AN IRREDUCIBILITY CRITERION FOR GROUP REPRESENTATIONS, WITH ARITHMETIC APPLICATIONS

MATTEO LONGO AND STEFANO VIGNI

ABSTRACT. We prove a criterion for the irreducibility of an integral group representation ρ over the fraction field of a noetherian domain R in terms of suitably defined reductions of ρ at prime ideals of R. As applications, we give irreducibility results for universal deformations of residual representations, with a special attention to universal deformations of residual Galois representations associated with modular forms of weight at least 2.

1. INTRODUCTION

Let G be a group, let R be a noetherian integral domain with fraction field K and consider a representation

$$\rho_K \colon G \longrightarrow \mathrm{GL}_d(K)$$

of G over K. A classical problem in representation theory is to find suitable conditions under which ρ_K is integral over R, i.e., under which there exists a representation

$$\rho_R \colon G \longrightarrow \mathrm{GL}_d(R)$$

of G over R which is equivalent (i.e., conjugated) to ρ_K. If this is the case, one says that ρ_K can be *realized over* R via ρ_R (see §2.1 for more precise definitions). At least when the group G is finite and the ring R is a Dedekind domain (which we do not require), dealing with this and related questions amounts to studying R-orders and lattices in non-commutative K-algebras (see, e.g., [4, Ch. 3]). Here we propose to tackle a different problem: we assume that ρ_K can be realized over R via a representation ρ_R as above and we look for properties of ρ_R which guarantee that ρ_K is irreducible.

More precisely, in §2.2 we define reductions $\bar{\rho}_{\mathfrak{p}}$ of ρ_R at prime ideals $\mathfrak{p}$ of R; these are representations of G over the residue fields of the localizations of R at the primes $\mathfrak{p}$, and our goal is to relate the irreducibility of the $\bar{\rho}_{\mathfrak{p}}$ to that of ρ_K. As a motivation, consider the toy case in which R is a discrete valuation ring with maximal ideal $\mathfrak{m}$: in this situation it is easy to see (essentially by applying Nakayama's lemma) that ρ_K is irreducible if $\bar{\rho}_{\mathfrak{m}}$ is.

Of course, in the general setting where R is allowed to be an arbitrary noetherian domain one expects extra complications to arise. Nevertheless, the main result of this note (Theorem 3.3) shows that a criterion of this sort is still valid; in fact, we can prove

Theorem 1.1. *If $\bar\rho_{\mathfrak{p}}$ is irreducible for a set of prime ideals $\mathfrak{p}$ of R with trivial intersection then ρ_K is irreducible.*

It is worthwhile to remark that the group G is *arbitrary* (in particular, it need not be finite). This result has a number of consequences (cf. §3.2 and §3.3). As an example, in Theorem 3.8 we extend the implication recalled above for discrete valuation rings to a much larger class of local domains; namely, we prove that if R is a regular local ring with maximal ideal $\mathfrak{m}$ then ρ_K is irreducible if $\bar\rho_{\mathfrak{m}}$ is.

Section 4 ends the paper with applications of our algebraic results to arithmetic contexts. In particular, in §4.1 we deal with deformations of residual representations in the sense of Mazur ([8]) and prove that an irreducible residual representation admits irreducible universal deformations when the deformation problem for it is unobstructed (see Proposition 4.5 for an accurate statement). Finally, in §4.2 we specialize this irreducibility result to the case of residual modular Galois representations. In this setting, using results of Weston ([11]), we show that if f is a newform and K_f is the number field generated by its Fourier coefficients then for infinitely many (in a strong sense) primes λ of K_f the residual Galois representation $\bar\rho_{f,\lambda}$ attached by Deligne to f and λ has irreducible universal deformation (see Proposition 4.7 for a precise formulation).

2. Representations over lattices and reductions

In this section we review the basic definitions concerning integral group representations and their reductions modulo prime ideals.

2.1. **Terminology and auxiliary results.** As in the introduction, let R be a noetherian domain with fraction field K and let G be a group. Let V be a vector space over K of dimension $d \geq 1$ and let

$$(1) \qquad\qquad \rho_V \colon G \longrightarrow \mathrm{Aut}_K(V) \simeq \mathrm{GL}_d(K)$$

be a representation of G in the K-vector space of K-linear automorphisms of V. If L is an R-submodule of V write KL for the K-subspace of V generated by L.

Definition 2.1. An *R-lattice* (or simply a *lattice*) of V is a finitely generated R-submodule L of V such that $KL = V$.

In other words, the lattice L is a finitely generated R-submodule of V which contains a basis of V over K.

Remark 2.2. 1) It can be shown (see [2, Ch. VII, §4.1]) that if L is an R-lattice of V then there exists a free R-submodule of L of rank d.

2) If the group G is finite then G-stable lattices in V always exist. However, such lattices are not necessarily free over R (see, e.g., [10, p. 550]).

