Carayol's theorem.

Let A be a complete noetherian local ring with maximal ideal $\mathfrak{m}$ such that $k = A/\mathfrak{m}$ is a finite field. We consider a continuous representation of a Galois group Γ (local or global) with values in a semilocal extension A' of A. Thus $A' = \prod A'_i$ where each A'_i is local with maximal ideal $\mathfrak{m}_i$ and residue field k'_i, an extension of k, and we have a continuous map

$$\rho' : \Gamma \rightarrow GL(n, A') = \prod_i GL(n, A'_i)$$

that defines a continuous map of A-algebras

$$\prod \rho'_i : R = A[\Gamma] \rightarrow \prod_i M(n, A'_i).$$

By linearity this extends to a map of A'-algebras

$$\prod \rho'_i : R' = A'[\Gamma] \rightarrow \prod_i M(n, A'_i) = M(n, A').$$

We make the following

Hypothesis 1. *For all $\gamma \in \Gamma$, the trace $tr(\gamma) \in A'$ in fact belongs to the subring A.*

In particular, for each i, the residual representation

$$\bar{\rho}'_i : k'_i[\Gamma] \rightarrow M(n, k'_i)$$

has the property that $tr(\rho'_i(\gamma)) \in k$ and in particular $\chi_i(\gamma) = tr(\rho'_i(\gamma))$ is independent of i for all $\gamma \in \Gamma$.

Hypothesis 2. *For some i, $\bar{\rho}'_i$ is absolutely irreducible.*

We will see in the corollary to Theorem 2 below that this implies that all the $\bar{\rho}'_i$ are absolutely irreducible.

Theorem 1. *Under Hypotheses 1 and 2, there exists a representation $\rho : \Gamma \rightarrow GL(n, A)$ such that ρ' is equivalent to $\rho \otimes A'$. Moreover, ρ is unique up to equivalence.*

It is explained in Carayol's article [C] that several of these hypotheses are unnecessary. In particular, it is enough that A be henselian. But in the applications, we will assume A complete.

As a necessary first step, we prove

Theorem 2. *Let ρ, ρ' be two representations of Γ with coefficients in A. Suppose $\bar{\rho}$ is absolutely irreducible and $tr(\rho) = tr(\rho')$ as functions on Γ. Then ρ and ρ' are equivalent.*

Proof. We first prove that $\bar{\rho}$ and $\bar{\rho}'$ are equivalent. It suffices by general principles (Hilbert's Theorem 90) to prove this after passage to the algebraic closure of k, so we may assume k algebraically closed. If k is of characteristic zero, then $\bar{\rho}$ is determined by its trace, and the claim is clear. If $char(k) = p > 0$, we need to use that the traces of distinct irreducible representations of $R \otimes k$ are linearly independent functions on R (cf. Curtis-Reiner, (27.8)). Now $\bar{\rho}'$ is not necessarily semisimple, but its semisimplification $(\bar{\rho}')^{ss}$ can be written as a finite sum $\oplus n_\pi \pi$ where the π are irreducible and mutually distinct. It follows from equality of traces that $n_{\bar{\rho}} \equiv 1 \pmod p$ and $n_\pi \equiv 0 \pmod p$ for $\pi \neq \bar{\rho}$. But $\dim \bar{\rho} = \dim \bar{\rho}'$ which means that there is no room for any more than a single copy of $\bar{\rho}$ in $(\bar{\rho}')^{ss}$.

Now we replace A by $A_d = A/\mathfrak{m}^{d+1}$, $d = 0, 1, 2, \ldots$, and we show by induction that $\rho_d = \rho \pmod{\mathfrak{m}^d}$ is equivalent to ρ'_d for all d. We have already shown this for $d = 0$; suppose we know it for $d - 1$. Thus, after conjugating by an appropriate element of $GL(n, A)$, we may assume that

$$\rho(r) \equiv \rho'(r) \pmod{\mathfrak{m}^d}, \forall r \in R.$$

Thus

$$\rho'_d(r) \equiv \rho_d(r) + \delta(r), \; \delta(r) \in M(n, \mathfrak{m}^d/\mathfrak{m}^{d+1}).$$

It is clear that δ is A-linear, hence factors through $R \otimes_A k = \bar{R}$. Since ρ'_d and ρ_d are homomorphisms, one checks that the map δ satisfies

$$\delta(r_1 r_2) = \bar{\rho}(r_1)\delta(r_2) + \delta(r_1)\bar{\rho}(r_2).$$

Moreover, since $tr(\rho) = tr(\rho')$, we know that $tr \circ \delta$ vanishes identically.

