$

contains $S = \mathbb{T}_{\mathfrak{m}}$ and we get a representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ upon fixing an isomorphism of the mod-3 reductions. Note that the traces in R at Frobenius elements away from 3 and 11 all lie in S, since $T_\ell \in \mathbb{T}$ "is" the trace (as can be checked modulo each minimal prime of the reduced $\mathbb{T}_{\mathbb{Q}_3}$). This is the key to descending the representation into $\mathrm{GL}_2(S)$, as we explain next.

3. Descent for Galois representations. Let R be a complete local ring with maximal ideal $\mathfrak{m}_R$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(R)$ be residually absolutely irreducible and continuous. Suppose further more that ρ is odd. Let S be a complete local subring of R with local inclusion map, so $\mathfrak{m}_S = \mathfrak{m}_R \cap S$ and we get an induced isomorphism of residue fields $S/\mathfrak{m}_S \cong R/\mathfrak{m}_R$. Assume that $\operatorname{tr} \rho(g) \in S$ for all $g \in G_{\mathbb{Q}}$.

Theorem. *If $n = 2$ and the residue characteristic is not 2 then some $\mathrm{GL}_2(R)$-conjugate of ρ is valued in $\mathrm{GL}_2(S)$.*

Proof. The argument is elementary, and apparently due to Wiles. By oddness, we can assume $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \operatorname{im} \rho$. For any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \operatorname{im} \rho$, the trace $2a = \operatorname{tr}(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right))$ lies in S, so $a \in S$. Similarly one finds $d \in S$. By residual irreducibility there is $g \in G_{\mathbb{Q}}$ with $\rho(g) \sim \left(\begin{smallmatrix} * & u \\ & * \end{smallmatrix}\right)$ where u is an R-unit. Conjugate by $\left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and we find that $\rho(g) \sim \left(\begin{smallmatrix} * & 1 \\ * & * \end{smallmatrix}\right)$ for some g. Messing around with this and the previous idea, one can conclude that $b, c \in S$ as well. □

Note that the preceding argument did not use the completeness of S. Now we use it. [*Where do we ever use completeness of R or S below?*] Taking S and R as above, and imposing no hypotheses on n or the residue characteristic, we have:

Theorem. *Assume $\rho : G \to \mathrm{GL}_n(R)$ is residually absolutely irreducible, where G is any group at all. Then some $\mathrm{GL}_n(R)$-conjugate of ρ is valued in $\mathrm{GL}_n(S)$.*

Proof. By Jacobson Density and the residual absolute irreducibility of ρ, there exist

$$x_1, \ldots, x_{n^2} \in \rho(G) \subset M_n(R)$$

such that $\overline{x}_i$ span $M_n(k)$, where $k = R/\mathfrak{m}_R$ is the residue field. It follows that the x_i's themselves freely span $M_n(R)$. (Relate them to a basis by a matrix; the reduction of that matrix mod $\mathfrak{m}_R$ is invertible over k, so it must be invertible over R itself.)

Let B be the S-submodule of $M_n(R)$ freely spanned over S by the x_i. It is free of rank n^2. The claim is that B is in fact an S-algebra containing $\rho(G)$. To see this, take $y \in \rho(G)$. We can write $y = \sum a_i x_i$ for $a_i \in R$. For each $1 \leq j \leq n^2$, the trace $\operatorname{tr}(y x_j)$ is equal to $\sum_i a_i \operatorname{tr}(x_i x_j)$. Consider the matrix

$$(\operatorname{tr}(x_i x_j)) \in M_{n^2} S.$$

Due to non-degeneracy of the trace pairing for matrix algebras over a field, a matrix of traces of products of basis elements for a matrix algebra over a field is invertible. So the reduction of this matrix mod $\mathfrak{m}_R$ (the same as its reduction mod $\mathfrak{m}_S$) is invertible. Hence it is invertible itself, so the a_i are in S and hence $y \in B$. Thus, $\rho(G) \subset B$. In particular $1 \in B$. It's not hard to check B is closed under multiplication, so it's a finite S-algebra that is free of rank n^2 and contains $M_n(S)$.

If k' denotes the residue field of S, then since the map $M_n(S) \to M_n(R)$ induces the injective map $M_n(k') \to M_n(k)$ modulo maximal ideals we conclude that the inclusion $M_n(S) \to B$ induces an injective map $M_n(k') \to B \otimes_S k'$. But $B \otimes_S k'$ has rank n^2, so $M_n(S) \to B$ is a map between finite free S-modules of rank n^2 and induces an isomorphism modulo $\mathfrak{m}_S$. Thus, it is an equality. □

4. Universal deformation ring. As before let k be a finite field and $\overline{\rho} : G \to \mathrm{GL}_n(k)$ an absolutely irreducible representation of a profinite group G. A **lifting** of $\overline{\rho}$ over a complete local Noetherian ring A with residue field k is a representations $\rho : G \to \mathrm{GL}_n(A)$ equipped with an isomorphism $\rho \otimes_A k \cong \overline{\rho}$. We will be especially interested in the case when $G = G_{\mathbb{Q},S}$, the Galois group of the largest extension of $\mathbb{Q}$ unramified outside of a fixed finite set of places S, or when G is the Galois group of a local (especially p-adic) field. These groups satisfy a certain finiteness property Φ_p: their open subgroups have only finitely many index-p open subgroups.

Claim. Assume that G satisfies Φ_p. There exists a complete local noetherian ring $R_{\overline{\rho}}$ and a deformation $\rho_{\text{univ}} : G_{\mathbb{Q},S} \to \mathrm{GL}_n(R_{\overline{\rho}})$ such that for any deformation (ρ_A, A) there exists a unique ring map $R_{\overline{\rho}} \to A$ such that ρ_A factors through ρ_{univ}, up to residually trivial conjugation. (Here the map $\mathrm{GL}_n(R_{\overline{\rho}}) \to \mathrm{GL}_n)(A)$ is induced by the map $R_{\overline{\rho}} \to A$.)

The proof of this will be explained next time by Mok.

Example. Let G be a finite group of order not divisible by p and consider $G \xrightarrow{\overline{\rho}} \mathrm{GL}_n(k)$ where the characteristic of k is p. Then $R_{\overline{\rho}} = W(k)$, the ring of Witt vectors for k. This will follow from the vanishing of p-torsion group cohomology for G and the computation of the "reduced" cotangent space to the deformation ring as in Mok's talk next time.

Example. Suppose $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ is odd, and $\mathrm{H}^2(G_{\mathbb{Q}}, \mathrm{Ad}^0(\overline{\rho})) = 0$. Then $R_{\overline{\rho}} = W(k)[\![X_1, X_2, X_3]\!]$. So generically, one expects the universal deformation ring to be 3-dimensional over $W(k)$.

5. Hecke algebras again. Let $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ be absolutely irreducible. Pick a level N. Let $f_1, \ldots, f_m$ be all the newforms of weight 2 and level dividing N, such that $\overline{\rho}_f \sim \overline{\rho} \otimes_k \overline{\mathbb{F}}_p$; we assume this set of f_i's is non-empty! Let f_i have coefficients contained in K_i, a number field with maximal order $\mathcal{O}_i$, and let $\mathcal{O}_{i,\lambda}$ be the completion of $\mathcal{O}_i$ in $\overline{\mathbb{Q}}_p$.

Let $\mathbb{T}$ be the $W(k)$-subalgebra of $\prod \mathcal{O}_i$ spanned by the images of all the $T(\ell)$ with $(\ell, Np) = 1$.

We have a map $\mathbb{T} \to \mathcal{O}_{i,\lambda} \to \overline{\mathbb{F}}_p$ sending $T(\ell)$ to $\operatorname{tr} \rho(\mathrm{Frob}_\ell)$, independent of i. Call the kernel $\mathfrak{m} \subset \mathbb{T}$, and let $\mathbb{T}_{\mathfrak{m}}$ be the completed localization. Thus, the representation

$$\prod \rho_{f_i} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\prod \mathcal{O}_{i,\lambda})$$

admits a conjugate valued in $\mathrm{GL}_2(\mathbb{T}_m)$, by using the same kind of argument carried out earlier with the elliptic curves of levels 11 and 33. Note that the residue field of $\mathbb{T}_{\mathfrak{m}}$ is equal to k.

By universality of $R_{\overline{\rho}}$ we obtain a local $W(k)$-algebra map $R_{\overline{\rho}} \twoheadrightarrow \mathbb{T}_{\mathfrak{m}}$ satisfying $\operatorname{tr} \rho \, \mathrm{Frob}_\ell \mapsto T(\ell)$, so this map is surjective. An $R = \mathbb{T}$ **theorem** says that this map identifies $\mathbb{T}_{\mathfrak{m}}$ with a certain quotient of $R_{\overline{\rho}}$ determined by local data. (In practice one needs some more flexibility, such as to include a Hecke operator at p, or to impose determinant conditions, to invert p before claiming to have an isomorphism, etc.)

Lecture 3. Mok on Deformations

Let G be a profinite group and $\overline{\rho} : G \to \mathrm{GL}_n(k)$ a representation defined over a finite field k of characteristic p. Let Λ be a complete discrete valuation ring with residue field k, e.g. $\Lambda = W(k)$. Let $\mathcal{C}_\Lambda$ be the category of artinian local Λ-algebras with residue field k, and local morphisms. Let $\widehat{\mathcal{C}}_\Lambda$ be the category of complete Noetherian local Λ-algebras with residue field k, i.e. the pro-category of $\mathcal{C}_\Lambda$.

1. Deformation functors. Define $\mathrm{Def}(\overline{\rho}) : \widehat{\mathcal{C}}_\Lambda \to \mathrm{Sets}$ by

$$\mathrm{Def}(\overline{\rho})(A) = \{(\rho, M, \iota)\}/\sim$$

where M is a free A-module of rank n, $\rho : G \to \mathrm{GL}_A(M)$ is a continuous representation, $\iota : \rho \otimes_A k \cong \overline{\rho}$ is an isomorphism, and two such triples are equivalent when the representations are isomorphic in a manner which respects the ι's. Define the **framed** deformation functor $\mathrm{Def}^\square(\overline{\rho})$ by

$$\mathrm{Def}^\square(\overline{\rho})(A) = \{(\rho, M, \iota, \beta)/\sim$$

where β is a basis for M lifting the standard basis for k^n under ι. Morally, $\mathrm{Def}^\square$ is the set of liftings of $\overline{\rho}$ into $\mathrm{GL}_n(A)$.

There is a forgetful functor $\mathrm{Def}^\square \to \mathrm{Def}$.

Equivalent definitions are

$$\mathrm{Def}^\square(\overline{\rho})(A) = \{\rho : G \to \mathrm{GL}_n A \,|\, \rho \bmod \mathfrak{m}_A = \overline{\rho}\},$$
$$\mathrm{Def}(\overline{\rho})(A) = \mathrm{Def}^\square(\overline{\rho})(A)/(\text{conjugation by } \Gamma_n(A) := \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(k))).$$

Note: it is easy to see that $\mathrm{Def}^\square(\overline{\rho})(A) = \varprojlim_i \mathrm{Def}^\square(\overline{\rho})(A/\mathfrak{m}_A^i)$. It is also true (but requires an argument) that $\mathrm{Def}(\overline{\rho})(A) = \varprojlim_i \mathrm{Def}(\overline{\rho})(A/\mathfrak{m}_A^i)$. In other words "we can compute these functors on the level of artinian quotients", so we just need to consider them on the category $\mathcal{C}_\Lambda$.

2. p-finiteness. We cannot hope to represent $\mathrm{Def}(\overline{\rho})$ or $\mathrm{Def}^\square(\overline{\rho})$ in $\widehat{\mathcal{C}}_\Lambda$ (which only contains Noetherian rings) unless G is "not too big".

Definition. We say G **satisfies the p-finiteness condition** if for every open subgroup $H \subset G$ of finite index, there are only finitely many continuous group homomorphisms $H \to \mathbb{Z}/p\mathbb{Z}$ (i.e., only finitely many open subgroups of index p). (This holds if and only if for any such H, the maximal pro-p quotient of H is topologically finitely generated.)

We are interested in two cases.

(1) $G = G_K$ for a local field K finite over $\mathbb{Q}_\ell$ (allowing $\ell = p$!).
(2) $G = G_{K,S}$ for a number field K and S a finite set of ramified primes.

In case (1), $H = G_{K'}$ for a finite extension K'/K, and the p-finiteness condition follows from the fact that the local field K' of characteristic 0 has only finitely many extensions of any given degree (such as degree p). For (2), H corresponds to some finite extension K'/K unramified outside of S, so the index-p open subgroups of H correspond to certain degree-p extensions of K' unramified away from the places of K' over S. Thus, the p-finiteness follows from the **Hermite-Minkowski theorem**, which says that only finitely many extensions of K of bounded degree unramified outside S.

Returning to the general situation, assume G satisfies p-finiteness. By *Schlessinger's criterion*, we will eventually see that $\mathrm{Def}^\square(\overline{\rho})$ is always representable in $\widehat{\mathcal{C}}_\Lambda$, so there exists a universal framed deformation ring $R^\square_{\overline{\rho}} \in \widehat{\mathcal{C}}_\Lambda$ and a universal framed deformation $\rho^\square_{\overline{\rho}}$ satisfying the natural universality property. We will also see that $\mathrm{Def}(\overline{\rho})$ is itself representable by a universal deformation ring $(R_{\overline{\rho}}, \rho_{\mathrm{univ}})$, at least when $\mathrm{End}_G(\overline{\rho}) = k$. This will be the case if $\overline{\rho}$ is absolutely irreducible, and also if $n = 2$ and $\overline{\rho}$ is a non-split extension of distinct characters.