If the lattice L is stable for the action of G (i.e., is a left $R[G]$-module) then we can define a representation

$$\rho_L \colon G \longrightarrow \mathrm{Aut}_R(L)$$

of G in the R-module of R-linear automorphisms of L. More generally, if A is any R-algebra (with trivial G-action) we can consider the representation

$$\rho_{L,A} \colon G \longrightarrow \mathrm{Aut}_A(L \otimes_R A)$$

of G in the A-module of A-linear automorphisms of $L \otimes_R A$ which is obtained by extending ρ_L by A-linearity.

Now we can give the following important

Definition 2.3. The representation ρ_V is *integral over R* if there exists a G-stable lattice L of V. If this is the case then the isomorphism $L \otimes_R K \simeq V$ is G-equivariant and we say that V can be *realized over L*.

Notice that, in light of part 1) of Remark 2.2, assuming the lattice L to be free over R is not too serious a restriction; in fact, in order not to burden our exposition with unenlightening technicalities, the main results of this paper will be proved under this condition.

To avoid ambiguities, we recall some standard terminology. The representation ρ_V is said to be *irreducible* if the only K-subspaces of V which are invariant for G under ρ_V are $\{0\}$ and V; if ρ_V is understood, we also say that the left $K[G]$-module V is *irreducible*. More generally, a left $R[G]$-module L which is finitely generated over R is said to be *irreducible* if L does not contain any (necessarily finitely generated, since R is noetherian) R-submodule M which is G-stable and such that KM is neither trivial nor equal to KL; in this case, we also say that the representation ρ_L defined as above is *irreducible*.

Proposition 2.4. *With notation as before, let ρ_V be realized over L. Then ρ_V is irreducible if and only if ρ_L is.*

Proof. Assume first that ρ_V is irreducible and let M be a finitely generated R-submodule of V which is G-stable. The K-subspace KM is then a $K[G]$-submodule of V, so it must be either trivial or equal to V, hence ρ_L is irreducible. Conversely, suppose that ρ_L is irreducible. If ρ_V were not irreducible then we could find a $K[G]$-submodule W of V such that $W \neq \{0\}$ and $W \neq V$.

Set $M := L \cap W$. Then M is a finitely generated R-submodule of L (because R is noetherian) which is G-stable and such that

$$KM = (KL) \cap W = V \cap W = W,$$

which contradicts the irreducibility of ρ_L. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Proposition 2.4 makes it possible to study the irreducibility of ρ_V in terms of that of ρ_L, and this will be the underlying theme of the rest of the paper.

2.2. **Reductions modulo prime ideals.** From now on let ρ_V be a representation of the group G which is realized over the lattice L. For any prime ideal $\mathfrak{p}$ of R write $R_{\mathfrak{p}}$ for the localization of R at $\mathfrak{p}$ and let

$$k_{\mathfrak{p}} := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}, \qquad \pi_{\mathfrak{p}} : R_{\mathfrak{p}} \longrightarrow k_{\mathfrak{p}}$$

be the residue field of $R_{\mathfrak{p}}$ and the canonical quotient map, respectively. Define $L_{\mathfrak{p}} := R_{\mathfrak{p}}L$ (as submodule of V) and set $\rho_{L,\mathfrak{p}} := \rho_{L,R_{\mathfrak{p}}}$, for short. Observe that $L_{\mathfrak{p}}$ is the localization of L at $\mathfrak{p}$, as suggested by the notation, so that there is a canonical isomorphism $L_{\mathfrak{p}} \simeq L \otimes_R R_{\mathfrak{p}}$. Moreover, $L_{\mathfrak{p}}$ is an $R_{\mathfrak{p}}$-lattice of V. We also have a residual representation $\bar{\rho}_{L,\mathfrak{p}}$ on the field $k_{\mathfrak{p}}$ which is defined as the composition

$$\bar{\rho}_{L,\mathfrak{p}} : G \xrightarrow{\rho_{L,\mathfrak{p}}} \mathrm{Aut}_{R_{\mathfrak{p}}}(L_{\mathfrak{p}}) \xrightarrow{\pi_{\mathfrak{p}}} \mathrm{Aut}_{k_{\mathfrak{p}}}(L_{\mathfrak{p}}/\mathfrak{p}L_{\mathfrak{p}}).$$

In particular, taking as $\mathfrak{p}$ the trivial ideal (0) of R gives $\rho_{L,(0)} = \bar{\rho}_{L,(0)} = \rho_V$. The notion of irreducibility for the representations $\bar{\rho}_{L,\mathfrak{p}}$ is the obvious one.

To motivate the main theorem of this note, in the next subsection we recall a classical result over discrete valuation rings.