Take $Y \in \ker(\bar{\rho})$, $r \in \bar{R}$. We have

$$\delta(rY) = \bar{\rho}(r)\delta(Y)$$

and since the kernel is an ideal in R, $tr(\bar{\rho}(r)\delta(Y)) = 0$. Now we apply Burnside's theorem: since $\bar{\rho}$ is absolutely irreducible, $\bar{\rho} : \bar{R} \rightarrow M(n, k)$ is *surjective*. It follows that for all $X \in M(n, k)$, $tr(X\delta(Y)) = 0$, hence $\delta(Y) = 0 \forall Y \in \ker(\bar{\rho})$. Thus δ factors through a derivation

$$d : \bar{R}/\ker(\bar{\rho}) = M(n, k) \rightarrow M(n, \mathfrak{m}^d/\mathfrak{m}^{d+1}) = M(n, k)^a$$

where $a = \dim_k \mathfrak{m}^d/\mathfrak{m}^{d+1}$. In other words, δ is a sum of derivations from $M(n, k)$ to itself. Now it is known that any derivation of $M(n, k)$ is inner, i.e. there exists a matrix $U \in M(n, \mathfrak{m}^d/\mathfrak{m}^{d+1})$ such that

$$\delta(r) = \bar{\rho}(r)U - U(\bar{\rho}(r)), \forall r \in R.$$

Hence

$$\begin{aligned} \rho'_d(r) &= \rho_d(r) + \bar{\rho}(r)(U) - U\bar{\rho}(r) \\ &= (1 - U)\rho_d(r)(1 + U) \end{aligned}$$

Here $\bar{\rho}$ is not well-defined in $M(n, A_d)$ but its product with U is, and indeed

$$U\rho_d(r) = U\bar{\rho}(r)$$

depends only on $\bar{\rho}(r)$. Thus ρ_d and ρ'_d are equivalent for all d by induction. By continuity, this implies that there is a convergent sequence of matrices $M_d \in GL(n, A)$ such that, if $M = \lim_d M_d$ then

$$\rho'(r) = M\rho(r)M^{-1}$$

for all $r \in R$.

Corollary. *Under Hypothesis 2, all $\bar{\rho}'_i$ are absolutely irreducible and equivalent when the k'_i are embedded in a common field.*

Proof of Theorem 1. Let $S' = M(n, A') = \prod_i M(n, A'_i)$ and let $S = \rho(R) \subset S'$. Thus for all $s \in S$, $Tr(s) \in A$.

Now for each i, $\bar{\rho}'_i : k'_i[\Gamma] \to M(n, k'_i)$ is surjective by Burnside's theorem. Since $\bar{\rho}'_i$ is deduced from a map of $k[\Gamma]$, it follows that there exists a sequence $r_1, \ldots, r_n$ of elements of R such that, for each i, the $\bar{\rho}'_i(r_j \otimes 1)$ form a k'_i-basis of $M(n, k'_i)$. Let $e_j = \rho'(r_j \otimes 1)$. By Nakayama's Lemma, the projections of e_j on each $S'_i = M(n, A'_i)$ forms a system of generators of the free module S'_i, and by comparing ranks we see they even form a basis.

I claim the e_j form a basis of S as A-module. Indeed, for any $s \in S$, we can write $s = \sum \alpha_j e_j$ with $\alpha_j \in A'$. Now for any $1 \leq \ell \leq n^2$,

$$(*) \qquad tr(s \cdot e_\ell) = \sum_j \alpha_j tr(e_j e_\ell) \in A.$$

Now for any basis e_j of a matrix algebra, the determinant of the matrix $tr(e_j e_\ell)$ is invertible. (This is clear over a field, the trace being a non-degenerate bilinear form, and so it follows easily over a semilocal ring.) Now the matrix $tr(e_j e_\ell)$ is invertible over A' but it has coefficients in A, hence the inverse also has coefficients in A. The system of equations (*) for α_j thus can be inverted to show that $\alpha_j \in A$ for all j. This proves the claim.

Now S is a free A-module of rank n^2, and the isomorphism $S \otimes_A A' \xrightarrow{\sim} S'$ induces isomoprhisms for each i:

$$(S \otimes_A k) \otimes_k k'_i \xrightarrow{\sim} S' \otimes_{A'_i} k'_i = M(n, k'_i).$$

Hence $\bar{S} = S \otimes_A k$ is a central simple algebra over k. Thus S is an Azumaya algebra over A, i.e. a twisted matrix algebra.