3. Zariski tangent space to the deformation functors. Let $k[\epsilon]$ denote the ring of dual numbers of k. The **tangent space** to a functor $F : \widehat{\mathcal{C}}_\Lambda \to Sets$ is $F(k[\epsilon]) =: t_F$. Initially this is just a set; the hypotheses of Schlessinger's criterion give it a natural structure of k-vector space (compatibly with natural transformations in F).

Let $V \in \mathrm{Def}(\overline{\rho})(k[\epsilon]) = t_{\mathrm{Def}(\overline{\rho})}$. Then by definition there is given a specified isomorphism $V/\epsilon V \cong \overline{\rho}$, so we obtain an exact sequence

$$0 \to \epsilon V \to V \to \overline{\rho} \to 0.$$

But it is easy to see that ϵV is naturally $k[G]$-isomorphic to $\overline{\rho}$ as well. Hence we see

$$t_{\mathrm{Def}(\overline{\rho})} = \mathrm{Ext}^1_{k[G]}(\overline{\rho}, \overline{\rho}) = \mathrm{H}^1(G, \mathrm{Ad}(\overline{\rho}));$$

this respects the k-linear structure on both sides.

More explicitly, given $\rho \in \mathrm{Def}^{\square}(\overline{\rho})(k[\epsilon])$ we can write $\rho(g) = \overline{\rho}(g) + \epsilon\Phi(g)\overline{\rho}(g)$ for $\Phi(g) \in \mathrm{Ad}(\overline{\rho})$. One can compute that the condition that ρ is a group homomorphism is the 1-cocycle condition on Φ. So $t_{\mathrm{Def}^{\square}(\overline{\rho})} = Z^1(G, \mathrm{Ad}(\overline{\rho}))$. Similarly one checks that two framed deformations are conjugate under $\Gamma_0(k[\epsilon]) = I_n + \epsilon M_n(k)$ if and only if their associated cocycles differ by a 1-coboundary. We conclude that $t_{\mathrm{Def}(\overline{\rho})} = \mathrm{H}^1(G, \mathrm{Ad}(\overline{\rho}))$, and

$$\dim_k B^1(G, \mathrm{Ad}(\overline{\rho})) = \dim \mathrm{Ad}(\overline{\rho}) - \dim \mathrm{H}^0(G, \mathrm{Ad}(\overline{\rho}))$$

is the **number of framed variables**. The p-finiteness hypothesis says precisely that $\dim Z^1, \dim \mathrm{H}^1 < \infty$. If moreover $\mathrm{End}_G(\overline{\rho}) = k$ then $h^0(G, \mathrm{Ad}(\overline{\rho})) = 1$, and we are in the representable situation. The forgetful functor $\mathrm{Def}^{\square}(\overline{\rho}) \to \mathrm{Def}(\overline{\rho})$ induces a map $R_{\overline{\rho}} \to R^{\square}_{\overline{\rho}}$, which turns out to be formally smooth, and thus realizes $R^{\square}_{\overline{\rho}}$ as a ring of formal power series (in some number d of variables) over $R_{\overline{\rho}}$. The number d is precisely the number of framed variables, which in this case is $n^2 - 1$.

Concretely, what is going on is that if $\overline{\rho}$ has only scalar endomorphism (so likewise for any lifting of $\overline{\rho}$) and we consider the universal deformation $R_{\overline{\rho}}$ then to "universally" specify a basis which residually lifts the identity is precisely to applying conjugation by a residually trivial matrix which is unique up to a unit scaling factor. And we can eliminate the unit scaling ambiguity by demanding (as we always may in a unique way) that the upper left matrix entry is not merely a unit but is equal to 1. Thus, the framing amounts to specifying a "point" of the formal $R_{\overline{\rho}}$-group of PGL_n at the identity, which thereby proves the asserted description of the universal framed deformation ring in these cases as a formal power series ring over $R_{\overline{\rho}}$ in $n^2 - 1$ variables. To be explicit, over

$$R^{\square}(\overline{\rho}) = R(\overline{\rho})[\![Y_{i,j}]\!]_{1 \le i,j \le n, (i,j) \ne (1,1)}$$

the universal framed deformation is the lifting $\overline{\rho}_{\mathrm{univ}}$ equipped with the basis obtained from the standard one by applying the invertible matrix $1_n + (Y_{i,j})$ where $Y_{1,1} := 0$.

It must be stressed that we will later need to work with cases in which $\overline{\rho}$ is *trivial* (of dimension 2), so $R_{\overline{\rho}}$ does not generally exist. This is why the framed deformation ring is useful.

3. References.

- Mazur's articles in "Galois groups over $\mathbb{Q}$" and "Modular Forms and Fermat's Last Theorem".
- Kisin's notes from CMI summer school in Hawaii.

4. More on Zariski tangent spaces to deformation functors. From now on fix G to be either G_K for local K or $G_{K,S}$ for a number field K. Fix $\overline{\rho} : G \to \mathrm{GL}_n(k)$ and suppose the characteristic of the finite field k is p. If F is a deformation functor represented by $R \in \widehat{\mathcal{C}}_\Lambda$, recall that

$$F(A) = \mathrm{Hom}_{\Lambda\text{-alg}}(R, A), \qquad t_F = F(k[\epsilon]) = \mathrm{Hom}_{\Lambda\text{-alg}}(R, k[\epsilon]) = \mathrm{Hom}_{\Lambda\text{-alg}}(R/(\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda R), k[\epsilon]).$$

The last equality is because the Λ-algebra maps are *local* morphisms, so in particular they send $\mathfrak{m}_R$ to $\epsilon k[\epsilon]$, and hence $\mathfrak{m}_R^2$ to zero. But by general nonsense we have

$$R/(\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda R) = k \oplus \frac{\mathfrak{m}_R}{\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda R},$$

where the second summand is square zero. Thus we see

$$t_F = \mathrm{Hom}_k(\frac{\mathfrak{m}_R}{\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda R}, k) = t_R^*,$$

where for $A \in \widehat{\mathcal{C}}_\Lambda$ we define the **reduced Zariski cotangent space of** A to be

$$t_A^* = \frac{\mathfrak{m}_A}{\mathfrak{m}_A^2 + \mathfrak{m}_\Lambda R}.$$

Exercise. Fix a map $A \xrightarrow{f} B$ in $\widehat{\mathcal{C}}_\Lambda$. Then f is surjective if and only if $t_f^* : t_A^* \to t_B^*$ is surjective. [Use completeness... it's a Nakayamal's lemma sort of thing.]

A corollary of the Exercise is that if $d = \dim_k t_F = \dim_k t_R^*$ then we can pick a k-basis $x_1, \ldots, x_d$ of t_R^*, lift it to a collection $\widetilde{x}_i \in \mathfrak{m}_R \subset R$, and then the map $\Lambda[\![X_1, \ldots, X_d]\!] \to R$ sending X_i to $\widetilde{x}_i$ will be surjective. *A priori* bounds for the number of generators in the kernel (and hence on the dimension of R) can be obtained by estimating certain H^2s in the cohomology of G, which will be discussed later. These dimension bounds are sometimes useful, but usually not strong enough to give good control on R.

5. Examples.

A local case. Let $K/\mathbb{Q}_\ell$ be local with $\ell \neq p$ and $G = G_K$. Let $\overline{\rho}$ be the trivial representation of dimension n. Then in particular $\mathrm{End}_G \overline{\rho} \supsetneq k$, so only the framed deformation functor is representable. In this case we can actually construct $R^\square(\overline{\rho})$ by hand. If $\rho : G \to \mathrm{GL}_n A$ is a deformation of the trivial representation $\overline{\rho}$, then G lands in the kernel $\Gamma_n A \subset \mathrm{GL}_n A$. Now $\Gamma_n A = I_n + M_n(\mathfrak{m}_A)$, explicitly, which is a pro-p group isomorphism to the additive group $M_n(A)$. In particular ρ factors throug h the maximal pro-p quotient of G.

In particular $\rho|_{I_K}$ factors through the p-part of the tame quotient $I_K^{\mathrm{tame}} = I_K/I_K^{\mathrm{wild}}$ of the inertia I_K of K. The picture to keep in mind is the tower of field extensions

$$K \hookrightarrow K^{\mathrm{unr}} \hookrightarrow K^{\mathrm{tame}} \hookrightarrow \overline{K}.$$

Now from the structure of local fields we know that the p-part of I_K^{tame} is

$$I_K^{\mathrm{tame},(p)} = \mathbb{Z}_p(1).$$

Here the twist means that if $\sigma \in I_K^{\mathrm{tame},(p)}$ then $\mathrm{Frob}_K \, \sigma \, \mathrm{Frob}_K^{-1} = \sigma^q$ where $q = \ell^r = \#(\mathcal{O}_K/\mathfrak{m}_K)$. Fix a lift $f \in G$ of Frob_K and τ a topological generator of $I_K^{\mathrm{tame},(p)}$. What we can conclude is that a lift ρ to any A is specified by the images of f and τ, subject to the relation

$$\rho(f)\rho(\tau) = \rho(\tau)^q \rho(f).$$

So we can take

$$R^\square(\overline{\rho}) = \Lambda[\![\{f_{ij}, \tau_{ij}\}_{1 \leq i,j \leq n}]\!]/I$$

where the ideal of relations I is generated by the ones given by the matrix equations

$$[I_n + (f_{ij})][I_n + (\tau_{ij})] = [I_n + (\tau_{ij})]^q [I_n + (f_{ij})].$$

A global case. For a global case we'll consider *characters* of $G = G_{K,S}$. Note that we have a wonderful fact in this case. The Teichmüller lift $[\cdot] : k \to W(k)$ is a multiplicative section of $W(k) \to k$. This allows us to twist any character $\overline{\rho}$ by the Teichmüller lift $[\overline{\rho}^{-1}]$ of its reciprocal. to conclude that $R(\overline{\rho}) = R(\mathbf{1})$ where $\mathbf{1} : G \to k^\times$ is the trivial character. In other words, the universal deformation of a character $\overline{\rho}$ is just a twist of the universal deformation of the trivial character (using the same coefficient ring).

Arguing just like in the local case, it follows that any lift ρ to A of the trivial mod p character $\overline{\rho}$, must factor through the maximal pro-p quotient $G_{K,S}^{\mathrm{ab},(p)}$ of the abelianization of $G_{K,S}$.

Let us specialize now to the case $K = \mathbb{Q}$ [the case of a general number field is similar, but requires class field theory]. Assume $p \in S$, since otherwise stuff is boring. By the Kronecker-Weber theorem we know that $G_{\mathbb{Q},S}^{\mathrm{ab}} = \prod_{\ell \in S} \mathbb{Z}_\ell^\times$, which implies that the maximal pro-p quotient is

$$G_{\mathbb{Q},S}^{\mathrm{ab},(p)} = \prod_{\ell \in S, \ell \equiv 1 (p)} (\mathbb{F}_\ell^\times)^{(p)} \times (1 + p\mathbb{Z}_p).$$

So we can, in this case, simply take $R = \Lambda[\![G_{\mathbb{Q},S}^{\mathrm{ab},(p)}]\!]$ to be the formal group algebra over Λ. From the description of $G_{\mathbb{Q},S}^{\mathrm{ab},(p)}$ we can be very explicit:

$$R = \frac{\Lambda[\![\{X_\ell\}_{\ell \in S, \ell \equiv 1 (p)}, T]\!]}{(\{((X_\ell + 1)^{p^{\mathrm{ord}_p(\ell - 1)}} - 1)\}_{\ell \in S, \ell \equiv 1 (p)})}$$

In particular if $S = \{p, \infty\}$ then $R \cong \Lambda[\![T]\!]$.

For a general number field K this relates to the *Leopoldt conjecture* which says that $\mathrm{rk}_{\mathbb{Z}_p}(G_{K,S}^{\mathrm{ab},(p)}) = 1 + r_2$, where r_2 is the number of conjugate pairs of complex embeddings of K.

6. Local and Global. We can relate the two examples from the last subsection in the following manner, which will be extremely important later in one of Kisin's key improvements of Wiles' method. Let $G = G_{K,S}$, $\overline{\rho} : G_{K,S} \to \mathrm{GL}_n(k)$ a fixed residual representations, and Σ a finite set of primes. For each $v \in \Sigma$ we have

$$\overline{\rho}|_{G_v} : G_{K_v} = G_v \hookrightarrow G_K \twoheadrightarrow G_{K,S} \xrightarrow{\overline{\rho}} \mathrm{GL}_n(k).$$

We have local framed deformation rings $R_v^\square := R^\square(\overline{\rho}|_{G_v})$. Define a variation of the global framed deformation functor by

$$\mathrm{Def}^{\square,\Sigma}(\overline{\rho})(A) = \{(\rho_A, \{\beta_v\}_{v \in \Sigma})\}/\sim;$$

here, ρ_A is a deformation of $\overline{\rho}$ and β_v is a basis for $\rho_A|_{G_v}$ which reduces to the standard basis for $\overline{\rho}$. Then in fact $\mathrm{Def}^{\square,\Sigma}(\overline{\rho})$ is also representable, by a ring $R_{K,S}^{\square,\Sigma}$. For each $v \in \Sigma$ we have a forgetful map

$$\mathrm{Def}^{\square,\Sigma}(\overline{\rho}) \to \mathrm{Def}(\overline{\rho}|_{G_v})$$

and hence on the revel of representing objects, an algebra

$$R_v^\square \to R_{K,S}^{\square,\Sigma}.$$

In concrete terms, this is saying that if we form the universal deformation of $\overline{\rho}$ equipped with a framing along Σ and then forget the framing away from v and restrict to G_v, the resulting framed deformation of $\overline{\rho}|_{G_v}$ with coefficients in $R_{K,S}^{\square,\Sigma}$ is uniquely obtained by specializing the universal framed deformation of $\overline{\rho}|_{G_v}$ along a unique local Λ-algebra homomorphism $R_v^\square \to R_{K,S}^{\square,\Sigma}$.

