Lecture 2: Serre's conjecture and more

Akshay
October 9, 2009
Notes by Sam Lichtenstein

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

$$k(\overline{\rho}) := \begin{cases} 1+pa+b & \text{“most of the time”} \\ 1+pa+b+p-1 & \text{...} \end{cases}$$

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 $0 \leq a \leq b$, 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*]

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

[*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 $\mathbb{Z}$.

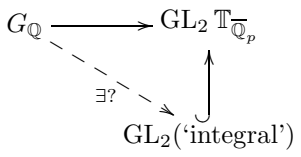
Proof. One approach is to show that $\mathbb{T}$ preserves a lattice in V, by using the arithmetic theory of modular curves (with models over $\mathbb{Z}$). An alternative which is easier to carry out rigorously and involves just topological/analytic tools is to embed V into $\mathrm{H}^1(X_0(N), \mathbb{C})$ 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 $\operatorname{Spec}\mathbb{T}$ lying over $\operatorname{Spec}\mathbb{Z}$ has two irreducible components,

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

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

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

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 $\operatorname{tr}(yx_j)$ 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.)