Deformations of Galois Representations I

Luca Marannino

Babyseminar SS2022 - Talk 13

1 Introduction and first examples

The study of the absolute Galois group of a number field is one of the most classical and important problems in number theory. In the last decades the investigation of the representations of such Galois groups has led to many developments in the theory.

For this introduction we fix a number field K and we let $\bar{K}$ be an algebraic closure of K and $G_K := \mathrm{Gal}(\bar{K}/K)$ denote the absolute Galois group. It is well-known that

$$G_K \cong \varprojlim_{\substack{K \subseteq L \\ \text{finite Galois}}} \mathrm{Gal}(L/K)$$

and that G_K becomes a profinite topological group under this identification.

If S denotes a finite set of non-archimedean places of K, we let $G_{K,S} := \mathrm{Gal}(\bar{K}_S/K)$ where $\bar{K}_S$ is the maximal algebraic extension of K inside $\bar{K}$ which is unramified outside S (i.e. the union of all finite extensions of K inside $\bar{K}$ which are unramified outside S or equivalently the union of all finite extensions of K inside $\bar{K}$ whose relative discriminant is not divisible by any prime outside S). Notice that $G_{K,S}$ is itself a profinite group, being a quotient of G_K.

If A is any topological ring, we endow the group $\mathrm{GL}_N(A)$ with the topology induced by the embedding

$$\mathrm{GL}_N(A) = \{(a_{1,1}, a_{1,2}, \dots, a_{N,N}, d) \in A^{N^2+1} \mid d \cdot \det([a_{i,j}]) = 1\} \subset A^{N^2+1}$$

Definition 1. A **Galois representation** of K is a continuous group homomorphism

$$\rho : G_{K,S} \to \mathrm{GL}_N(A)$$

for some topological ring A.

Galois representations arise naturally while studying arithmetic objects.

Example 2. Let E be an elliptic curve over K with identity element $O \in E(K)$. Let $n \in \mathbb{Z}_{\geq 1}$. As usual we let

$$E[n] = \{x \in E(\bar{K}) \mid [n] \cdot x = O\}$$

denote the group of n-torsion points of the curve. It is easy to see that there is a natural action of G_K on $E[n]$. Fixing an isomorphism $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ induces a continuous homomorphism $G_K \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which factors through $G_{K,S}$ where S is the set of primes dividing n or of bad reduction for E. Indeed if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ such that E has good reduction modulo $\mathfrak{p}$ and $\mathfrak{p} \nmid n\mathcal{O}_K$, let us $\bar{E}$ denote the reduction of E modulo $\mathfrak{p}$. Then by our assumptions we get that $\bar{E}[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ is a $G_{k(\mathfrak{p})}$-module (with

$k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$), with Galois action induced by the Galois action on $E[n]$. This implies that the Galois action on $E[n]$ is trivial on the inertia subgroup relative to the prime $\mathfrak{p}$, i.e. our representation $G_K \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is unramified at $\mathfrak{p}$. Thus we get a Galois representation

$$\rho_{E,n} : G_{K,S} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

If we fix a rational prime $p > 1$ and we let

$$S = \{\text{prime of bad reductions of } E\} \cup \{p\}$$

we can form an inverse system of representations $(\rho_{E,p^k})_{k\geq 1}$ where at each step the maps are given by

$$E[p^{k+1}] \to E[p^k] \quad x \mapsto [p] \cdot x$$

obtaining $T_p(E) = \varprojlim_k E[p^k] \cong \mathbb{Z}_p^2$ (the p-adic Tate module of E) and hence a representation

$$\rho_{E,p^\infty} : G_{K,S} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

In what follows we would like to interpret such a representation as a prototypical example of lifting of a Galois representation over $\mathbb{F}_p$ via the study of a suitable deformation problem.

2 Mod p representations of profinite groups and the associated deformation problems

Let us start this more general treatment by fixing some definitions and notations.

We let k denote a finite field and $p := \mathrm{char}(k)$.

Definition 3. A **k-coefficient ring** (or simply a **coefficient ring**, when the field k is clear from the context) is a complete noetherian local ring A with residue field k.

A homomorphism of k-coefficient rings is a continuous local homomorphism of k-coefficient rings.

Remark 4. We let $W(k)$ denote the ring of Witt vectors of k. Then by the universal properties of Witt vectors, any k-coefficient ring A is endowed with a homomorphism (in the above sense) $W(k) \to A$ and becomes naturally a topological $W(k)$-algebra.