Hence, by the universal property of completed tensor products (to be discussed in Samit's talk rather generally) we get an important map

$$\widehat{\bigotimes}_\Lambda R_v^\square \to R_{K,S}^{\square,\Sigma}$$

in $\widehat{\mathcal{C}}_\Lambda$. (Note that we have to take the completion of the algebraic tensor product, which is not itself a complete ring. For example, $\Lambda[\![x]\!] \otimes_\Lambda \Lambda[\![y]\!]$ is a gigantic non-noetherian ring, but the corresponding completed tensor product is $\Lambda[\![x,y]\!]$.) This is a rather interesting extra algebra structure on the global framed deformation ring, much richer than its mere Λ-algebra structure; of course, this all has perfectly good analogues without the framings, assuming that $\overline{\rho}$ and its local restrictions at each $v \in \Sigma$ have only scalar endomorphisms.

This idea of viewing a global deformation ring as an algebra over a (completed) tensor product of local deformation rings is the key to Kisin's method for "patching" deformation rings in settings going far beyond the original Taylor-Wiles method (where only the Λ-algebra structure was used).

Lecture 4. Brian on Characteristic Zero points of Deformation Rings

1. Some observations. Fix $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ absolutely irreducible, and let $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2(R)$ be the universal deformation. We're interested in the map $R \to \mathbb{T}_\mathfrak{m}$ for some Hecke algebra defined in terms of $\overline{\rho}$. Note that the Hecke algebra is 1-dimensional, and even finite free over $\mathbb{Z}_p$. The universal deformation ring R, however, often has dimension > 1 and nonzero p-torsion. In other words, the surjection $R \twoheadrightarrow \mathbb{T}_\mathfrak{m}$ is not even close to being an isomorphism in general.

Example. Consider $X_0(49)$ which is an elliptic curve. [Cf. Nigel Boston's papers on explicit deformation rings for the details of this example.] Let $\overline{\rho}$ the representation from the 3-torsion of E, and let $S = \{3, 7, \infty\}$. Boston computed the universal deformation as

$$\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2\left(\frac{\mathbb{Z}_3[\![x_1, x_2, x_3]\!]}{(1+x_1)^3 - 1}\right).$$

Just by looking at the ring on the right side, it's clear that its dimension is at least 2. (This example doesn't illustrate the phenomenon of p-torsion, but oh well...)

Morally, the reason for the higher dimension of R is that we are not imposing any local conditions at all for the places in S.

A key observation is that even when we succeed in proving a modularity lifting theorem, we don't know until we're done that R is $\mathbb{Z}_p$-finite and flat. In other words, even when in fact R turns out to be nice, we have very little grasp of why it is nice without proving an $R = \mathbb{T}$ theorem.

However, this is really not so bad. For example, if we could show that $R[1/p] \cong \mathbb{T}_m[1/p]$, that's totally fine. After all, we're trying to study deformations of $\overline{\rho}$ over p-adic integer rings, which are p-torsion free and reduced, so we rig the Hecke algebra to have the same properties. In other words, **we only care about the "p-adic points" of** R so we can just as well study the structure of $R[1/p]$/nilpotents. And via Kisin's methods, it turns out that a thorough understanding of the "structure" of this ring is attainable in interesting cases and is exactly what is needed for modularity lifting theorems. Things we would like to know:

- Characterize in some moduli-theoretic manner the connected components of its spectrum (e.g., so we can detect when two p-adic points lie on the same component).
- Dimension.
- Singularities, i.e. the extent to which an appropriately defined notion of smoothness fails to hold.

For the last point, it is just as good in practice to pass to a formally smooth R-algebra (such as a power series ring over R). So we can consider the framed deformation ring.

Remark. A key point is that $R[1/p]$ is **very** far from being a local ring. For example, say $R = \mathbb{Z}_p[\![x]\!]$ (which is a rough prototype of the sort of ring that arises). Then

$$R[1/p] = \mathbb{Z}_p[\![x]\!][1/p] = \{f \in \mathbb{Q}_p[\![x]\!] \mid \text{denominators are } \textit{bounded} \text{ powers of } p\} \subsetneq \mathbb{Q}_p[\![x]\!].$$

This ring has lots of $\mathbb{Q}_p$-algebra maps $\mathbb{Z}_p[\![x]\!][1/p] \twoheadrightarrow \mathcal{O}_K[1/p]$ for finite extensions $K/\mathbb{Q}_p$, sending x into $\mathfrak{m}_K$. Hence it has lots of maximal ideals.

2. Digression on Jacobson rings.

Definition. A **Jacobson ring** is a Noetherian ring A such that any $\mathfrak{p} \in \operatorname{Spec} A$ is the intersection of the maximal ideals containing $\mathfrak{p}$.

Clearly a quotient of a Jacobson ring is Jacobson. Less evident, but in the exercises of Atiyah-MacDonald, is that a finitely generated algebra over a Jacobson ring is Jacobson. Note that any field is Jacobson, as is any Dedekind domain with *infinitely many* primes (but not a dvr, nor a local ring which is not 0-dimensional!). In particular, a general localization of a Jacobson ring is certainly not Jacobson, though localization at a single element is (since it is a finitely generated algebra).

A consequence of the definition is that if $X_0 = \operatorname{MaxSpec}(A) \overset{j}{\hookrightarrow} \operatorname{Spec} A = X$, then j is a dense *quasihomeomorphism*, which means that $U_0 = X_0 \cap U \leftrightarrow U$ is a bijection between the collections of open sets in X_0 and X. Jacobson rings abstract the nice properties enjoyed by algebras of finite type over a field.

Claim. If R is a quotient of a formal power series ring over a complete dvr A with uniforizer π then $R[1/\pi]$ is Jacobson, and for all maximal ideals $\mathfrak{m} \subset R[1/\pi]$, the quotient $R[1/\pi]/\mathfrak{m}$ is finite over the fraction field $K = A[1/\pi]$ of A. Moreover, every K-algebra map from $R[1/\pi]$ to a finite extension K' of K carries R into the valuation ring A' of K', with the map $R \to A'$ actually a local map.

Note it is elementary that every K-algebra map from $R[1/\pi]$ to a finite extension K' of K has kernel that is maximal: the kernel P is at least a prime ideal, and $R[1/\pi]/P$ is an intermediate ring between the field K and the field K' of finite degree over K, so it is a domain of finite dimension over a field (namely K) and hence is itself a field. Hence, P is maximal.

Also, everything in the Claim can be deduced from facts in rigid geometry concerning K-affinoid algebras, by using the approach in deJong's IHES paper *Crystalline Dieudonné theory via formal and rigid geometry.* For convenience, we give a direct proof using commutative algebra, avoiding rigid geometry (but inspired by it for some of the arguments).

The proof of the Claim is somewhat long (and was omitted in the lecture).

Proof. To prove the claim, first note that if the claim holds for R then it holds for any quotient of R. Hence, it suffices to treat the case when $R = A[\![x_1, \ldots, x_n]\!]$ is a formal power series ring over A. We first check the more concrete second part of the Claim: for finite K'/K, any K-algebra map $R[1/\pi] \to K'$ carries R into the valuation ring A' of K' with $R \to A'$ moreover a local map. In other words, we are studying A-algebra maps $R \to K'$. This can be uniquely "promoted" to an A'-algebra map

$$A' \otimes_A R \to K',$$

and we can pass the tensor product through the "formal power series" formation since A' is a finite free A-module. In other words, we can rename A' as A to reduce to the case $K' = K$. So we claim that any A-algebra map $R \to K$ must be "evaluation" at an n-tuple in the maximal ideal of A. If we can show it carries each x_i to some a_i in the maximal ideal of A then the map kills $x_i - a_i$ for all i. By completeness of R it would be legal to make a "change of variables" renaming $x_i - a_i$ as x_i to reduce to the case when the map kills all x_i's. Since the quotient of R by the ideal generated by the x_i's is identified with A, after inverting π we get K (as a K-algebra!), so we'd have proved what we want.

Let's now show that indeed each x_i is carried to some a_i in the maximal ideal of A. By composing the given A-algebra map $R \to K$ with the natural inclusion $A[\![x_i]\!] \to R$ we are reduced to the case $n = 1$. That is, we wish to prove that any A-algebra map $A[\![x]\!] \to K$ must carry x to an element a in the maximal ideal of A. This map must kill some nonzero $f \in A[\![x]\!]$, as $A[\![x]\!][1/\pi]$ has infinite K-dimension as a vector space, and we can write $f = \pi^e f_0$ for some $e \geq 0$ and some f_0 not divisible by π. Thus, f_0 also dies in K, so by renaming it as f we arrange that f has some coefficient not divisible by π. This coefficient must occur in positive degree, as otherwise f would be a unit, which is absurd (as it is in the kernel of a map to a field). Now by the formal Weierstrass Preparation Theorem (in one variable –see Lang's *Algebra*), if $d > 0$ is the least degree of a coefficient of f not divisible by π then f is a unit multiple of a "distinguished" polynomial: a monic polynomial in x of degree d over A with all lower-degree coefficients divisible by π. Scaling away the unit, we can assume that f is a monic polynomial of degree $d > 0$ with all lower-degree coefficients divisible by π. Hence, $A[\![x]\!]/(f) = A[x]/(f)$ by long-division of formal power series (thanks to completeness of A!). Our map of interest therefore "is" an A-algebra map

$$A[x]/(f) \to K$$

and so it carries x to an element a of K that is a root of f. Since f is monic over A, we see $a \in A$. Since f has all lower-degree coefficients in the maximal ideal, necessarily a is in the maximal ideal too. That completes the proof of the second part of the Claim.

Now it remains to show the first part of the Claim: R is Jacobson, and if M is a maximal ideal of $R[1/\pi]$ then $R[1/\pi]/M$ is of finite degree over $A[1/\pi] = K$. We argue by induction on the number n of variables (motivated by the method of proof of the analytic Weierstrass Preparation theorem over $\mathbb{C}$ or non-archimedean fields), the case $n = 0$ being trivial. Also, it is harmless (even for the Jacobson property) to make a finite extension on K if we wish. We will use this later, to deal with a technical problem when the residue field k is finite (which is of course the case of most interest to us).

Assume $n > 0$, and consider a nonzero $f \in R = A[\![x_1, \ldots, x_n]\!]$ contained in some chosen nonzero prime or maximal ideal; clearly f can be scaled by π-powers so it is not divisible by π. We want to get to the situation in which f involves a monomial term that is just a power of a single variable. Pick a monomial of least total degree appearing in f with coefficient in $A^\times$. (Such a term exists, since f is not divisible by π.) This least total degree d must be positive (as otherwise $f(0) \in A^\times$, so $f \in R^\times$, a contradiction). By relabeling, we may suppose x_1 appears in this monomial. If $n = 1$, this term is an $A^\times$-multiple of a power of x_1, so we're happy. Now assume $n > 1$ and consider the *homogeneous* change of variables which replaces x_i with $x_i + c_i x_1$ for all $i > 1$ (and leaves x_1 alone), with $c_i \in A$ to be determined in a moment. Each degree-d monomial

$$a_I x_1^{i_1} \cdots x_n^{i_n}$$

in f (before the change of variable) with total degree d contributes

$$a_I c_2^{i_2} \cdots c_n^{i_n} x_1^d$$

to the x_1^d term after the change of variable (with $i_1 = d - (i_2 + \cdots + i_n)$). All other monomials can only contribute to x_1^d with coefficient in maximal ideal of A. Thus, these other terms can be ignored for the purpose of seeing if we get x_1^d to appear with an $A^\times$-coefficient after the change of variables.

To summarize (when $n > 1$), whatever c_i's we choose in A, we get after change of variable that x_1^d appears with coefficient $h(c)$ for some polynomial h in $n - 1$ variables over A that has *some* coefficient in $A^\times$ (since i_1 is determined by $i_2, \ldots, i_n$). Thus, h has nonzero reduction as a polynomial over the residue field k of A, so as long as this reduction is nonzero at some point in k^{n-1} we can choose the c's to lift that into A^{n-1}

to get the coefficient of x_1^d to be in $A^\times$. If k is infinite, no problem. If k is finite (case of most interest!), for some finite extension k' of k we can find the required point in k'^{n-1}, so go back and replace A with the corresponding unramified extension (and the chosen prime with each of the ones over it after scalar extension) to do the job.

The upshot is that after a suitable change of variables (and possible replacement of A with a finite extension in case k is finite), we can assume that f contains some x_1^d with an $A^\times$-coefficient. Thus, if we view f in

$$R = (A[\![x_2, \ldots, x_n]\!])[\![x_1]\!]$$

then it satisfies the hypotheses of the general Weierstrass Preparation (with complete coefficient ring) as in Lang's *Algebra*. This implies that f is a unit multiple of a *monic* polynomial in x_1 whose lower-degree coefficients are in the maximal ideal of $R' = A[\![x_2, \ldots, x_n]\!]$ (which means A if $n = 1$). We can therefore scale away the unit so that f is such a "distinguished" polynomial, and then do long division in $R'[\![x_1]\!]$ due to completeness of R' to infer that

$$R/(f) = R'[\![x_1]\!]/(f) = R'[x_1]/(f).$$

This is a finite free R'-module!