But since A is Henselian, any Azumaya algebra over A is determined by its reduction mod $\mathfrak{m}$. Since k is finite, the only central simple algebras over k are the matrix algebras. Thus there exists an isomorphism

$$\phi : S \xrightarrow{\sim} M(n, A).$$

Now define $\rho(r) = \phi(\rho'(r \otimes 1)$. This defines a representation of Γ with coefficients in A. It remains to show that $\rho \otimes_A A'$ is equivalent to ρ'. But consider

$$M(n, A') = S' = S \otimes_A A' \xrightarrow{\phi \otimes 1} M(n, A').$$

This is an automorphism of $M(n, A')$, and any automorphism of $M(n, A')$ is inner (because $M(n, A') = \prod M(n, A'_i)$ and this is true for any local ring), say is given by conjugation by a matrix $\beta \in M(n, A')$. This conjugation defines the desired equivalence.

Applications to deformation rings.

I follow the article of de Smit and Lenstra [dS-L] that proves a more general version of Mazur's theorem on existence of deformation rings without appealing to Schlessinger's criterion. The next few paragraphs are copied from the lecture on Schlessinger's theorem, to which I refer as [Sch].

In what follows, G is either (i) $Gal(K_S/K)$, where K is a number field, S is a finite set of places of K, and K_S is the maximal extension of K unramified outside S, or (ii) $Gal(\bar{K}/K)$, where K is a p-adic field. In case (i), if L is a finite extension of K, let L_S be the maximal extension of L unramified outside the primes of L above S. Let $\mathcal{O}$ be an ℓ-adic integer ring with finite residue field k. We let $\mathcal{C} = \mathcal{O}$ be the category of artinian local $\mathcal{O}$-algebras with residue field k (such that the structure map $\mathcal{O} \mapsto A$ induces the identity map on residue fields), and $\hat{\mathcal{C}}$ the category of complete noetherian local $\mathcal{O}$-algebras with residue field k as above.

Lemma 1. *For any finite extension L/K, let $G_L = Gal(L_S/L)$ in case (i), resp. $G_L = Gal(\bar{K}/L)$ in case (ii). Then $Hom(G_L, k)$ is a finite set.*

The proof is in [Sch].

Now let $\bar{r} : G \rightarrow GL(n,k)$ be a finite-dimensional representation. For A in $\mathcal{C}$, a *lifting* of $\bar{r}$ to A is a homomorphism

$$\rho : G \rightarrow GL(n,A); \rho = \bar{r} \pmod{\mathfrak{m}_A}.$$

For all N, let $\Gamma(\mathfrak{m}_A^N)$ be the principal congruence subgroup of $GL(n,A)$:

$$\Gamma(\mathfrak{m}_A^N) = \{\gamma \in GL(n,A) \mid \gamma \equiv 1 \pmod{\mathfrak{m}_A^N}\}.$$

A *deformation* of $\bar{r}$ to A is an equivalence class of liftings ρ, where ρ_1 and ρ_2 are equivalent if there exists a matrix $\gamma \in GL(n,A)$, with $\gamma \in \Gamma(\mathfrak{m}_A)$, such that $\rho_2 = \gamma \circ \rho_1 \circ \gamma^{-1}$. Define the functor $Def(\bar{r})$ on $\hat{\mathcal{C}}$ for which $Def(\bar{r})(A)$ is the set of deformations of $\bar{r}$ to A.

The functor of liftings is more or less obviously prorepresentable by some sort of ring (take generators and relations). Here is the construction, following [dS-L]. First let G' be a finite quotient of G. Let $\mathcal{O}[G,n]$ be the commutative $\mathcal{O}$-algebra with generators $X^g_{i,j}, g \in G', 1 \leq i,j, \leq n$ and relations

$$X^e_{i,j} = \delta_{ij};\ X^{gh}_{i,j} = \sum_{k=1}^{n} X^g_{ik} X^h_{kj}.$$

This is just the ring of coordinates of homomorphisms from G' to $GL(n)$; more precisely, there is an obvious canonical bijection

$$Hom_{\mathcal{O}}(\mathcal{O}[G,n], A) \xrightarrow{\sim} Hom(G, GL(n,A))$$

for any $\mathcal{O}$-algebra A. In particular, $\bar{r}$ corresponds to a homomorphism from $\mathcal{O}[G,n]$ to the finite field k, whose kernel is a maximal ideal $m_{\bar{r}}$, and we let R_b denote the completion of $\mathcal{O}[G,n]$ at $m_{\bar{r}}$. Then R_b is an object in $\hat{\mathcal{C}}$, and

Lemma 2. *The natural map*

$$Hom_{\hat{\mathcal{C}}}(R_b, A) \rightarrow Hom_{\bar{r}}(G, GL(n,A))$$

is a bijection for any A in $\hat{C}$.