If A is a k-coefficient ring with maximal ideal $\mathfrak{m}_A$, then the topology on $\mathrm{GL}_N(A)$ is the same as the profinite topology given by the identification

$$\mathrm{GL}_N(A) = \varprojlim_n \mathrm{GL}_N(A/m_A^n)$$

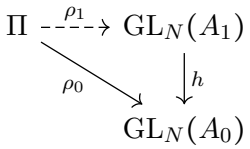
From now on we let Π be a profinite group and assume that we have a representation of Π with k-coefficient ring A_0 and degree N, i.e. a representation

$$\rho_0 : \Pi \to \mathrm{GL}_N(A_0).$$

If $h : A_1 \to A_0$ is a homomorphism of k-coefficient rings, let us also denote by the same letter the induced group homomorphism

$$h : \mathrm{GL}_N(A_1) \to \mathrm{GL}_N(A_0)$$

Definition 5. A **deformation** of ρ_0 to the k-coefficient ring A_1 is a strict equivalence class of liftings



where two liftings ρ_1 and ρ_1' are **strictly equivalent** if there exists a matrix $x \in \mathrm{Ker}(h)$ such that $\rho_1(\pi) = x^{-1}\rho_1'(\pi)x$ for all $\pi \in \Pi$.

Definition 6. Let Λ be a k-coefficient ring. A k-coefficient Λ-algebra is a k-coefficient ring A together with a k-coefficient ring homomorphism $\Lambda \to A$.

Given a k-coefficient Λ-algebra we consider the category $\hat{\mathcal{C}}_\Lambda(A)$ whose objects are k-coefficients Λ-algebras together with a fixed k-coefficient Λ-algebras homomorphism to A (sometimes called A-**augmentation**) and where morphisms are morphisms of k-coefficients Λ-algebras commuting with augmentations in the obvious way.

We let $\mathcal{C}_\Lambda(A)$ denote the full subcategory of $\hat{\mathcal{C}}_\Lambda(A)$ whose objects are those objects in $\hat{\mathcal{C}}_\Lambda(A)$ which are also artinian rings.

When $A = k$ we simply write $\hat{\mathcal{C}}_\Lambda = \hat{\mathcal{C}}_\Lambda(k)$ and $\mathcal{C}_\Lambda = \hat{\mathcal{C}}_\Lambda(k)$.

Given a k-coefficient ring Λ, a profinite group Π and a *residual* representation $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$ we define the functor

$$D_{\bar{\rho}} : \hat{\mathcal{C}}_\Lambda \to Sets \tag{1}$$

assigning to any object $\Lambda \to B$ of $\hat{\mathcal{C}}_\Lambda$ the set of deformations of $\bar{\rho}$ to B, with morphisms acting via post-composition (note that this is well-defined!).

We can also define relative versions of this functor as follows. For any representation $\rho : \Pi \to \mathrm{GL}_N(A)$ (which should be interpreted as a choice of a lifting, i.e. an actual group homomorphism, not a strict equivalence class, of $\bar{\rho}$) to a k-coefficient Λ-algebra A, we let

$$D_\rho : \hat{\mathcal{C}}_\Lambda(A) \to Sets \tag{2}$$

the functor associating to any A-augmented Λ-algebra B the set of deformations of ρ to B.

Proposition 7 (cf. Prop. 20.2 in [2])**.** *The functors D_ρ and $D_{\bar{\rho}}$ defined above are* ***continuous****, i.e. for every A-augmented Λ-algebra B it holds,*

$$D_\rho(B) = \varprojlim_n D_{\rho_n}(B/\mathfrak{m}_B^n)$$

where $\rho_n : \Pi \xrightarrow{\rho} \mathrm{GL}_N(A) \twoheadrightarrow \mathrm{GL}_N(A/\mathfrak{m}_A^n)$, and for every k-coefficient Λ-algebra B it holds

$$D_{\bar{\rho}}(B) = \varprojlim_n D_{\bar{\rho}}(B/\mathfrak{m}_B^n)$$

Proof. We refer to [2] for the proof. □

The above proposition shows that the functor $D_{\bar{\rho}}$ is uniquely determined by its restriction to the category $\mathcal{C}_\Lambda$ and that the functor D_ρ is uniquely determined by the restrictions of the functors D_{ρ_n} to the category $\mathcal{C}_\Lambda(A)$. In particular we can now apply the machinery for functors on artinian rings that was developed in the previous talks.

3 Pro-representability and near representability

In this section we introduce the version of Schlessinger's criterion that is needed to prove that our functors $D_{\bar{\rho}}$ and D_ρ of the previous section enjoy good properties under some suitable hypothesis.

In this section we let $D : \mathcal{C}_\Lambda \to Sets$ and $D_A : \mathcal{C}_\Lambda(A) \to Sets$ be covariant functors such that $D(k)$ and $D_A(A)$ consist of a single element. We let $k[\varepsilon]$ denotes the ring of dual numbers and $A[\varepsilon] = A \otimes_k k[\varepsilon]$, as the notation suggests. We will **always** view $k[\varepsilon]$ as Λ-algebra via the composition $\Lambda \twoheadrightarrow k \hookrightarrow k[\varepsilon]$ (and similarly for $A[\varepsilon]$).