We may now draw two consequences. First, if P is a prime ideal of $R[1/\pi]$ containing f then $R[1/\pi]/P$ is module-finite over the ring $R'[1/\pi]$ which is Jacobson by induction, so $R[1/\pi]/P$ is Jacobson. Hence, P is the intersection of all maximals over it, whence we have proved that $R[1/\pi]$ is Jacobson. Second, for a maximal ideal M of $R[1/\pi]$ containing f, the ring map $R'[1/\pi] \to R[1/\pi]/M$ is module-finite so its prime ideal kernel is actually maximal. That is, we get a *maximal* ideal M' of $R'[1/\pi]$ such that $R'[1/\pi]/M' \to R[1/\pi]/M$ is of finite degree. By induction, $R'[1/\pi]/M'$ is of finite degree over K, so we are done. $\square$

3. Visualizing $R[1/p]$**.** Let $R = A[\![x_1, \ldots, x_n]\!]/(f_1, \ldots, f_m)$ and K be in the last subsection. Observe that $\mathrm{Hom}_{\mathrm{loc}.A-\mathrm{alg}}(R, A') = \mathrm{Hom}_{\mathrm{Frac}(A)-\mathrm{alg}}(R[1/\pi], A'[1/\pi] = \mathrm{Frac}(A'))$ for any finite dvr extension A' of A. This suggests the following geometric perspective on the ring $R[1/\pi]$: it corresponds to the locus of geometric points (x_i) with coordinates in $\overline{\mathrm{Frac}(A)}$ lying in the open polydisk $\{|x_1|, \ldots, |x_n| < 1\}$ at which the convergent power series $f_1, \ldots, f_m$ all vanish. To make this viewpoint precise, one must regard the spaces in question as **rigid analytic spaces**.

4. Final thought. We'll see that for Galois deformation rings R, the completions of $R[1/p]$ at maximal ideals are deformation rings for *characteristic zero* representations corresponding to the maximal ideals in question. This is very interesting, since R itself was entirely about deforming mod p things!

5. Back to examples of explicit universal deformation rings. Caveat: These sorts of examples are kind of "useless". The reference for N. Boston's examples is *Inv. Math.* **103** (1991).

Example 1 [loc. cit., Prop. 8.1.] Let $E : y^2 = x(x^2 - 8x + 8)$, an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-2})$. Let $\overline{\rho}$ be the representation on the 3-torsion:

$$G_{\mathbb{Q},\{2?,3,5,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_3).$$

In general we know that there is some surjection $\mathbb{Z}_3[\![T_1, \ldots, T_d]\!] \twoheadrightarrow R(\overline{\rho})$ where we know the smallest d is (by NAK) $d = \dim \mathfrak{m}_R/(\mathfrak{m}_R^2, 3)$, and $\mathfrak{m}_R/(\mathfrak{m}_R^2, 3) = \mathrm{H}^1(G_{\mathbb{Q},\{2?,3,5,\infty\}}, \mathrm{Ad}(\overline{\rho}))$. Here the adjoint module is $\mathrm{Ad}(\overline{\rho}) = \mathrm{End}_{\mathbb{F}_3}(\overline{\rho})$ with $G_{\mathbb{Q},\{2?,3,5,\infty\}}$ acting by conjugation via $\overline{\rho}$. In this particular case one can compute that $d = 5$, so

$$R(\overline{\rho}) = \mathbb{Z}_3[\![T_1, \ldots, T_5]\!]/I$$

where the ideal of relations has the form

$$I = \delta \cdot (f, g)$$

for

$$f = 8u^4 - 8u^2 + 1, g = 8e^3 - 4u, \qquad u = (1 + T_4T_5)^{1/2}$$

and δ (which may involve all the T_is) is obtained by choosing a certain presentation of a pro-3 group (coming from a wild inertia group, perhaps for the splitting field of $\overline{\rho}$?), and setting $\delta = \det(\rho^{\mathrm{univ}}(y) - 1)$ where y is a particular generator in said presentation. Consequently one can write down some "explicit" deformations of $\overline{\rho}$ by looking for solutions to the relations above in a $\mathbb{Z}_3$-algebra...

Example 2 [Boston-Ullom]. Let $E = X_0(49)$ and $\overline{\rho} = \overline{\rho}_{E,3}$ the representation on the 3-torsion:

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

In this case the universal deformation ring is particularly simple:

$$R \cong \mathbb{Z}_3[\![T_1, \ldots, T_4]\!]/((1+T_4)^3 - 1).$$

We have $(1+T_4)^3-1 = T_4(T_4^2+3T_4+3)$. The quadratic factor is irreducible over $\mathbb{Q}_3$, but not over $\mathbb{Q}_3(\sqrt{-3})$. So, loosely speaking, $\operatorname{Spec} R$ has two irreducible components but three "geometric" irreducible components: $T_4 = 0$ and T_4 equal to either of the conjugate roots of the quadratic factor. For example, to recover the 3-adic Tate module of E one considers the map $R \to \mathbb{Z}_3$ given by mapping all T_is to 0. This is a sort of "canonical" $\mathbb{Z}_3$-point of $\operatorname{Spec} R$. Since the quadratic factor of the relation is $\mathbb{Q}_3$-irreducible, so that quadratic field cannot be $\mathbb{Q}_3$-embedded into $\mathbb{Q}_3$, *every* $\mathbb{Z}_3$-point lies in the $T_4 = 0$ component.

The lesson to take from this seems to be that it can be hard to detect components, or more generally aspects of the geometry, of $\operatorname{Spec} R$, when only looking at p-adic points over a small field like $\mathbb{Q}_p$; we have to expect to work with points in many finite extensions in order to effectively probe the geometry. All this is by way of motivation for our interest in characteristic zero points of deformation rings, and (for example) our willingness to throw out all possible nastiness at p by studying $R[1/p]$ instead of R itself.

6. Back to Characteristic 0. Now let Λ be a p-adic dvr with fraction field K and residue field k. Let $R = \Lambda[\![X_n, \ldots, X_n]\!]/I$ be the universal deformation ring of a residual representation $\overline{\rho} : \Gamma \to \mathrm{GL}_N(k)$, for a profinite group Γ satisfying the requisite p-finiteness conditions (e.g. G_K for local K or $G_{K,S}$ for a number field K).

Remark. We have seen above that for any maximal ideal $\mathfrak{m} \subset R[1/p]$, the residue field $R[1/p]/\mathfrak{m}$ is of finite degree over k. The intuition for this fact is that these closed points of $\operatorname{Spec} R[1/p]$ correspond to Galois orbits over K of $\overline{K}$-solutions to $I = 0$ in the open unit n-polydisk. (The case $n = 1$ is a consequence of the Weierstrass Preparation Lemma. One *can* relate the geometry of $\operatorname{Spec} R[1/p]$ to the geometry of the aforementioned "rigid analytic space" $I = 0$. For example, if $R[1/p]$ is connected (no nontrivial idempotents) then $I = 0$ is connected in the sense of rigid geometry. One can also match up the dimensions of the components. The input for this equivalence is the (self-contained!) §7 of de Jong's IHES paper *Crystalline Dieudonné theory* ..., but we won't use it.

We also saw above that any K-algebra map $R[1/p] \to K'$ for a finite extension K'/K is actually given by sending all the X_is to elements $x_i \in \mathfrak{m}_{K'} \subset \mathcal{O}_{K'} \subset K'$. In other words, $R \subset R[1/p]$ actually lands in $\mathcal{O}_{K'}$!

Now fix a K-algebra map $x : R[1/p] \twoheadrightarrow K'$ into a finite extension of K. ("Contemplate a p-adic point of $\operatorname{Spec} R$".) Let

$$\rho_x : \Gamma \xrightarrow{\rho^{\mathrm{univ}}} \mathrm{GL}_N(R) \to \mathrm{GL}_N(R[1/p]) \to \mathrm{GL}_N(K')$$

be the specialized representation. (In the Boston-Ullom example above, when we take $x : R[1/3] \to \mathbb{Q}_3$ to be the map sending all the T_is to zero, then ρ_x is the 3-adic Tate module of $X_0(49)$.)

Goal: Understand the dimension $\dim R[1/p]_{\mathfrak{m}_x} = \dim R[1/p]^\wedge_{\mathfrak{m}_x}$**.** (Here $(\cdot)^\wedge$ denotes completion.)

For instance, is this complete local ring regular? Perhaps even a power series ring over K'? If so, then its dimension is $\dim \mathfrak{m}_x/\mathfrak{m}_x^2$.

Theorem. *Let* $\rho_x^{\mathrm{univ}} : \Gamma \to \mathrm{GL}_N(R[1/p]^\wedge_{\mathfrak{m}_x})$ *be induced from* ρ^{univ} *by the natural map* $R \to R[1/p]^\wedge_{\mathfrak{m}_x}$*. Then the diagram*

$$\begin{array}{ccc} \Gamma & \xrightarrow{\rho_x^{\mathrm{univ}}} & \mathrm{GL}_N(R[1/p]^\wedge_{\mathfrak{m}_x}) \\ & \underset{\text{cont}}{\overset{\rho_x}{\searrow}} & \downarrow \\ & & \mathrm{GL}_N(K') \end{array}$$

commutes, and in fact ρ_x^{univ} *is the universal for continuous deformations of* ρ_x*.*

More precisely, if one considers the category $\widehat{\mathcal{C}}$ *of complete local noetherian* K'*-algebras with residue field* K'*, and the functor on the category* $\mathcal{C}$ *of artinian quotients of objects in* $\widehat{\mathcal{C}}$ *which picks out those deformations of* ρ_x *which are continuous for the* p*-adic topology on such artinian quotients, regarded as finite-dimensional* K'*-vector spaces, then* $R[1/p]^\wedge_{\mathfrak{m}_x}$ *is the representing object.*

Remark. If A is a complete local Noetherian F-algebra and the characteristic of F is zero, and $A/\mathfrak{m} = F'$ is a finite extension of F, then there exists a unique F-algebra lift $F' \hookrightarrow A$. Why? By completeness we have Hensel's lemma and by characteristic zero we have F'/F separable. So we can find solutions in A to the defining polynomial of F' over F.

Why do we care about the theorem?

(1) The deformation ring $R[1/p]^\wedge_{\mathfrak{m}_x}$ is isomorphic to $K'[\![T_1, \ldots, T_n]\!]$ if and only if $R[1/p]^\wedge_{\mathfrak{m}_x}$ is regular (by the Cohen structure theorem), and the power series description is precisely the condition that the corresponding deformation functor for ρ_x is formally smooth (i.e., no obstruction to lifting artinian points in characteristic 0). This holds precisely when $\mathrm{H}^2(\Gamma, \mathrm{Ad}(\rho_x)) = 0$. So that is interesting: a computation in Galois cohomology in characteristic 0 can tell us information about the structure of $R[1/p]$ at closed points.

(2) $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \cong \mathrm{H}^1_{\mathrm{cont}}(\Gamma, \mathrm{Ad}(\rho_x))$, by the continuity condition we imposed on the deformations in the theorem.

Combining (1) and (2), we can check regularity of $R[1/p]$ at a closed point and in such cases then even compute $\dim_x R[1/p]$ by doing computations in (continuous) Galois cohomology with p-adic coefficients!

7. Proof of theorem.

Step 1: Reduce to the case $K' = K$. Here is the trick. Set $\Lambda' = \mathcal{O}_{K'}$. Note that $\Lambda' \otimes_\Lambda R$ is local because $(\Lambda' \otimes_\Lambda R)/\mathfrak{m}_R = \Lambda' \otimes_\Lambda k = k'$ is a field. The Λ'-algebra $\Lambda' \otimes_\Lambda R$ is the universal deformation ring of $\overline{\rho} \otimes_k k'$ (where k' is the residue field of K') when using Λ'-coefficients; this behavior of deformation ring with respect to finite extension of the coefficients will be proved in Samit's talk. Consider the diagram

$$\begin{array}{ccc}
K' \otimes_K R[1/p] & \xrightarrow{x'} & K' \\
\| & & \uparrow \\
(\Lambda' \otimes_\Lambda R)[1/p] & & \\
\uparrow & & \\
\Lambda' \otimes_\Lambda R & \longrightarrow & \Lambda'
\end{array}$$

Exercise: $(\Lambda' \otimes_\Lambda R)[1/p]^\wedge_{\mathfrak{m}_{x'}} \cong R[1/p]^\wedge_{\mathfrak{m}_x}$ as K'-algebras.

So we can rename Λ' as Λ, completing the reduction.

Step 2: Observe that since $\overline{\rho}$ is absolutely irreducible, so is ρ_x. Consequently any deformation of ρ_x has only scalar endomorphisms.