2.3. **Discrete valuation rings.** Suppose now that $\mathcal{O}$ is a discrete valuation ring and fix a generator π of its maximal ideal $\wp$. Let F denote the fraction field of $\mathcal{O}$. In this case, since $\mathcal{O}$ is a principal ideal domain, every $\mathcal{O}$-lattice L in a finite-dimensional F-vector space V is free over $\mathcal{O}$. Of course, $\mathcal{O}_{\wp} = \mathcal{O}$, hence $L_{\wp} = L$ and the reduced representation $\bar{\rho}_{L,\wp}$ is equal to the composition

$$\bar{\rho}_{L,\wp} : G \xrightarrow{\rho_L} \mathrm{Aut}_{\mathcal{O}}(L) \xrightarrow{\pi_{\wp}} \mathrm{Aut}_{k_{\wp}}(L/\wp L)$$

where $k_{\wp} := \mathcal{O}/\wp$ is the residue field of $\mathcal{O}$. The result we are about to state is well known, but we recall it here because it represents a motivation for the theorem that will be proved in the subsequent section.

Proposition 2.5. *Let $\mathcal{O}$, ρ_V and ρ_L be as above. If $\bar{\rho}_{L,\wp}$ is irreducible then ρ_V is irreducible.*

Proof. By Proposition 2.4, we can equivalently prove that ρ_L is irreducible. Arguing by contradiction, suppose that M is a G-stable $\mathcal{O}$-submodule of L such that KM is neither trivial nor equal to V; in particular, $M \neq L$. It is easy to see that there exists $n \in \mathbb{N}$ such that

$$M \subset \wp^n L, \qquad M \not\subset \wp^{n+1}L.$$

Hence, at the cost of multiplying M by a suitable power of π, we can assume that $M \not\subset \wp L$. Since $M \neq L$, Nakayama's lemma ensures that $M + \wp L \neq L$ (see, e.g., [1, Corollary 2.7]), hence the image of M in $L/\wp L$ is non-trivial and strictly smaller than $L/\wp L$. This contradicts the irreducibility of $\bar{\rho}_{L,\wp}$. □

The question of finding an analogue of Proposition 2.5 when the discrete valuation ring $\mathcal{O}$ is replaced by an arbitrary noetherian domain has been the starting point of our investigation. Theorem 3.3 gives a reasonable answer to this problem for a large class of rings.

3. The irreducibility theorem

This section is devoted to the proof of the main result of this paper, which is given in §3.2.

3.1. **Algebraic preliminaries.** For lack of an explicit reference, we give a proof of the following elementary result in linear algebra.

Lemma 3.1. *Let A be a ring, let M be a free A-module of finite rank and let $\{N_\lambda\}_{\lambda \in \Lambda}$ be a family of A-modules. There is a canonical isomorphism*

$$\left(\prod_{\lambda \in \Lambda} N_\lambda \right) \otimes_A M \simeq \prod_{\lambda \in \Lambda} (N_\lambda \otimes_A M)$$

of A-modules.

Proof. Let $\{e_1, \ldots, e_t\}$ be a basis of M over A, so that we can write

$$M = \bigoplus_{i=1}^{t} A e_i.$$

There are canonical isomorphisms of A-modules

$$(2) \qquad \left(\prod_{\lambda \in \Lambda} N_\lambda \right) \otimes_A M \simeq \bigoplus_{i=1}^{t} \left[\left(\prod_{\lambda \in \Lambda} N_\lambda \right) \otimes_A A e_i \right] \simeq \bigoplus_{i=1}^{t} \left(\prod_{\lambda \in \Lambda} N_\lambda \right) e_i$$

and

$$(3) \qquad \prod_{\lambda \in \Lambda} (N_\lambda \otimes_A M) \simeq \prod_{\lambda \in \Lambda} \left[\bigoplus_{i=1}^{t} (N_\lambda \otimes_A A e_i) \right] \simeq \prod_{\lambda \in \Lambda} \left(\bigoplus_{i=1}^{t} N_\lambda e_i \right).$$

But there is also a canonical isomorphism of A-modules

$$\bigoplus_{i=1}^{t} \left(\prod_{\lambda \in \Lambda} N_\lambda \right) e_i \qquad \xrightarrow{\simeq} \qquad \prod_{\lambda \in \Lambda} \left(\bigoplus_{i=1}^{t} N_\lambda e_i \right)$$

$$\left((n_{1,\lambda})_\lambda e_1, \ldots, (n_{t,\lambda})_\lambda e_t \right) \longmapsto \left((n_{1,\lambda} e_1, \ldots, n_{t,\lambda} e_t) \right)_{\lambda \in \Lambda},$$

and the claim follows by combining (2) and (3). □

We use this result to prove

Proposition 3.2. *Let A be a ring, let M be a free A-module of finite rank, let N be an A-module and let $\{N_\lambda\}_{\lambda \in \Lambda}$ be a family of A-submodules of N. There is a canonical isomorphism*

$$(4) \qquad \left(\bigcap_{\lambda \in \Lambda} N_\lambda \right) \otimes_A M \simeq \bigcap_{\lambda \in \Lambda} (N_\lambda \otimes_A M)$$

of A-submodules of $N \otimes_A M$.