We also make the following hypothesis.

($\mathbf{T}_k$) The natural map

$$D(k[\varepsilon] \times_k k[\varepsilon]) \to D(k[\varepsilon]) \times D(k[\varepsilon])$$

is a bijection.

($\mathbf{T}_A$) The natural map

$$D_A(A[\varepsilon] \times_A A[\varepsilon]) \to D_A(A[\varepsilon]) \times D_A(A[\varepsilon])$$

is a bijection.

Definition 8. We define the **Zariski tangent k-vector space** to D as $t_D \coloneqq D(k[\varepsilon])$ and the **Zariski tangent A-module** to D_A as $t_{D,A} \coloneqq D_A(A[\varepsilon])$.

It was already shown in the previous talks that hypothesis $\mathbf{T}_k$ implies that t_D is indeed endowed with a natural structure of a k-vector space. The same proof shows that, under the hypothesis $\mathbf{T}_A$, the set $t_{D,A}$ is naturally an A-module.

Given any diagram $A \to C \leftarrow B$ in $\mathcal{C}_\Lambda$ we have seen in the previous talks that the fibre product $A \times_C B$ exists in $\mathcal{C}_\Lambda$. In this case we always denote by h the natural map

$$h : D(A \times_C B) \to D(A) \times_{D(C)} D(B)$$

obtained by the universal property of fibre products in $Sets$.

Recall that a morphism $A \to C$ in $\mathcal{C}_\Lambda$ is a **small extension** if it is surjective and its kernel is a principal ideal annihilated by $\mathfrak{m}_A$. Note that this means that such kernel is endowed with the structure of one-dimensional k-vector space.

We are now ready to state the version of Schlessinger's criterion that we need (note that this is also the original formulation given in [4], theorem 2.11).

Theorem 9 (Schlessinger's criterion)**.** *Let $D : \mathcal{C}_\Lambda \to$ be a covariant functor such that $D(k)$ consists of a single element. Then D is **pro-representable** (in the sense of the previous talks) if and only if the following four conditions hold.*

(H1) The map h defined above is surjective if $A \to C$ is a small extension.

(H2) The map h is bijective if $A \to C$ is the morphism $k[\varepsilon] \twoheadrightarrow k$ (so in particular ($\mathbf{T}_k$) holds).

(H3) t_D is a finite dimensional k-vector space.

(H4) The map h is bijective if $A \to C$ and $B \to C$ are the same small extension.

*Moreover, D has a **hull** (in the sense of the previous talks) if and only if the conditions (H1), (H2) and (H3) hold.*

For the functors D_A we define a weaker notion.

Definition 10. Let $D_A : \mathcal{C}_\Lambda(A) \to Sets$ be a covariant functor such that $D_A(A)$ consists of a single element. We say that D_A is **nearly representable** if hypothesis $(\mathbf{T}_A)$ holds and furthermore the A-module $t_{D,A}$ is of finite type.

4 The role of p-finiteness

It is now time to go back to the study of the deformation problems associated to representations of profinite groups. It turns out that, if $p := \mathrm{char}(k)$ and Π is our profinite group as before, there is a condition on Π called p-**finiteness** that enables us to ensure that our deformation functors are good candidates for pro-representability (or near representability in the relative case).

Definition 11. We say that a profinite group Π satisfies the p-**finiteness condition** if for all open subgroups Π_0 of Π, there are only a finitely many continuous group homomorphisms $\Pi_0 \to \mathbb{Z}/p\mathbb{Z}$.

Proposition 12. *The groups $G_{K,S}$ introduced in section 1 satisfy the p-finiteness condition for every prime p.*

Proof. One checks that every open subgroup of $\Pi = G_{K,S}$ is of the form $\Pi_0 = G_{L,T}$ for a finite extension L of K (uniquely determined by taking the preimage of Π_0 along the projection $G_K \twoheadrightarrow G_{K,S}$) and the set T of all non-archimedean places of L lying over the places in S. Thus it is enough to prove that the set

$$\mathrm{Hom}_{cont}(G_{K,S}, \mathbb{Z}/p\mathbb{Z})$$

This is equivalent to proving that there are only finitely many finite cyclic Galois extensions L/K inside $\bar{K}$ of degree p (i.e. with Galois group $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$) which are unramified outside S.