Step 3: Consider any deformation

$$\begin{array}{ccc}
\Gamma & \xrightarrow{\theta} & \mathrm{GL}_N(A) \\
& \searrow^{\rho_x} & \downarrow \\
& & \mathrm{GL}_N(K)
\end{array}$$

where A is a finite local K-algebra with residue field K. We would like to show that there exists a unique K-map $R[1/p]^\wedge_{\mathfrak{m}_x} \to A$ which takes ρ_x^{univ} to θ, up to conjugation. Why is this sufficient? Because if so, then there would be lifts of ρ_x to $\mathrm{GL}_N(A)$, one coming from ρ_x^{univ} and the other being θ, which are $\mathrm{GL}_N(A)$-conjugate to one another by some matrix M. Upon reduction to $\mathrm{GL}_N(K)$, the matrix $\overline{M}$ would centralize ρ_x. So by Step 2, $\overline{M}$ must be a scalar endomorphism $c \in K^\times$. Consequently we can replace M by $c^{-1}M$ to conclude that the two lifts are conjugate to one another by a matrix which is residually trivial. The latter is precisely what we need to prove that ρ_x^{univ} is universal. (Note that if we used framed deformations throughout then this little step wouldn't be needed. It is important because in later applications we will certainly want to apply the Theorem to cases for which $\overline{\rho}$ is not absolutely irreducible. The reader can check that the proof of the Theorem works in the framed setting once the preceding little step is bypassed.)

The map we need is the same as making a local K-algebra map

$$R[1/p]_{\mathfrak{m}_x} \to A$$

with the same property with respect to θ, since A is a complete K-algebra. (Note that this "uncompletion" step is only possible since we already did Step 1! We originally completed $R[1/p]_{\mathfrak{m}_x}$, which is a K-algebra and generally not a K'-algebra.) The latter is the same as a K-algebra map $R[1/p] \to A$ such that $R[1/p] \to A \to K$ is the original point x, which takes ρ^{univ} to θ. ("It's all a game in trying to get back to R".) In other words, we wanted a dotted map in the diagram

$$\begin{array}{ccccc} R & \longrightarrow & R[1/p] & \overset{\exists!?}{\dashrightarrow} & A \\ {\scriptstyle \exists!\widetilde{x}}\downarrow & & & \searrow^{x} & \downarrow \\ \Lambda & & \longrightarrow & & K \end{array}$$

(The existence of $\widetilde{x}$ is by one of the propositions from §6.) But $R[1/p]$ is just a localization of R and A is a $\Lambda[1/p]$-algebra (it is a K-algebra!), so in fact the existence of a unique dotted map above is equivalent to the existence of a unique dotted map α in the diagram

$$\begin{array}{ccc} R & \overset{\exists!?}{\underset{\alpha}{\dashrightarrow}} & A \\ {\scriptstyle \widetilde{x}}\downarrow & & \downarrow \\ \Lambda & \longrightarrow & K \end{array}$$

such that α takes ρ^{univ} to θ. Now unfortunately A is not in the category $\widehat{\mathcal{C}}_\Lambda$ [typically it is something like $K[t]/(t^7)$], so θ is not quite a deformation of $\overline{\rho}$, so we cannot appeal directly to the universal property of $(R, \rho^{\mathrm{univ}})$. Instead we need to mess around a bit.

Here's the point. $A = K \oplus \mathfrak{m}_A$ and $\mathfrak{m}_A$ is a finite-dimensional K-vector space which is nilpotent.

Claim. $\mathfrak{m}_A = \varinjlim I$ where the limit is taken over Λ-finite multiplicatively stable Λ-modules I.

(Idea of the proof: take products and products and more products. By nilpotence and finite-dimensionality of $\mathfrak{m}_A$ over K, you don't have to keep going forever. Then take the Λ-span of finite collections of such products to get the desired I's.)

Write Λ_I for $\Lambda \oplus I$.

Lemma/Exercise: Any Λ-algebra map $R \to A$ lands in some Λ_I. (Hint: choose I containing the images of all the X's.)

So it's enough to show two things.

(1) For some I we have a map $R \to \Lambda_I$ giving a deformation θ_I of the "integral lattice" version $\rho_{\widetilde{x}}$ of ρ_x. The image of Γ under ρ^{univ} is topologically finitely generated (since $\mathrm{GL}_N(R)$ is essentially pro-p and Γ satisfies the p-finiteness condition), so then there exists *some* I_0 such that θ factors through $\mathrm{GL}_N(\Lambda_{I_0})$, giving a map $\theta_{I_0} : \Gamma \to \mathrm{GL}_N(\Lambda_{I_0})$.

(2) The map from (1) is unique.

Indeed, by then comparing any two I and I' with a common one, we'd get the desired existence and *uniqueness* at the level of coefficients in A.

To prove (1), note that $\Lambda_I \in \widehat{\mathcal{C}}_\Lambda$ and θ_I deforms $\rho_{\widetilde{x}}$, and hence $\overline{\rho}$. Here is the picture:

$$\begin{array}{ccc} \rho^{\mathrm{univ}} & \overset{\exists}{\dashrightarrow} & \theta_I \\ & \searrow \quad \swarrow & \\ & \rho_{\widetilde{x}} & \\ & \downarrow & \\ & \overline{\rho} & \end{array}$$

The induced map $R \to \Lambda_I$ respects the map to Λ coming from the fact that $\rho_{\widetilde{x}}$ deforms $\overline{\rho}$, because if not, then we would have another map $R \to \Lambda_I \to \Lambda$, which contradicts the universal property of R.

To prove (2) just use the uniqueness from the universal property of (R, ρ^{univ}) for deforms on $\widehat{\mathcal{C}}_\Lambda$.

1. Samit on Dimensions of Deformation Rings

This lecture is about getting bounds for the dimension of deformation rings, by bounding the number of generators and relations. The reference for this lecture is Kisin's article in CDM, or stuff from his Hawaii notes.

1.1. **Local setup and statement.** Let $K/\mathbb{Q}_p$ be finite, $\mathcal{O} = \mathcal{O}_K, \pi$ a uniformizer, $k = \mathcal{O}/(\pi)$, Γ a profinite group satisfying the p-finiteness condition "Φ_p", and $\overline{\rho} : \Gamma \to \mathrm{GL}_n(k)$ a mod π representation. We consider deformations to complete local noetherian $\mathcal{O}$-algebras with residue field k. The framed deformation ring $R^{\square}_{\overline{\rho}}$ always exists, so we have a universal representation

$$\Gamma \overset{\rho^{\square}_{\text{univ}}}{\to} \mathrm{GL}_n(R^{\square}_{\overline{\rho}}).$$

Assuming $\mathrm{End}_\Gamma\, \overline{\rho} = k$, we also know $R_{\overline{\rho}}$ exists, and we then get a universal deformation

$$\Gamma \overset{\rho^{\text{univ}}}{\to} \mathrm{GL}_n(R_{\overline{\rho}}).$$

Recall that

$$D^{\square}_{\overline{\rho}}(k[\epsilon]) = \mathrm{Hom}_k(\mathfrak{m}_{R^\square}/(\mathfrak{m}^2_{R^\square}, \pi), k) \cong Z^1(\Gamma, \mathrm{ad}\, \overline{\rho})$$

and $D_{\overline{\rho}}(k[\epsilon]) = \mathrm{H}^1(\Gamma, \mathrm{ad}\, \overline{\rho})$ as k-vector spaces.

Theorem. *Let $r = \dim_k Z^1(\Gamma, \mathrm{ad}\, \overline{\rho})$. Then there exists an $\mathcal{O}$-algebra isomorphism*

$$\mathcal{O}[\![x_1, \dots, x_r]\!]/(f_1, \dots, f_s) \cong R^{\square}_{\overline{\rho}}$$

where $s = \dim_k \mathrm{H}^2(\Gamma, \mathrm{ad}\, \overline{\rho})$.

Corollary. (i) $\dim R^{\square}_{\overline{\rho}} \geq 1 + n^2 - \chi(\Gamma, \mathrm{ad}\, \overline{\rho}) = 1 + n^2 - h^0(\mathrm{ad}\, \overline{\rho}) + h^1(\mathrm{ad}\, \overline{\rho}) - h^2(\mathrm{ad}\, \overline{\rho})$.
(ii) $\dim R_{\overline{\rho}} \geq 2 - \chi(\Gamma, \mathrm{ad}\, \overline{\rho})$.

Proof of corollary. From $\mathcal{O}$ we get a contribution of 1. hence we get $\dim R^{\square}_{\overline{\rho}} \geq 1 + \dim Z^1 - h^2$. Now (i) follows formally noting that $\dim Z^0 = \dim C^0 = n^2$. (Use $h^1 = \dim Z^1 - \dim B^1$ and $\dim B^1 = \dim C^0 - \dim Z^0 = \dim C^0 - h^0$.) Then (ii) is immediate using the fact that $R^{\square}_{\overline{\rho}}$ is basically a PGL_n-bundle over $R_{\overline{\rho}}$. □

1.2. **Proof of Theorem 1.1.** Using completeness [exercise] we can choose a surjection

$$\varphi : \mathcal{O}[\![x]\!] := \mathcal{O}[\![x_1, \dots, x_r]\!] \twoheadrightarrow R^{\square}_{\overline{\rho}}.$$

(Send the x_i's to elements which reduce to a basis for the tangent space $Z^1(\Gamma, \mathrm{ad}\, \overline{\rho})$ of the framed deformation ring.) The problem is to show that the minimal number of generators of the kernel $\mathbb{J} = \ker \varphi \subset \mathcal{O}[\![x]\!]$ is at most s. Let $\mathbf{m} = \mathfrak{m}_{\mathcal{O}}[\![x]\!] \subset \mathcal{O}[\![x]\!]$ be the maximal ideal $(\pi, x_1, \dots, x_r)$. It would suffice to construct a linear injection $(\mathbb{J}/\mathbf{m}\mathbb{J})^* \hookrightarrow \mathrm{H}^2(\Gamma, \mathrm{ad}\, \overline{\rho})$. There is a subtle technical problem in an attempt to construct such an injection. We explain the problem, and then the fix to get around it.

For each $\gamma \in \Gamma$ choose a set-theoretic lift $\widetilde{\rho}(\gamma) \in \mathrm{GL}_n(\mathcal{O}[\![x]\!]/\mathbf{m}\mathbb{J})$ of $\rho^{\square}(\gamma) \in \mathrm{GL}_n(\mathcal{O}[\![x]\!]/\mathbb{J}) = \mathrm{GL}_n(R^\square)$. We need to make this choice so that $\widetilde{\rho}$ is a *continuous* function of γ. It is not clear if the map

$$\mathcal{O}[\![x]\!]/\mathbf{m}\mathbb{J} \twoheadrightarrow \mathcal{O}[\![x]\!]/\mathbb{J}$$

admits a continuous section as topological spaces, so it is not clear how to find a continuous $\widetilde{\rho}$. To handle this problem, we now prove:

Claim: For $r > 0$, let $\mathbb{J}_r = (\mathbb{J} + \mathbf{m}^r)/\mathbf{m}^r \in \mathcal{O}[\![x]\!]/\mathbf{m}^r$ and let $\mathbf{m}_r = \mathbf{m}/\mathbf{m}^r$. For $r \gg 0$, the natural map $\mathbb{J}/\mathbf{m}\mathbb{J} \to \mathbb{J}_r/\mathbf{m}_r\mathbb{J}_r$ is an isomorphism.

Proof. The map is surjective, and for injectivity we have to show that $\mathbb{J} \cap (\mathbf{m}\mathbb{J} + \mathbf{m}^r) = \mathbf{m}\mathbb{J}$ for large r. Certainly $\mathbf{m}\mathbb{J}$ lies in the intersection for all r, so since $\mathbb{J}/\mathbf{m}\mathbb{J}$ has finite length we see that the intersection stabilizes at some intermediate ideal for $r \gg 0$. This stabilizing ideal must then be the total intersection. But by Artin-Rees applied to $\mathbf{m}\mathbb{J}$ as a finite $\mathcal{O}[\![x]\!]$-module, the intersection of all $(\mathbf{m}\mathbb{J} + \mathbf{m}^r)$'s is $\mathbf{m}\mathbb{J}$. □

By the Claim, to prove the desired result about minimal number of generators of $\mathbb{J}$, we can replace $\mathcal{O}[\![x]\!]$ and $R^{\square} := R^{\square}_{\overline{\rho}}$ with their quotients by rth power of maximal ideal for some large r. The quotient of $R^{\square}$ by rth power of its maximal ideal is universal in the category of complete local noetherian $\mathcal{O}$-algebras whose maximal ideal has vanishing rth power (exercise!). So working within this full subcategory of local $\mathcal{O}$-algebras, we can still exploit universal mapping properties. But we gain the advantage that now our rings are of finite length as $\mathcal{O}/\pi^r$-modules, so in particular they're all discrete with their max-adic topology and hence the Galois representations which arise have open kernel. We can therefore find the required continuous section, working throughout with local rings whose maximal ideal has a fixed but large order of nilpotence.

So we now proceed in such a modified setting (so the definition of $\mathbb{J}$ changes accordingly, but the Claim shows that this does not affect $\mathbb{J}/\mathbf{m}\mathbb{J}$, which is to say the minimal number of generators of $\mathbb{J}$). In particular, in the new setting we will construct a k-linear injection of $\mathbb{J}/\mathfrak{m}\mathbb{J}$ into $\mathrm{H}^2(\Gamma, \mathrm{ad}\,\overline{\rho})$, thereby finishing the proof.

For $f \in (\mathbb{J}/\mathbf{m}\mathbb{J})^*$. let

$$\rho_f(\gamma, \delta) = f(\widetilde{\rho}(\gamma\delta)\widetilde{\rho}(\delta)^{-1}\widetilde{\rho}(\gamma)^{-1} - \mathbf{1}),$$

where we apply the map f "entry-wise" to the given matrix in $\mathrm{Mat}_{n\times n}(\mathbb{J}/\mathbf{m}\mathbb{J})$. That is, the map φ_f has the form

$$\Gamma^2 \to \mathrm{Mat}_{n\times n}(\mathbb{J}/\mathbf{m}\mathbb{J}) \xrightarrow{f} \mathrm{Mat}_{n\times n}(k).$$

Now we observe the following facts.