Proof. First of all, since M is flat over A, for all $\lambda \in \Lambda$ there is a canonical isomorphism

$$(5) \qquad (N/N_\lambda) \otimes_A M \simeq (N \otimes_A M)/(N_\lambda \otimes_A M)$$

of A-modules. Define the A-linear map

$$N \xrightarrow{\varphi} \prod_{\lambda \in \Lambda} (N/N_\lambda)$$

$$x \longmapsto \left([x]_\lambda \right)_{\lambda \in \Lambda}$$

where $[x]_\lambda$ denotes the natural image of $x \in N$ in N/N_λ. Then the sequence

$$0 \longrightarrow \bigcap_{\lambda \in \Lambda} N_\lambda \longrightarrow N \xrightarrow{\varphi} \prod_{\lambda \in \Lambda} (N/N_\lambda)$$

is exact and, since M is free of finite rank over A, by Lemma 3.1 and isomorphism (5) the same is true of the sequence

$$0 \longrightarrow \left(\bigcap_{\lambda \in \Lambda} N_\lambda \right) \otimes_A M \longrightarrow N \otimes_A M \longrightarrow \prod_{\lambda \in \Lambda} (N \otimes_A M)/(N_\lambda \otimes_A M),$$

which proves the proposition. $\square$

3.2. **Proof of the irreducibility criterion.** The main result on the irreducibility of ρ_V we wish to prove is the following

Theorem 3.3. *Let R be a noetherian domain with field of fractions K, let ρ_V, ρ_L be as above and assume that the lattice L is free over R. Suppose that there exists a set $\mathcal{S}$ of prime ideals of R such that*

   (i) *$\bigcap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p} = \{0\}$;*
   (ii) *$\bar{\rho}_{L,\mathfrak{p}}$ is irreducible for every $\mathfrak{p} \in \mathcal{S}$.*
Then ρ_V is irreducible.

Of course, if the trivial ideal of R belongs to $\mathcal{S}$ there is nothing to prove, so we can implicitly assume that $(0) \notin \mathcal{S}$.

Proof. Let $W \neq V$ be a non-trivial G-stable K-subspace of V of dimension $m \geq 1$ and define

$$M := L \cap W.$$

It is clear that M is an R-submodule of L which is G-stable. Moreover, M is a lattice of W by [2, Ch. VII, §4, Proposition 3 (ii)].

Let now $\mathfrak{p}$ be a prime ideal of R such that $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible and set

$$M_{\mathfrak{p}} := R_{\mathfrak{p}}M.$$

Then $M_{\mathfrak{p}}$ is an $R_{\mathfrak{p}}$-submodule of $L_{\mathfrak{p}}$ which is G-stable. Furthermore, $M_{\mathfrak{p}} \neq L_{\mathfrak{p}}$ because otherwise we would have

$$W = KM_{\mathfrak{p}} = KL_{\mathfrak{p}} = V,$$

contrary to our assumption. By Nakayama's lemma, this implies that $M_{\mathfrak{p}} + \mathfrak{p}L_{\mathfrak{p}} \neq L_{\mathfrak{p}}$, hence the image of $M_{\mathfrak{p}}$ in $L_{\mathfrak{p}}/\mathfrak{p}L_{\mathfrak{p}}$ is strictly smaller than $L_{\mathfrak{p}}/\mathfrak{p}L_{\mathfrak{p}}$. But $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible, so there is an inclusion

(6) $$M_{\mathfrak{p}} \subset \mathfrak{p}L_{\mathfrak{p}}.$$

Since M is a lattice in W, it contains a free R-module M' of rank m (cf. part 1) of Remark 2.2). To prove that ρ_V is irreducible we want to show that $M' = \{0\}$, a fact that would contradict the non-triviality of W. Since M' injects naturally into $M_{\mathfrak{p}}$, inclusion (6) yields an inclusion

(7) $$M' \subset \mathfrak{p}L_{\mathfrak{p}} \cap L = \mathfrak{p}L$$

for all prime ideals $\mathfrak{p}$ of R such that $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible. Observe that the equality appearing in (7) is an easy consequence of the fact that L is free (of finite rank) over R. In light of condition (ii), to show that $M' = \{0\}$ it is then enough to show that

(8) $$\bigcap_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}L = \{0\}.$$

Since L is free (hence flat) over R, for any ideal $\mathfrak{a}$ of R there is a canonical isomorphism

(9) $$\mathfrak{a}L \simeq \mathfrak{a} \otimes_R L$$

of R-modules. Moreover, since L has finite rank over R, if $\mathcal{A}$ is a family of ideals of R then Proposition 3.2 provides a canonical isomorphism

(10) $$\left(\bigcap_{\mathfrak{a}\in\mathcal{A}} \mathfrak{a} \right) \otimes_R L \simeq \bigcap_{\mathfrak{a}\in\mathcal{A}} (\mathfrak{a} \otimes_R L)$$

of R-modules. Applying (9) and (10) to $\mathcal{A} = \mathcal{S}$ yields an isomorphism

$$\bigcap_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}L \simeq \left(\bigcap_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p} \right) \otimes_R L$$

of R-modules, and (8) follows immediately from condition (i). $\qquad\square$

Remark 3.4. 1) Since R is a domain, any set of non-trivial prime ideals of R satisfying condition (i) of Theorem 3.3 is necessarily infinite. Thus the irreducibility criterion of Theorem 3.3 is interesting only for rings with infinitely many prime ideals.