Here $Hom_{\bar{r}}$ means continuous liftings of $\bar{r}$. Given a lift ρ on the right, it defines a map from $\mathcal{O}[G,n]$ that obviously extends to a map $f = f_\rho$ of completions at $m_{\bar{r}}$

and $\mathfrak{m}_A$ respectively, but A is already complete at $\mathfrak{m}_A$. Since the elements $X^g_{i,j}$ are dense in R_b and their images under f are determined by ρ, this shows that f is unique. The identification in the other direction is just as easy.

Now if we write $G = \varprojlim G_i$ with G_i finite, we get rings $R_{b,i}$ as above in $\hat{\mathcal{C}}$, with maps between them corresponding to maps between the G_i, and let $R_b = \varprojlim R_{b,i}$. This is not necessarily in $\hat{\mathcal{C}}$, in particular it is not obviously noetherian. We can fix this. Let $H = \ker(\bar{r})$, $G' = G/H$, which is a finite quotient of G. Obviously R_b is a finite R_b^H-algebra. If we can show R_b^H is noetherian, then it follows that so is R_b. So we may replace G by H and assume $\bar{r}$ is trivial. Now in [Sch] I prove that

$$t_{R_b} \xrightarrow{\sim} H^1(H, Ad(\rho)) = Hom(H, k) \otimes Ad(\rho)$$

which is finite-dimensional by Lemma 1. On the other hand,

$$\begin{aligned} t_{R_b} = Hom_{cont}(R_b, k[\varepsilon]) &= \varinjlim_i Hom_{\mathcal{O}}(R_{b,i}, k[\varepsilon]) \\ &= \varinjlim_i Hom_k(m_i/(m_i^2 + \mathfrak{m}R_{b,i}, k) \end{aligned}$$

where m_i is the maximal ideal of $R_{b,i}$ and $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$. Moreover, the transition maps in the inductive limit are injective. So it follows that $\dim(m_i/m_i^2)$ is bounded. Now it is easy to show (cf. [dS-L], (5.3)) that this boundedness implies that R_b is noetherian as well as a complete local $\mathcal{O}$-algebra.

We now apply a variant of Carayol's theorem. Let ρ_b be the universal lifting of $\bar{r}$ over R_b, and let $R \subset R_b$ be the closed subring generated by $Tr(\rho_b)(g)$. In [dS-L] it is proved that, as long as $\bar{r}$ is irreducible, then ρ_b is obtained from a representation of G on a free R-module of rank n. The proof is elementary and does not require that R or R_b be noetherian, only that they are both projective limits of Artin algebras; k does not even have to be finite. Admitting this result, let $A \in \mathcal{C}$ and ρ_A be a lift of $\bar{r}$ to A, i.e. $\rho_A \in Hom_{\bar{r}}(G, GL(n, A))$. Thus there is a map $f_b : R_b \to A$ classifying ρ_A in the sense that $\rho_A = f_b \circ \rho_b$. But $\rho_b = \rho \otimes_R R_b$, so $\rho_A = f \circ \rho$ where f is the restriction of f_b to R. Now it suffices to show that f is uniquely determined by ρ_A up to isomorphism. But $Tr(\rho_A)(g) = f(Tr(\rho)(g))$ for all $g \in G$. Of course $Tr(\rho_A)(g)$ is determined by the equivalence class of ρ_A, so the elements $f(Tr(\rho)(g) \in A$ are determined by the equivalence class of ρ_A. Since the traces are dense in R and f is continuous, it follows that f is determined uniquely by the equivalence class of ρ_A, and this proves that (R, ρ) represents $Def_{\bar{r}}$ on $\mathcal{C}$.

A slightly more complicated proof, due to Faltings, shows that this works (for a slightly bigger R) provided $End_G(\bar{r}) = k$, which is possible even if $\bar{r}$ is reducible.

[C] H. Carayol, Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet, *Contemp. Math.*, **165** (1994) 213-237.

[dS-L] B. de Smit and H.W. Lenstra, Jr., Explicit construction of universal deformation rings, in G. Cornell, J. Silverman, and G. Stevens, eds. *Modular Forms and Fermat's Last Theorem*, Springer-Verlag (1997), 313-326.