(1) $\varphi_f \in Z^2(\Gamma, \mathrm{ad}\,\overline{\rho})$.
(2) $[\varphi_f] \in \mathrm{H}^2(\Gamma, \mathrm{ad}\,\overline{\rho})$ is independent of the choice of lift $\widetilde{\rho}$.
(3) $f \mapsto [\varphi_f]$ is k-linear.
(4) $f \mapsto [\varphi_f]$ is injective, but more precisely we have $[\varphi_f] = 0 \Leftrightarrow$ we can choose $\widetilde{\rho}$ to be a homomorphism "mod $\mathbb{J}_f$" where $\mathbb{J}_f = \ker(\mathbb{J} \to \mathbb{J}/\mathbf{m}\mathbb{J} \xrightarrow{f} k) \Leftrightarrow f = 0 \Leftrightarrow \mathbb{J}_f = \mathbb{J}$.

Note that (4) provides the desired linear injection, and hence proves the theorem; (1)-(3) are necessary to make sense of (4).

Let us prove the facts above.

(1) This is a formal computation, which goes as follows. Note that we can identify $\mathrm{Mat}_{n\times n}(\mathbb{J}/\mathbf{m}\mathbb{J})$ under addition with $(\mathbf{1} + \mathrm{Mat}_{n\times n}(\mathbb{J}/\mathbf{m}\mathbb{J}))$ under multiplication, since $\mathbb{J} \subset \mathbf{m}$. Using this identification, we have

$$\mathrm{d}\,\varphi_f(\gamma, \delta, \epsilon) = \gamma\varphi_f(\delta, \epsilon) - \varphi_f(\gamma\delta, \epsilon) + \varphi_f(\gamma, \delta\epsilon) - \varphi_f(\gamma, \delta) \in \mathrm{Mat}_{n\times n}(k).$$

If we want to prove this is zero, it's enough to check "upstairs" in $\mathrm{Mat}_{n\times n}(\mathbb{J}/\mathbf{m}\mathbb{J})$, i.e. before applying f. Thus we really want to check that

$$(\widetilde{\rho}(\gamma)\widetilde{\rho}(\delta\epsilon)\widetilde{\rho}(\epsilon)^{-1}\widetilde{\rho}(\delta)^{-1}\widetilde{\rho}(\gamma)^{-1}) \times (\widetilde{\rho}(\gamma\delta)\widetilde{\rho}(\epsilon)\widetilde{\rho}(\gamma\delta\epsilon)^{-1}) \\ \times (\widetilde{\rho}(\gamma\delta\epsilon)\widetilde{\rho}(\delta\epsilon)^{-1}\widetilde{\rho}(\gamma)^{-1}) \times (\widetilde{\rho}(\gamma)\widetilde{\rho}(\delta)\widetilde{\rho}(\gamma\delta)^{-1}) \stackrel{?}{=} \mathbf{1}\,.$$

The trick is to insert the bracketed term (which is 1) below:

$$\widetilde{\rho}(\gamma)\widetilde{\rho}(\delta\epsilon)\widetilde{\rho}(\epsilon)^{-1}\widetilde{\rho}(\delta)^{-1}\widetilde{\rho}(\gamma)^{-1}\widetilde{\rho}(\gamma\delta)\,\overbrace{\widetilde{\rho}(\delta)^{-1}\widetilde{\rho}(\delta)}^{insert}\,\widetilde{\rho}(\epsilon)\widetilde{\rho}(\gamma\delta\epsilon)^{-1} \\ \times \widetilde{\rho}(\gamma\delta\epsilon)\widetilde{\rho}(\delta\epsilon)^{-1}\widetilde{\rho}(\gamma)^{-1} \times (\widetilde{\rho}(\gamma)\widetilde{\rho}(\delta)\widetilde{\rho}(\gamma\delta)^{-1}) \stackrel{?}{=} \mathbf{1}\,.$$

Now observe that the bracketed terms below reduce to 0 in $\mathrm{Mat}_{n\times n}(k)$ and hence can be commuted with one another (!):

$$\widetilde{\rho}(\gamma)\,\overbrace{\widetilde{\rho}(\delta\epsilon)\widetilde{\rho}(\epsilon)^{-1}\widetilde{\rho}(\delta)^{-1}}^{I}\,\overbrace{\widetilde{\rho}(\gamma)^{-1}\widetilde{\rho}(\gamma\delta)\widetilde{\rho}(\delta)^{-1}}^{II}\,\widetilde{\rho}(\delta)\widetilde{\rho}(\epsilon)\widetilde{\rho}(\gamma\delta\epsilon)^{-1} \\ \times \widetilde{\rho}(\gamma\delta\epsilon)\widetilde{\rho}(\delta\epsilon)^{-1}\widetilde{\rho}(\gamma)^{-1} \times (\widetilde{\rho}(\gamma)\widetilde{\rho}(\delta)\widetilde{\rho}(\gamma\delta)^{-1}) \stackrel{?}{=} \mathbf{1}\,.$$

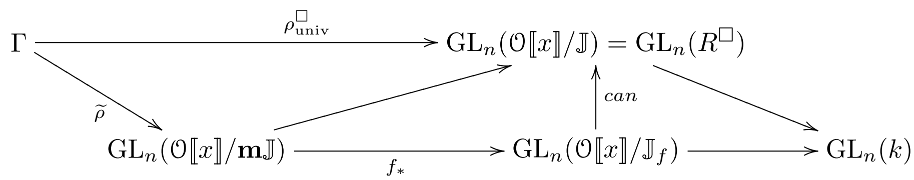
After swapping I and II one sees that in fact everything cancels magically. (Is there is a "conceptual" proof of (1)?)

(2) This is similar to (1). First write $\widetilde{\rho}^{\text{new}}(\gamma) = a(\gamma)\widetilde{\rho}(\gamma)$ for some
$$a : \Gamma \to \mathbf{1} + \mathrm{Mat}_{n\times n}(\mathbb{J}/\mathbf{m}\mathbb{J}).$$
The idea is to show formally that $a(\gamma)$ (which is of course a *continuous* 1-cocycle on Γ) changes φ_f by $\mathrm{d}\, a$. This is done with a similar "insert $\mathbf{1}$ cleverly and commute stuff" trick as in (1).

(3) OK.

(4) The last equivalence in (4) is clear. For the other two equivalences, the implications "$\Leftarrow$" are OK. The implication that $[\varphi_f] = 0$ implies we can choose $\widetilde{\rho}$ to be a homomorphism mod $\mathbb{J}_f$ follows from the previous calculation [omitted] that $\widetilde{\rho} \rightsquigarrow a \cdot \widetilde{\rho}$ changes φ by $\mathrm{d}\, a$. In particular, if φ is already a coboundary, then by changing the choice of lift we can make $\varphi = 0$, which is the same as saying our lift is a homomorphism mod $\mathbb{J}_f$. So the crux of the matter is the second "$\Rightarrow$".

Here's the situation. We have a diagram



We'd like to prove that $\mathcal{O}[\![x]\!]/\mathbb{J}_f \to \mathcal{O}[\![x]\!]/\mathbb{J}$ is an isomorphism. By the universality of $R^{\square}$ we get the map
$$\mathcal{O}[\![x]\!]/\mathbb{J} \overset{\exists!}{\to} \mathcal{O}[\![x]\!]/\mathbb{J}_f \overset{\text{can}}{\to} \mathcal{O}[\![x]\!]/\mathbb{J}$$
and again by universality the composition is the identity. Now it would be enough to check that $\mathbb{J} \subset \mathbb{J}_f$. Note that the image of x_i in $\mathcal{O}[\![x]\!]/\mathbb{J}$ maps to $x_i + a_i \in \mathcal{O}[\![x]\!]/\mathbb{J}_f$ where a_i is some element of $\mathbb{J}$. It will suffice to show that if $g(x_1, \ldots, x_n) \in \mathbb{J}$ then g maps to g itself in $\mathcal{O}[\![x]\!]/\mathbb{J}_f$.

First we claim that $\mathbb{J} \subset (\mathbf{m}^2, \pi)$ [recall that $\mathbb{J} = \ker(\mathcal{O}[\![x]\!] \twoheadrightarrow R^{\square})$]. Indeed, if $g \in \mathbb{J}$ then $g = g_0 + \sum g_i x_i + O(\mathbf{m}^2)$. Moreover $g_0 \in (\pi)$ and each g_i lies in (π) since the x_i's map to a *basis* of $\mathbf{m}/(\mathbf{m}^2, \pi)$. Thus $g \in (\mathbf{m}^2, \pi)$. Consequently, it's enough to show what we want for $g \in (\mathbf{m}^2, \pi)$. [This will be important later on!]

But if $g \in (\mathbf{m}^2, \pi)$ then under $\mathcal{O}[\![x]\!]/\mathbb{J} \to \mathcal{O}[\![x]\!]/\mathbb{J}_f$ we still have
$$g = g_0 + \sum g_i x_i + O(\mathbf{m}^2) \mapsto g_0 + \sum g_i(x_i + a_i) + O(\mathbf{m}^2),$$
and the observation is that when we subtract off g from this we get $\sum g_i a_i$ in the $O(\mathbf{m})$ term, which [by inspection] is in $\mathbf{m}\mathbb{J} \subset \mathbb{J}_f$. Similarly one sees that the higher order terms vanish mod $\mathbb{J}_f$.

This concludes the proof of (4), hence the claim, hence the theorem.

1.3. **Completed tensor products.**

Example. Let R be a Noetherian ring, and consider $R[x] \otimes_R R[y] \cong R[x, y]$. However $R[\![x]\!] \otimes_R R[\![y]\!]$ is something weird, being just a part of $R[\![x, y]\!]$. It's easy to see that it does at least inject into $R[\![x, y]\!]$. The idea is that $M \otimes R^I \hookrightarrow M^I$ for any free R-module R^I (here I is an arbitrary index set) but this map fails to be an isomorphism.

To check the injectivity, note that it's OK for M finite free, which allows one to deduce it for M finitely presented, and then pass to a direct limit to conclude the general case. Applying this to $I = \mathbb{Z}$ and $M = R[\![x]\!]$ gives what we want in our case. But to see that our map $R[\![x]\!] \otimes R[\![y]\!] \hookrightarrow R[\![x, y]\!]$ is not surjective, observe that $\sum x^n y^n$ is not in the image!

Definition. Let $\mathcal{O}$ be a complete Noetherian local ring and R, S complete Noetherian local $\mathcal{O}$-algebras (meaning the structure maps are local morphisms). Assume at least one of the residue field extensions $\mathcal{O}/\mathfrak{m}_{\mathcal{O}} \subset R/\mathfrak{m}_R$ and $\mathcal{O}/\mathfrak{m}_{\mathcal{O}} \subset S/\mathfrak{m}_S$ is finite. Then set $\mathfrak{m} \lhd R \otimes_{\mathcal{O}} S$ to be the ideal generated by
$$\mathfrak{m}_R \otimes_{\mathcal{O}} S + R \otimes_{\mathcal{O}} \mathfrak{m}_S.$$
[Note: $(R \otimes_{\mathcal{O}} S)/\mathfrak{m} \cong \Bbbk_R \otimes_{\Bbbk_{\mathcal{O}}} \Bbbk_S$ is not necessarily a field, or even a local ring, but it is artinian.] Now define the completed tensor product $R \widehat{\otimes}_{\mathcal{O}} S$ to be the $\mathfrak{m}$-adic completion of $R \otimes_{\mathcal{O}} S$.

Universal property. $R\widehat{\otimes}_{\mathcal{O}}S$ is the coproduct in the category of complete semilocal Noetherian $\mathcal{O}$-algebras and continuous maps. It is thus the universal (i.e. initial) complete semilocal Noetherian $\mathcal{O}$-algebra equipped with continuous $\mathcal{O}$-algebra maps from R and S.

Example. We have $\mathcal{O}[\![x]\!]\widehat{\otimes}_{\mathcal{O}}\mathcal{O}'[\![y]\!] \cong \mathcal{O}'[\![x,y]\!]$ when $\mathcal{O}'$ is any complete Noetherian local $\mathcal{O}$-algebra. We also have

$$(\mathcal{O}[\![x_1,\dots,x_r]\!]/\mathbb{J})\widehat{\otimes}_{\mathcal{O}}(\mathcal{O}'[\![y_1,\dots,y_s]\!]/\mathbb{J}') \cong \mathcal{O}'[\![x_1,\dots,x_r,y_1,\dots,y_s]\!]/(\mathbb{J},\mathbb{J}')$$

in this setup.

1.4. **Global setup and statement.** Let F be a number field, and p a prime. Let S be a finite set of places of F containing $\{v|p\}$. Fix an algebraic closure $\overline{F}/F$ and let $F_S \subset \overline{F}$ be the maximal extension unramified outside S. Let $G_{F,S} = \mathrm{Gal}(F_S/F)$. Let $\Sigma \subset S$ be any subset of places [for now; later we'll impose conditions].

For $v \in \Sigma$, fix algebraic closures $\overline{F}_v/F_v$ and choose embeddings $\overline{F} \hookrightarrow \overline{F}_v$, or, what is the same thing, choices of decomposition group $\mathrm{Gal}(\overline{F}_v/F_v) = G_v \subset G_{F,S}$. Now let $K/\mathbb{Q}_p$ be a finite extension, and $\mathcal{O}$, π, and k be as above. Fix a character $\psi : G_{F,S} \to \mathcal{O}^\times$.