2) For an example of a different representation-theoretic context in which irreducibility modulo prime ideals plays an important role see [6, §3].

It is useful to slightly reformulate condition (ii) of the above theorem. For every prime ideal $\mathfrak{p}$ of R define the representation $\tilde{\rho}_{L,\mathfrak{p}}$ over the noetherian domain $R/\mathfrak{p}$ as the composition

$$\tilde{\rho}_{L,\mathfrak{p}} \colon G \xrightarrow{\rho_L} \operatorname{Aut}_R(L) \longrightarrow \operatorname{Aut}_{R/\mathfrak{p}}(L/\mathfrak{p}L),$$

where the second map is induced by the canonical projection $R \to R/\mathfrak{p}$. If $\operatorname{frac}(R/\mathfrak{p})$ is the fraction field of $R/\mathfrak{p}$ then there is a natural identification

$$\operatorname{frac}(R/\mathfrak{p}) = k_{\mathfrak{p}}$$

and $L/\mathfrak{p}L$ is an $R/\mathfrak{p}$-lattice in $L_{\mathfrak{p}}/\mathfrak{p}L_{\mathfrak{p}}$, hence Proposition 2.4 ensures that condition (ii) in Theorem 3.3 is equivalent to

(ii') $\tilde{\rho}_{L,\mathfrak{p}}$ is irreducible for every $\mathfrak{p} \in \mathcal{S}$.

For the rest of the paper we make the following

Assumption 3.5. The lattice L is *free* over R.

The next result is an easy consequence of the previous theorem.

Corollary 3.6. *With notation as above, if $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible for infinitely many height 1 prime ideals $\mathfrak{p}$ of R then ρ_V is irreducible.*

Proof. By Theorem 3.3, it suffices to show that the intersection of infinitely many height 1 prime ideals of R is trivial. So let $\mathcal{S}$ be an infinite set of prime ideals of R of height 1 and define

$$I := \bigcap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}.$$

If $I \neq \{0\}$ then every $\mathfrak{p} \in \mathcal{S}$, having height 1, is minimal among the prime ideals of R containing I. But the set of such prime ideals of R has only finitely many minimal elements by [7, Exercise 4.12], and this is a contradiction. $\qquad\square$

Another by-product of Theorem 3.3 is the following

Proposition 3.7. *Let R be a local noetherian domain with maximal ideal $\mathfrak{m}$ and let ρ_V, ρ_L be as above. Suppose that the representation $\bar{\rho}_{L,\mathfrak{m}}$ is irreducible and that there exists a set $\mathcal{S}$ of prime ideals of R such that*

(i) $\bigcap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p} = \{0\}$;
(ii) $R/\mathfrak{p}$ *is a discrete valuation ring for every $\mathfrak{p} \in \mathcal{S}$.*

Then ρ_V is irreducible.

Proof. The representation $\bar{\rho}_{L,\mathfrak{m}}$ coincides with $\tilde{\rho}_{L,\mathfrak{m}}$ and so it naturally identifies, for every prime ideal $\mathfrak{p} \in \mathcal{S}$, with the reduction of $\tilde{\rho}_{L,\mathfrak{p}}$ modulo the maximal ideal $\mathfrak{m}/\mathfrak{p}$ of the discrete valuation ring $R/\mathfrak{p}$. Since we are assuming that $\bar{\rho}_{L,\mathfrak{m}}$ is irreducible, Proposition 2.5 ensures that $\tilde{\rho}_{L,\mathfrak{p}}$ is irreducible for every $\mathfrak{p} \in \mathcal{S}$. In other words, condition (ii') is satisfied, and the irreducibility of ρ_V follows from Theorem 3.3. $\qquad\square$

3.3. **Representations over regular local rings.** In this subsection we consider a regular local ring R with maximal ideal $\mathfrak{m}$ and residue field $\kappa := R/\mathfrak{m}$. It is known that such a ring is necessarily a domain (see, e.g., [7, Theorem 14.3]). If one also assumes that R is complete with respect to its $\mathfrak{m}$-adic topology (which we will not do) then classical structure theorems of Cohen ([3]) give very precise descriptions of R in terms of formal power series rings over either κ or a complete discrete valuation ring of characteristic zero with residue field κ. Recall that a regular ring is a noetherian ring such that every localization $R_\mathfrak{p}$ of R at a prime ideal $\mathfrak{p}$ is a regular local ring. If R is a regular (respectively, regular local) ring then any formal power series ring over R is a regular (respectively, regular local) ring as well ([7, Theorem 19.5]).