Let V_k be a finite dimensional continuous representation of $G_{F,S}$ over k such that $\det V_k = \psi \bmod \pi$.

Since we're fixing $\det = \psi$ in this subsection, we'll be dealing (from now on in this talk) with $\mathrm{ad}^0 V_k$ rather than $\mathrm{ad}\, V_k$. [More on this later.] A caution is in order: if $p|\dim V_k$ then $\mathrm{ad}^0 V_k$ is not a direct summand of $\mathrm{ad}\, V_k$. Usually the scalars in $\mathrm{ad}\, V_k$ give a splitting, but when $p|\dim V_k$ the scalars actually sit inside $\mathrm{ad}^0 V_k$. Hence we shall assume from now on that $p \nmid \dim V_k$.

For each $v \in \Sigma$ fix a basis β_v of V_k. We're going to consider deformation functors (and the representing rings) with determinant conditions. Set $D_v^{\square,\psi}$ to be the functor of framed deformations of $V_k|_{G_v}$ with the basis β_v, with fixed determinant $\psi \bmod \pi$, and let $R_v^{\square,\psi}$ be the ring (pro-)representing it. This always exists. Likewise let $D_{F,S}^{\square,\psi}$ be the functor of deformations V_A of V_k with determinant $\psi \bmod \pi$, equipped with an A-basis $\widetilde{\beta}_v$ of V_A lifting β_v for each $v \in \Sigma$. Let $R_{F,S}^{\square,\psi}$ be the ring representing it. Again, this always exists.

We have analogous respective unframed counterparts R_v^ψ and $R_{F,S}^\psi$ under the usual condition that V_k has only scalar endomorphisms as a representation space for G_v and $G_{F,S}$ respectively.

Now *define* $R_\Sigma^{\square,\psi} = \widehat{\bigotimes}_{v\in\Sigma} R_v^{\square,\psi}$ [completed tensor product over $\mathcal{O}$]. Since each $R_v^{\square,\psi}$ has the same residue field, in this case the completed tensor product actually *is* local! Let $\mathfrak{m}_\psi^\square$ be its maximal ideal. Analogously define R_Σ^ψ and $\mathfrak{m}_\Sigma$. Denote the maximal ideal of the local ring $R_{F,S}^{\square,\psi}$ by $\mathfrak{m}_{F,S}^\square$ and likewise that of $R_{F,S}^\psi$ by $\mathfrak{m}_{F,S}$.

There is a natural R_Σ^ψ-algebra structure on $R_{F,S}^\psi$ via the universal property of $\widehat{\otimes}_{\mathcal{O}}$. Indeed, for each $v \in \Sigma$, by restricting the universal deformation of V_k valued in $R_{F,S}^\psi$ to $G_v \subset G_{F,S}$ the universal property of R_v^ψ induces a canonical local $\mathcal{O}$-algebra morphism $R_v^\psi \to R_{F,S}^\psi$. We then use the universal property of completed tensor products.

Theorem. *For $i \geq 1$ let h_Σ^i (resp. c_Σ^i) denote the k-dimension of the kernel (resp. cokernel) of the map*

$$\theta_i : \mathrm{H}^i(G_{F,S}, \mathrm{ad}^0 V_k) \to \prod_{v\in\Sigma} \mathrm{H}^i(G_v, \mathrm{ad}^0 V_k).$$

Then we have an isomorphism of R_Σ^ψ-algebras

$$R_{F,S}^\psi \cong R_\Sigma^\psi[\![x_1,\dots,x_r]\!]/(f_1,\dots,f_{r+s})$$

where $r = h_\Sigma^1$ and $s = c_\Sigma^1 + h_\Sigma^2 - h_\Sigma^1$.

To get the desired presentation, as in the proof of Theorem 1.1, first consider a surjection

$$\mathbb{B} := R_\Sigma^\psi[\![x_1,\dots,x_r]\!] \twoheadrightarrow R_{F,S}^\psi$$

where $r = \dim_k \mathrm{coker}(\mathfrak{m}_\Sigma/(\mathfrak{m}_\Sigma^2,\pi) \to \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2,\pi))$; this surjectivity uses completeness. Dualizing, we have

$$r = \dim_k \ker(\mathrm{Hom}_k(\mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2,\pi),k) \to \mathrm{Hom}_k(\mathfrak{m}_\Sigma/(\mathfrak{m}_\Sigma^2,\pi),k)).$$

Using the computation from Mok's lecture, this is

$$\dim_k \ker\theta_1 = h_\Sigma^1.$$

The key point that makes these computations work is that the completed tensor product represents the product of the functors represented by the R_v^ψ, which is most easily checked by computing on artinian points (for which the completed tensor product collapses to an ordinary tensor product). That then brings us down to the elementary fact that the tangent space of the product of functors is the product of the tangent spaces.

Denote by $\mathbf{m}$ the maximal ideal of $\mathbb{B}$, and by $\mathbb{J}$ the kernel $\ker(\mathbb{B} \twoheadrightarrow R_{F,S}^\psi)$. Now comes a delicate technical point. Like in the proof of Theorem 1.1, we can set-theoretically lift $\rho : G_{F,S} \to \mathrm{GL}_n(R_{F,S}^\psi)$ to $\widetilde{\rho} : G_{F,S} \to \mathrm{GL}_n(\mathbb{B}/\mathbf{m}\mathbb{J})$, not necessarily a homomorphism, and there arises the problem of finding a continuous such $\widetilde{\rho}$. We seek a better method than the trick as earlier with finite residue fields because we wish to later apply the same technique to future situations involving characteristic-0 deformation theory, for which the residue field is a p-adic field and not a finite field. The reader who prefers to ignore this problem should skip the next section.

1.5. **Continuity nonsense.** To explain the difficulty and its solution, let us first formulate a general situation. Consider a surjective map $R' \twoheadrightarrow R$ between complete local noetherian rings with kernel $\mathbb{J}$ killed by $\mathfrak{m}_{R'}$, and assume that we are in one of two cases:

Case 1: residue field k is finite of characteristic p, so R and R' are given the usual max-adic topologies that are profinite. These topologies are the inverse limits of the discrete topologies on artinian quotients.

Case 2 (to come up later!): residue field k is a p-adic field and R and R' are $\mathbb{Q}_p$-algebras, whence uniquely k-algebras in a compatible way (by Hensel). Their artinian quotients are then finite-dimensional as k-vector spaces, and so are naturally topologized as such (making them topological k-algebras, with transition maps that are quotient maps, as for any k-linear surjections between k-vector spaces of finite dimension). Give R and R' the inverse limit of those topologies (which induce the natural k-linear topologies back on the finite-dimensional artinian quotients).

In both cases, let $\rho : G \to \mathrm{GL}_n(R)$ be a continuous representation. We seek to make an obstruction class in a "continuous" $\mathrm{H}^2(G, \mathrm{ad}\,\rho)$ (over k) for measuring whether or not ρ can be lifted to a *continuous* representation into $\mathrm{GL}_n(R')$. The problem is to determine if ρ has a continuous set-theoretic lifting (moreover with with a fixed determinant if we wish to study deformations with a fixed determinant, assuming that p doesn't divide n).

We saw earlier how to handle Case 1 when R is *artinian*, by a trick. That trick rested on ρ at artinian level factoring through a *finite* quotient of G. Such an argument has no chance of applying when k is a p-adic field in interesting cases, and we're sure going to need that later when studying generic fibers of deformation rings and proving smoothness by proving vanishing of a p-adic H^2. So we need an improvement of the method from artinian Case 1 which addresses the following two points:

(i) what to do when k is p-adic,

(ii) how to incorporate additional things like working with a fixed determinant.

Actually, (ii) will be very simple once we see how to deal with (i), as we will see below. This is important because in practice we want to deal with more general constraints than just "fixed determinant" and so we want a general method which works for any "reasonable property", not just something ad hoc for the property of fixed determinant.

To deal with (i) (and along the way, (ii)), we will use a variant on fix from artinian Case 1. That argument allows us to reduce to deal with the case when R and R' are artinian, but we need to show in that *artinian setting* we can make a continuous set-theoretic lifting without the crutch of "factoring through finite quotient of G" (which is available for finite k but not p-adic k).

First conjugate so the reduction $\rho_0 : G \to \mathrm{GL}_n(k)$ lands in $\mathrm{GL}_n(\mathcal{O}_k)$. Then by using the method from Brian's talk on p-adic points of deformation rings, we can find a finite flat local $\mathcal{O}_k$-algebra $\mathcal{O}_k$-lattice A inside of R with residue field equal to that of $\mathcal{O}_k$ and containing the compact $\rho(G)$, and then we can find a similar such A' in R' mapping onto A. We'd like to lift

$$\rho : G \to \mathrm{GL}_n(A)$$

to $\mathrm{GL}_n(A')$ set-theoretically in a continuous way. Note that $\mathrm{GL}_n(A') \to \mathrm{GL}_n(A)$ is surjective.

The point is that $\mathrm{GL}_n(A)$ and $\mathrm{GL}_n(A')$ are respectively open in $\mathrm{GL}_n(R)$ and $\mathrm{GL}_n(R')$ with subspace topologies that arise from the ones on A inside R and A' inside R' which are their natural topologies as finite free $\mathcal{O}_k$-modules. This makes them *profinite*, much as $\mathrm{GL}_n(R)$ and $\mathrm{GL}_n(R')$ were in the case of finite

k. So we have reduced ourselves to the following situation, in which we will use an argument suggested by Lurie that also gives another approach for handling the case of finite k as well.

Let $H' \to H$ be a continuous surjective map of profinite groups, and $\rho : G \to H$ a continuous homomorphism. We claim that there is a continuous set-theoretic lifting $G \to H'$ of ρ that also respects properties like "fixed det" in the case of intended applications. To see this, let $F \twoheadrightarrow G$ be a surjection from a "free profinite group". The composite map

$$F \twoheadrightarrow G \to H$$

can be lifted continuously to $F \to H'$ even as a homomorphism by individually lifting from H to H' the images of each member of the "generating set" for the free profinite F. Those individual lifts can be rigged to have a desired det, or whatever other "reasonable homomorphic property" can be checked pointwise through a surjection, and so such a property is inherited by the map $F \to H'$. But what about $G \to H'$? If we can find a continuous set-theoretic section of $F \twoheadrightarrow G$ then composing that section with $F \to H'$ will give the required $G \to H'$. So our continuity problems will be settled once we prove the following fact.

Claim: If $f : G' \to G$ is a continuous homomorphism between profinite groups then it has a continuous section (as topological spaces).

Proof. For closed normal subgroups $N' \lhd G'$ and $N := f(N')$ = closed normal in G, consider continuous sections $s : G/N \to G'/N'$ to the induced quotient map $G'/N' \to G/N$ arising from f. For example, such an s exists if $N' = G'$ (so $N = G$). If (N', s) and (M', t) are two such pairs with N' containing M', say $(M', t) \geq (N', s)$ if

$$t : G/M \to G'/M' \qquad \textit{and} \qquad s : G/N \to G'/N'$$

are compatible via the projections $G/M \twoheadrightarrow G/N$ and $G'/M' \twoheadrightarrow G'/N'$.

I claim that the criterion for Zorn's Lemma is satisfied. Let $\{(N_i', s_i)\}$ be a chain of such pairs, and let $N' = \bigcap N_i'$. Then the natural map

$$G'/N' \to \varprojlim G'/N_i'$$

is surjective (since an inverse limit of surjections $G'/N' \to G'/N_i'$ between compact Hausdorff spaces), yet also injective and thus a homeomorphism. Likewise, for $N := \bigcap N_i$ the map $G/N \to \varprojlim G/N_i$ a homeomorphism, and I claim that $N = f(N')$. Indeed, if x is in N then $f^{-1}(x)$ meets each N_i' in a non-empty closed set, and these satisfy the finite intersection property since $\{N_i'\}$ is a chain ordered by inclusion, so $f^{-1}(x)$ contains a point in the intersection N' of all N_i'. That says x is in $f(N')$ as desired. (The inclusion of $f(N')$ inside of N is clear.)

It follows that the compatible continuous sections $s_i : G_i/N_i \to G_i'/N_i'$ induced upon passing to the projective limit define a continuous section

$$s : G/N \to G'/N',$$

so (N', s') is an upper bound on the chain $\{(N_i', s_i)\}$.

Now we apply Zorn's Lemma to get a maximal element (N', s). This is a continuous section $s : G/N \to G'/N'$ where $N = f(N')$. I claim $N' = \{1\}$, so we will be done. If not, then since $N' \cap U'$ for open normal subgroups U' in G' define a base of opens in N' around 1 (as N' gets its profinite topology as subspace topology from G'), there must exist such U' so that $N' \cap U'$ is a proper subgroup of N'. Replacing G' with $G'/(N' \cap U')$ and G with quotient by image of $N' \cap U'$ in G brings us to the case where N is finite and *non-trivial* yet (N', s) retains the maximality property (no continuous section using a proper [closed] subgroup of N' normal in G'). We seek a contradiction.