Theorem 3.8. *With notation as above, let R be a regular local ring. If $\bar{\rho}_{L,\mathfrak{m}}$ is irreducible then ρ_V is irreducible.*

Proof. We proceed by induction on the Krull dimension d of R. If $d = 1$ then R is a discrete valuation ring, hence the claim of the theorem follows from Proposition 2.5. Now suppose that the theorem has been proved for rings of dimension t and take $d = t + 1$. Write $\mathfrak{m} = (x_1, \ldots, x_{t+1})$ and consider the infinite set $\mathcal{S}$ of prime ideals of R given by

$$\mathcal{S} := \big\{ (x_2 - x_1^i) \mid i \geq 1 \big\}.$$

We want to prove that $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible for every $\mathfrak{p} \in \mathcal{S}$. If $\mathfrak{p} \in \mathcal{S}$ then the noetherian local ring $R/\mathfrak{p}$ is regular of dimension t ([7, Theorem 14.2]); moreover, the reduction of $\tilde{\rho}_{L,\mathfrak{p}}$ modulo the maximal ideal $\mathfrak{m}/\mathfrak{p}$ coincides with $\bar{\rho}_{L,\mathfrak{m}}$, which is irreducible by hypothesis. The inductive assumption then gives the irreducibility of $\tilde{\rho}_{L,\mathfrak{p}}$, which is equivalent to the irreducibility of $\bar{\rho}_{L,\mathfrak{p}}$. Finally, since all prime ideals in $\mathcal{S}$ have height 1 (for example, by Krull's principal ideal theorem), the irreducibility of ρ_V follows from Corollary 3.6. $\qquad\square$

Notice that this theorem extends the result proved in Proposition 2.5 for discrete valuation rings to the much larger class of regular local rings.

Corollary 3.9. (1) *Let R be a noetherian domain and suppose that there exists a prime ideal $\mathfrak{p}$ of R such that*

(i) *$R_\mathfrak{p}$ is a regular local ring;*
(ii) *$\bar{\rho}_{L,\mathfrak{p}}$ is irreducible.*

Then ρ_V is irreducible.

(2) *If R is a regular domain and there exists a prime ideal $\mathfrak{p}$ of R such that $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible then ρ_V is irreducible.*

Proof. Since, by definition of a regular ring, part (2) is an immediate consequence of part (1), it suffices to prove the first claim. Since $R_{\mathfrak{p}}$ is a regular local ring and $\bar{\rho}_{L,\mathfrak{p}}$ is irreducible, the representation $\rho_{L,\mathfrak{p}}$ over $R_{\mathfrak{p}}$ is irreducible by Theorem 3.8. But the fraction field of $R_{\mathfrak{p}}$ is equal to K, hence the corollary follows from Proposition 2.4. $\square$

In particular, this corollary applies to the special case where R is a Dedekind domain (e.g., the ring of algebraic integers of a number field).

4. ARITHMETIC APPLICATIONS

We offer applications of Theorem 3.3 (or, rather, of Theorem 3.8) in situations of arithmetic interest.

4.1. Universal deformations of residual representations.
We briefly recall the basic definitions about deformations of residual representations; for more details, the reader is referred to the original article [8] by Mazur and to the survey papers [5] and [9].

Fix a prime number p and a finite field κ of characteristic p. Let Π be a profinite group satisfying Mazur's finiteness condition Φ_p ([8, §1.1]), i.e. such that for every open subgroup Π_0 of Π there are only finitely many continuous homomorphisms from Π_0 to the field $\mathbb{F}_p$ with p elements. A remarkable example of a group with this property is represented by the Galois group $G_{\mathbb{Q},S}$ over $\mathbb{Q}$ of the maximal field extension of $\mathbb{Q}$ which is unramified outside a finite set S of primes of $\mathbb{Q}$.

If $n \geq 1$ is an integer, by a *residual representation of dimension n* (of Π over κ) we shall mean a continuous representation

$$\bar{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(\kappa).$$

Write $\mathcal{C}$ for the category of *coefficient rings* in the sense of Mazur ([9, §2]), whose objects are complete noetherian local rings with residue field κ and whose morphisms are (local) homomorphisms of complete local rings inducing the identity on κ. More generally, for an object $\Lambda \in \mathcal{C}$ we can consider the category $\mathcal{C}_\Lambda$ of *coefficient Λ-algebras*, whose objects are complete noetherian local Λ-algebras with residue field κ and whose morphisms are coefficient-ring homomorphisms which are also Λ-algebra homomorphisms. Observe that $\mathcal{C} = \mathcal{C}_{W(\kappa)}$ where $W(\kappa)$ is the ring of Witt vectors of κ, i.e. the (unique) unramified extension of $\mathbb{Z}_p$ with residue field κ.

If $A \in \mathcal{C}_\Lambda$ then two continuous representations

$$\rho_1, \rho_2 \colon \Pi \longrightarrow \mathrm{GL}_n(A)$$

will be said to be *strictly equivalent* if there exists M in the kernel of the reduction map $\mathrm{GL}_n(A) \to \mathrm{GL}_n(\kappa)$ such that $\rho_1 = M\rho_2 M^{-1}$. Given a residual representation $\bar{\rho}$ as above, a *deformation* of $\bar{\rho}$ to $A \in \mathcal{C}$ is a strict equivalence class $\boldsymbol{\rho}$ of (continuous) representations

$$\rho \colon \Pi \longrightarrow \mathrm{GL}_n(A)$$

which reduce to $\bar{\rho}$ via the map $\mathrm{GL}_n(A) \to \mathrm{GL}_n(\kappa)$. By abuse of notation, we will write

$$\boldsymbol{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(A)$$

to denote a deformation of $\bar{\rho}$ to A.

Finally, given an n-dimensional residual representation $\bar{\rho}$, endow κ^n with a (left) Π-module structure via $\bar{\rho}$ and define

$$C(\bar{\rho}) := \mathrm{Hom}_\Pi(\kappa^n, \kappa^n)$$

to be its ring of Π-module endomorphisms.

Theorem 4.1 (Mazur, Ramakrishna). *With notation as above, let $\Lambda \in \mathcal{C}$ and let*

$$\bar{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(\kappa)$$

be a residual representation such that $C(\bar{\rho}) = \kappa$. Then there exists a ring $\mathcal{R}_\Lambda = \mathcal{R}_\Lambda(\Pi, \kappa, \bar{\rho}) \in \mathcal{C}_\Lambda$ and a deformation

$$\boldsymbol{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R}_\Lambda)$$

of $\bar{\rho}$ to $\mathcal{R}$ such that any deformation of $\bar{\rho}$ to a ring $A \in \mathcal{C}_\Lambda$ is obtained from $\boldsymbol{\rho}$ via a unique morphism $\mathcal{R}_\Lambda \to A$.

For a proof, see [5, Theorem 3.10]. We call $\mathcal{R}_\Lambda$ the *universal deformation ring* and $\boldsymbol{\rho}$ the *universal deformation* of $\bar{\rho}$.

Remark 4.2. By Schur's lemma, $C(\bar{\rho}) = \kappa$ if $\bar{\rho}$ is absolutely irreducible, so any absolutely irreducible residual representation admits universal deformation.

Let now $\mathrm{ad}(\bar{\rho})$ be the adjoint representation of $\bar{\rho}$, i.e. the κ-vector space $\mathrm{M}_n(\kappa)$ on which Π acts on the left by conjugation via $\bar{\rho}$ (hence $C(\bar{\rho})$ is non-canonically isomorphic to the subspace of Π-invariants of $\mathrm{ad}(\bar{\rho})$). The following result is part of a theorem of Mazur, for a proof of which we refer to [8, Proposition 2] or [5, Theorem 4.2].

Theorem 4.3 (Mazur). *Suppose $C(\bar{\rho}) = \kappa$, let $\mathcal{R}_\Lambda$ be the universal deformation ring of $\bar{\rho}$ and define*

(11) $$d_1 := \dim_\kappa H^1\big(\Pi, \mathrm{ad}(\bar{\rho})\big), \qquad d_2 := \dim_\kappa H^2\big(\Pi, \mathrm{ad}(\bar{\rho})\big).$$

If $d_2 = 0$ then $\mathcal{R}_\Lambda \simeq \Lambda[\![x_1, \ldots, x_{d_1}]\!]$.

When $d_2 = 0$ we say that the deformation problem for $\bar{\rho}$ is *unobstructed*. It is convenient to introduce the following terminology.

Definition 4.4. Suppose that the coefficient ring A is a domain. A deformation $\boldsymbol{\rho}$ of $\bar{\rho}$ to A is said to be *irreducible* if every $\rho \in \boldsymbol{\rho}$ is irreducible.

Here the irreducibility of a representation over A is understood in the sense of §2.1. Of course, since all representations in a deformation of $\bar{\rho}$ to A are equivalent, Definition 4.4 amounts to requiring that there exists $\rho \in \boldsymbol{\rho}$ which is irreducible.

Let now $\mathcal{O}$ be a complete regular local ring with residue field κ. As an easy consequence of the results in §3.3, we obtain

Proposition 4.5. *With notation as before, let*

$$\bar{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(\kappa)$$

be an n-dimensional irreducible residual representation such that $C(\bar{\rho}) = \kappa$ and $d_2 = 0$. The universal deformation

$$\boldsymbol{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R}_{\mathcal{O}})$$

of $\bar{\rho}$ is irreducible.

Proof. Since we are in the unobstructed case, Theorem 4.3 ensures that there is an $\mathcal{O}$-algebra isomorphism $\mathcal{R}_{\mathcal{O}} \simeq \mathcal{O}[\![x_1, \ldots, x_{d_1}]\!]$ with d_1 as in (11). In particular, the deformation ring $\mathcal{R}_{\mathcal{O}}$ is a regular local ring, whose maximal ideal we denote by $\mathfrak{m}$. Moreover, every representation $\rho \in \boldsymbol{\rho}$ reduces modulo $\mathfrak{m}$ to $\bar{\rho}$, which is irreducible by assumption, hence the proposition follows from Theorem 3.8. $\square$

Remark 4.6. The reader may have noticed that Proposition 4.5 has not been stated in the greatest generality. In fact, all we really need to know in order to deduce the irreducibility of $\boldsymbol{\rho}$ from Theorem 3.8 is that $\bar{\rho}$ is irreducible and admits a universal deformation ring which is a regular local ring. However, the conditions appearing in Proposition 4.5 are the ones that can be checked more easily in "practical" situations, so we preferred to formulate our results in a slightly less general but more readily applicable form.