Since N' and N are finite, the quotient maps $q' : G' \twoheadrightarrow G'/N'$ and $q : G \twoheadrightarrow G/N$ are covering spaces with finite constant degree > 0. By total disconnectedness, these covering spaces admit sections. Composing s with a section to q' gives a continuous section $G/N \to G'$ to

$$G' \xrightarrow{f} G \xrightarrow{q} G/N.$$

Composing such a section with q gives a continuous map $t : G \to G'$ so that $f(t(g)) = g \bmod N$, so by profiniteness of G and finiteness of N we get an open normal subgroup U in G such that for each representative g_i of G/U there exists $n_i \in N$ such that $f(t(g_i u)) = n_i g_i u$ for all $u \in U$. But $n_i = f(n_i')$, so replacing t on $g_i U$ with $(n_i')^{-1} t$ for each i gives a new t so that $f(t(g_i u)) = g_i u$ for all $u \in U$ and all i, which is to say $ft = \mathbf{1}_G$. This exhibits a continuous section t to f, contradicting that N was arranged to be nontrivial and maximal with respect to the preceding Zorn's Lemma construction. Hence, in fact N above is $\{1\}$ so we are done. $\square$

1.6. **Proof of Theorem 1.4.** Returning to the situation of interest, we now have a continuous $\widetilde{\rho}$ that can even be arranged to satisfy $\det \widetilde{\rho} \equiv \psi \bmod \mathbf{m}\mathbb{J}$. Still following the argument from the proof of Theorem 1.1, define for $f \in \mathrm{Hom}_k(\mathbb{J}/\mathbf{m}\mathbb{J}, k)$ the continuous 2-cocycle φ_f as before, and observe that this time the determinant condition entails that $[\varphi_f] \in \mathrm{H}^2(G_{F,S}, \mathrm{ad}^0 V_k)$. The proof of the well-definedness of $[\varphi_f]$ is as before. Also we still have the equivalence that $[\varphi_f] = 0$ if and only if $\widetilde{\rho}$ can be chosen to be a homomorphism $\bmod \ker f$.

Now for the restriction of ρ to each G_v, we know we can find a continuous lift, namely coming from the universal representation ρ_v at v:

$$G_v \xrightarrow{\rho_v} \mathrm{GL}_n(R_v^{\psi}) \to \mathrm{GL}_n(R_\Sigma^{\psi}) \to \mathrm{GL}_n(\mathbb{B})$$

where the other maps are the obvious ones. Hence the class $[\varphi_f]|_{G_v} \in \mathrm{H}^2(G_v, \mathrm{ad}^0 V_k)$ is always trivial. In other words, we have a k-linear map $\mathrm{Hom}_k(\mathbb{J}/\mathbf{m}\mathbb{J}, k) \xrightarrow{\Phi} \ker \theta_2$ satisfying $f \mapsto [\varphi_f]$; the target has dimension h^2_Σ by definition. Therefore [easy exercise] it suffices to show that $\dim_k \ker \Phi \leq c^1_\Sigma$. (All we need is the inequality, because we can always throw in extra trivial "relations" $f_i = 0$ into the denominator of $R^{\psi}_{F,S}$.)

Let $I = \ker(\mathfrak{m}_\Sigma/(\mathfrak{m}_\Sigma^2, \pi) \to \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \pi))$. Then $\mathrm{Hom}_k(I, k) \cong \mathrm{coker}(\theta_1)$. So it is enough to construct a linear injection $\ker \Phi \hookrightarrow \mathrm{Hom}_k(I, k)$.

Step 1: Observe that $I = \ker(\mathbf{m}/(\mathbf{m}^2, \pi) \to \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \pi))$ because we chose the x_i's to map onto a basis of $\mathrm{coker}(\mathfrak{m}_\Sigma/(\mathfrak{m}_\Sigma^2, \pi) \to \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \pi))$. (In other words, none of the extra stuff in $\mathbf{m}$ dies when we map to $\mathfrak{m}_{F,S}$.)

Step 2: We next claim that $\mathbb{J}/\mathbf{m}\mathbb{J}$ surjects onto I. To prove this, first note that the map $\mathbb{J}/\mathbf{m}\mathbb{J} \to \mathbf{m}/(\mathbf{m}^2, \pi)$ comes from tensoring

$$0 \to \mathbb{J} \to \mathbf{m} \to \mathfrak{m}_{F,S} \to 0$$

over $\mathbb{B}$ with $\mathbb{B}/\mathbf{m}$ and then reducing mod π. We need to show that this map is surjective onto I. Fix $x \in I \subset \mathbf{m}/(\mathbf{m}^2, \pi)$. We know

$$\mathbb{J}/\mathbf{m}\mathbb{J} \twoheadrightarrow \ker(\mathbf{m}/\mathbf{m}^2 \to \mathfrak{m}_{F,S}/\mathfrak{m}_{F,S}^2).$$

We can lift x to $\widetilde{x} \in \mathbf{m}/\mathbf{m}^2$. Since x maps to zero in $\mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \pi)$, $\widetilde{x}$ maps to $\pi r \bmod \mathfrak{m}_{F,S}^2$ for some $r \in R^{\psi}_{F,S}$. But now we can just choose some $\widetilde{r} \in \mathbb{B}$ mapping to $r \in R^{\psi}_{F,S}$ (i.e. mod $\mathbb{J}$). Now replace $\widetilde{x}$ with $\widetilde{x} - (\pi \widetilde{r} \bmod \mathfrak{m}^2)$ so that $\widetilde{x}$ has vanishing image in $\mathfrak{m}_{F,S}/\mathfrak{m}_{F,S}^2$. That says $\widetilde{x}$ is in the image of $\mathbb{J}/\mathfrak{m}\mathbb{J}$ in $\mathfrak{m}/\mathfrak{m}^2$, so x is hit by $\mathbb{J}/\mathfrak{m}\mathbb{J}$ as desired.

Step 3: By Step 2 we get $\mathrm{Hom}_k(I, k) \hookrightarrow \mathrm{Hom}_k(\mathbb{J}/\mathbf{m}\mathbb{J}, k) \supset \ker \Phi$. So we need to show that $\ker \Phi \subset \mathrm{Hom}_k(I, k)$. In other words, if $[\varphi_f] = 0$ then we claim that $f : \mathbb{J}/\mathbf{m}\mathbb{J} \to k$ should factor through I, or equivalently vanish on $K = \ker(\mathbb{J}/\mathbf{m}\mathbb{J} \twoheadrightarrow I)$. Or equivalently, we need to show that $K = \mathbb{J} \cap (\mathbf{m}^2, \pi) \subset \mathbb{J}_f = \ker f$. But in fact this is really what we showed at the end of the proof of Theorem 1.1 when we showed property (4) of Φ.

1.7. **The framed case.** Let

$$\eta : \mathfrak{m}_\Sigma^\square/((\mathfrak{m}_\Sigma^\square)^2, \pi) \to \mathfrak{m}_{F,S}^\square/((\mathfrak{m}_{F,S}^\square)^2, \pi).$$

Then

$$R^{\square,\psi}_{F,S} \cong R^{\square,\psi}_\Sigma[\![x_1, \ldots, x_{r^\square}]\!]/(f_1, \ldots, f_{r^\square + s^\square}),$$

where $r^\square = \dim_k \mathrm{coker}\, \eta$ and $r^\square + s^\square = h^2_\Sigma + \dim_k \ker \eta$.

The proof is the same as in the unframed case, just with extra squares floating around all over the place. But now our H's have turned into Z's (that is, elements of the tangent space which were cohomology classes are now cocycles) so it's better to phrase the result as above.

1.8. **Formulas for r's and s's.**

Theorem. *Suppose that $\{v|p\} \subset \Sigma$, that $\{v|\infty\} \subset S$, and that $S - \Sigma$ contains at least one finite prime. Then (with notation as above)*

$$s = \sum_{v|\infty, v \notin \Sigma} \dim_k (\mathrm{ad}^0 V_k)^{G_v}.$$

Remark. We also have $r^{\square} \geq \#\Sigma - 1, r^{\square} \stackrel{?}{=} r + \#\Sigma - 1, s^{\square} = s - \#\Sigma + 1$.

Proof. Let $Y = \mathrm{ad}^0 V_k$ and $X = Y^{\vee}(1)$. (In the notation of Rebecca's talk, $X = Y'$; it is written as a "twisted Pontrjagin dual" here because instead of being Hom into $\mathbb{Q}/\mathbb{Z}$ (trivial G-module) the target is given the action of the cyclotomic character.) Recall the end of the Poitou-Tate exact sequence (from Rebecca's talk)

$$\mathrm{H}^2(G_{F,S}, Y) \to \prod_{v \in S} \mathrm{H}^2(G_v, Y) \to \mathrm{H}^0(G_{F,S}, X)^{\vee} \to 0.$$

Split the product into two pieces:

$$\prod_{v \in S} \mathrm{H}^2(G_v, Y) = \prod_{v \in \Sigma} \mathrm{H}^2(G_v, Y) \times \prod_{v \in S - \Sigma} \mathrm{H}^2(G_v, Y).$$

The claim is that as long as the second factor is nonzero (which it is by hypothesis), it surjects onto $\mathrm{H}^0(G_{F,S}, X)^{\vee}$. Indeed, trivially $\mathrm{H}^0(G_{F,S}, X) \hookrightarrow \mathrm{H}^0(G_v, X)$ since restricting to the decomposition group gives more invariants. Dually, we have $\mathrm{H}^0(G_v, X)^{\vee} \twoheadrightarrow \mathrm{H}^0(G_{F,S}, X)^{\vee}$. But by the Tate pairing, $\mathrm{H}^0(G_v, X)^{\vee} \cong \mathrm{H}^2(G_v, Y)$. On each factor, the last map in the Tate-Poitou sequence is none other than the composition $\mathrm{H}^2(G_v, Y) \cong \mathrm{H}^0(G_v, X)^{\vee} \twoheadrightarrow \mathrm{H}^0(G_{F,S}, X)^{\vee}$. Thus the claim is true.

Now we do a little diagram chase. We have

$$\mathrm{H}^2(G_{F,S}, Y) \to \prod_{v \in \Sigma} \mathrm{H}^2(G_v, Y) \times \prod_{v \in S - \Sigma} \mathrm{H}^2(G_v, Y) \to \mathrm{H}^2(G_{F,S}, X)^{\vee} \to 0.$$

The claim is that $\mathrm{H}^2(G_{F,S}, Y) \twoheadrightarrow \prod_{v \in \Sigma} \mathrm{H}^2(G_v, Y)$. Indeed, given $(a_v)_{\Sigma} \in \prod_{v \in \Sigma} \mathrm{H}^2(G_v, Y)$, suppose its image in $\mathrm{H}^2(G_{F,S}, X)^{\vee}$ is γ. Since $\prod_{v \in S - \Sigma} \mathrm{H}^2(G_v, Y) \twoheadrightarrow \mathrm{H}^2(G_{F,S}, X)^{\vee}$, we can find

$$(b_v)_{S - \Sigma} \in \prod_{v \in S - \Sigma} \mathrm{H}^2(G_v, Y)$$

such that the image of $(b_v)_{S - \Sigma}$ in $\mathrm{H}^2(G_{F,S}, X)^{\vee}$ is $-\gamma$. Then

$$(a_v)_{\Sigma} \times (b_v)_{S - \Sigma} \in \ker(\prod_{S} \mathrm{H}^2(G_v, Y) \twoheadrightarrow \mathrm{H}^2(G_{F,S}, X)^{\vee}),$$

whence this tuple is in the image of $\mathrm{H}^2(G_{F,S}, Y)$. Projecting onto the $\prod_{v \in \Sigma}$ factor proves the claim. But the surjectivity of $\mathrm{H}^2(G_{F,S}, Y) \twoheadrightarrow \prod_{v \in \Sigma} \mathrm{H}^2(G_v, Y)$ says precisely that $c^2_{\Sigma} = \dim \operatorname{coker} \theta_2 = 0$.

Consequently we have $h^2_{\Sigma} = h^2(G_{F,S}, Y) - \sum_{v \in \Sigma} h^2(G_v, Y)$. So by the formulas at the end of Theorem 1.4,

$$s = -h^1_{\Sigma} + c^1_{\Sigma} + h^2_{\Sigma} = -h^1(G_{F,S}, Y) + \sum_{v \in \Sigma} h^2(G_v, Y) + h^2(G_{F,S}, Y) - \sum_{v \in \Sigma} h^2(G_v, Y).$$

Now recall that we have assumed throughout that $\mathrm{End}_{G_{F,S}} V_k = (\mathrm{ad}\, V_k)^{G_{F,S}} = k$ (since we need this to make sure the unframed deformation ring even exists!). In particular, $(\mathrm{ad}^0 V_k)^{G_{F,S}} = 0$. That is, $h^0(G_{F,S}, Y) = h^0(G_v, Y) = 0$. So we can add $h^0(G_{F,S}, Y) - \sum_{v \in \Sigma} h^0(G_v, Y)$ to s and nothing changes. But now we recognize from the equation above that in fact $s = \chi(G_{F,S}, Y) - \sum_{v \in \Sigma} \chi(G_v, Y)$.

We now invoke the Tate global Euler characteristic formula. [Reference: Milne, *Arithmetic Duality Theorems* Ch. I, Thm. 5.1.] We conclude that

$$\chi(G_{F,S}, Y) = \sum_{v | \infty} h^0(G_v, Y) - [F : \mathbb{Q}] \dim_k Y.$$

We also have for $v < \infty, v \nmid p$, that $\chi(G_v, Y) = 0$. For $v < \infty, v | p$, we have $\chi(G_v, Y) = -[F_v : \mathbb{Q}_p] \dim_k Y$. For $v | \infty$, we have $\chi(G_v, Y) = h^0(G_v, Y)$. One sees that in $s = \chi(G_{F,S}, Y) - \sum_{v \in \Sigma} \chi(G_v, Y)$, the degree contributions all cancel out, so there are no non-archimedean terms. Of the archimedean places, all those in Σ cancel as well, and we are left with the statement of the theorem. $\square$