4.2. **Deformations of residual modular representations.** Of remarkable arithmetic interest are the residual Galois representations associated with modular forms, and now we want to specialize Proposition 4.5 to this setting.

Let f be a newform of level N and weight $k \geq 2$ and let K_f be the number field generated by the Fourier coefficients of f. For every prime λ of K_f Deligne has associated with f a semisimple representation

$$\bar{\rho}_{f,\lambda} \colon G_{\mathbb{Q},S} \longrightarrow \mathrm{GL}_2(\kappa_\lambda)$$

over the residue field κ_λ of K_f at λ; here $G_{\mathbb{Q},S}$ is the Galois group over $\mathbb{Q}$ of the maximal extension of $\mathbb{Q}$ unramified outside the finite set S of places dividing $N\ell\infty$ where ℓ is the characteristic of κ_λ and ∞ denotes the unique archimedean place of $\mathbb{Q}$. The representation $\bar{\rho}_{f,\lambda}$ is absolutely irreducible for all but finitely many primes λ; for such a λ let $\mathcal{R}_{f,\lambda}^S$ be the universal deformation ring parametrizing deformations of $\bar{\rho}_{f,\lambda}$ to complete noetherian local rings with residue field κ_λ (cf. Remark 4.2).

As a sample result in the context of residual modular representations, we prove

Proposition 4.7. *If $k > 2$ then the universal deformation*

$$\boldsymbol{\rho}_{f,\lambda} \colon G_{\mathbb{Q},S} \longrightarrow \mathrm{GL}_2\big(\mathcal{R}_{f,\lambda}^S\big)$$

of $\bar{\rho}_{f,\lambda}$ is irreducible for all but finitely many primes λ of K_f, while if $k = 2$ then $\boldsymbol{\rho}_{f,\lambda}$ is irreducible for a subset of primes λ of K_f of density 1.

Proof. By a theorem of Weston ([11, Theorem 1]), if $k > 2$ (respectively, $k = 2$) then the deformation problem for $\bar{\rho}_{f,\lambda}$ is unobstructed for almost all primes λ of K_f (respectively, for a subset of primes λ of K_f of density 1). Moreover, for every such λ there is an isomorphism

$$\mathcal{R}_{f,\lambda}^S \simeq W(\kappa_\lambda)[\![x_1, x_2, x_3]\!]$$

where $W(\kappa_\lambda)$ is the ring of Witt vectors of κ_λ. Since $\bar{\rho}_{f,\lambda}$ is (absolutely) irreducible, the proposition follows from Theorem 3.8. $\qquad\square$

See [12] for explicit results on the set of obstructed primes for f in the case where the level N is square-free.

REFERENCES

[1] M. F. Atiyah, I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Company, London, 1969.
[2] N. Bourbaki, *Commutative algebra*, Hermann, Paris, 1972.
[3] I. S. Cohen, On the structure and ideal theory of complete local rings, *Trans. Amer. Math. Soc.* **59(1)** (1946), 54–106.
[4] C. W . Curtis, I. Reiner, *Methods of representation theory. Volume I*, John Wiley & Sons, Inc., New York, 1981.
[5] F. Q. Gouvêa, Deformations of Galois representations, in *Arithmetic algebraic geometry*, B. Conrad and K. Rubin (eds.), IAS/Park City Math. Ser. **9**, American Mathematical Society, Providence, RI, 2001, 233–406.
[6] B. H. Gross, Group representations and lattices, *J. Amer. Math. Soc.* **3(4)** (1990), 929–960.
[7] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, Cambridge, 1989.
[8] B. Mazur, Deforming Galois representations, in *Galois groups over $\mathbb{Q}$*, Y. Ihara, K. Ribet and J.-P. Serre (eds.), MSRI Publications **16**, Springer-Verlag, New York, 1989, 385–437.
[9] B. Mazur, An introduction to the deformation theory of Galois representations, in *Modular forms and Fermat's last theorem*, G. Cornell, J. H. Silverman and G. Stevens (eds.), Springer-Verlag, New York, 1997, 243–311.
[10] J.-P. Serre, Three letters to Walter Feit on group representations and quaternions, *J. Algebra* **319(2)** (2008), 549–557.
[11] T. Weston, Unobstructed modular deformation problems, *Amer. J. Math.* **126(6)** (2004), 1237–1252.
[12] T. Weston, Explicit unobstructed primes for modular deformation problems of squarefree level, *J. Number Theory* **110(1)** (2005), 199–218.

Matteo Long
Dipartimento di Matematica Pura e Applicata
Università di Padova
Via Trieste 63
35121 Padova, Italy
  E-mail address: `mlongo@math.unipd.it`

Stefano Vigni
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
C. Jordi Girona 1-3
08034 Barcelona, Spain
  E-mail address: `stefano.vigni@upc.edu`