Let $\mathcal{D} := \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$ denote the different of such an extension (an $\mathcal{O}_L$-ideal) and $\delta := \delta_{\mathcal{O}_L/\mathcal{O}_K}$ denote the discriminant (an $\mathcal{O}_K$-ideal), so that $\delta = N_{L/K}(\mathcal{D})$. One can check that a prime $\mathfrak{q}$ of K ramifies in L if and only if $\mathfrak{q} \mid \delta$. More specifically if $\mathfrak{Q}$ is a prime of L with $\mathfrak{Q} \mid \mathfrak{q}$ then the ramification index $e(\mathfrak{Q}/\mathfrak{q}) > 1$ if and only if $\mathfrak{Q} \mid \mathcal{D}$. Assume that $e(\mathfrak{Q}/\mathfrak{q}) > 1$ and that the exact power of $\mathfrak{Q}$ dividing $\mathcal{D}$ is $\mathfrak{Q}^r$ $(r \geq 1)$. In this case we have the two following cases:

(i) if $\mathrm{char}(\mathcal{O}_K/\mathfrak{q}) \nmid e(\mathfrak{Q}/\mathfrak{q})$ (tame ramification), then $r = e(\mathfrak{Q}/\mathfrak{q}) - 1$;

(ii) if $\mathrm{char}(\mathcal{O}_K/\mathfrak{p}) \mid e(\mathfrak{Q}/\mathfrak{q})$ (wild ramification), then

$$e(\mathfrak{Q}/\mathfrak{q}) \leq r \leq e(\mathfrak{Q}/\mathfrak{q}) - 1 + v_{\mathfrak{Q}}(e(\mathfrak{Q}/\mathfrak{q})).$$

where $v_{\mathfrak{Q}}$ denotes the $\mathfrak{Q}$-adic valuation on L, normalized so that $v_{\mathfrak{Q}}(\pi) = 1$ if π is any uniformizer in the $\mathfrak{Q}$-adic completion $\mathcal{O}_{L,\mathfrak{Q}}$ of $\mathcal{O}_L$.

In our situation if $\mathfrak{q} \in S$ ramifies if and only if $\mathfrak{q} = \mathfrak{Q}^p$ for a prime $\mathfrak{Q}$ of L (with norm $N_{L/K}(\mathfrak{Q}) = \mathfrak{q}$), so that $r = p - 1$ in case of tame ramification and $p \leq r \leq p - 1 + v_{\mathfrak{Q}}(p)$ if $\mathfrak{q} \mid p\mathcal{O}_K$. Since $v_{\mathfrak{Q}}(p)$ is bounded (say by $[K : \mathbb{Q}] \cdot p$) and S is finite, we deduce that there are only finitely many possible relative discriminants δ for such extensions.

Since the global discriminant $\Delta_{L/\mathbb{Q}}$ satisfies

$$\Delta_{L/\mathbb{Q}} = \pm(\Delta_{K/\mathbb{Q}})^p \cdot N_{K/\mathbb{Q}}(\delta),$$

we deduce that the possible global discriminants for such number fields L lie in a finite subset of $\mathbb{Z}$.

We conclude by the classical Hermite-Minkowski's theorem (stating that there are only finitely many number fields with a fixed discriminant) that the possible extensions L/K Galois of degree p unramified outside S form a finite set. □

For the last part of the above proof and the Hermite-Minkowski's theorem we refer to [3], chapter III §2.

Remark 13. In order to prove the above proposition one could observe that

$$\mathrm{Hom}_{cont}(G_{K,S}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{cont}(G_{K,S}^{ab}, \mathbb{Z}/p\mathbb{Z}),$$

where $G_{K,S}^{ab}$ denotes the quotient of $G_{K,S}$ by the closure of its commutator subgroup (equivalently it can be interpreted as the Galois group of the maximal abelian extension of K unramified outside S). One can use class field theory to prove that the profinite group $G_{K,S}^{ab}$ is topologically finitely generated (a property which is in general not known for the group $G_{K,S}$) and deduce our statement as a consequence of this fact.

Note also that local class field theory shows that the absolute Galois group of finite extensions K of $\mathbb{Q}_p$ satisfies the p-finiteness condition for all p, since it provides an isomorphism of topological groups

$$G_K^{ab} \cong \mathrm{Gal}(K^{an}/K^{unr}) \times \mathrm{Gal}(K^{unr}/K) \cong \mathcal{O}_K^{\times} \times \hat{\mathbb{Z}}.$$

We can now state the following crucial result (the notation is the usual one).

Theorem 14 (cf. [2] prop. 20.2)**.** *Let $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$ be a continuous residual representation, with k a finite field of characteristic p and Π a profinite group satisfying the p-finiteness condition. Let Λ a coefficient ring with residue field k. Then the following assertions hold.*

(i) The functor $D_{\bar{\rho}} : \mathcal{C}_\Lambda \to Sets$ satisfies the conditions (H1), (H2), (H3) of theorem 9, so it has a hull.

(ii) If $\bar{\rho}$ is absolutely irreducible (i.e. irreducible over an algebraic closure of k), then $DD_{\bar{\rho}}$ is pro-representable.

Moreover, for any (artinian) coefficient Λ-algebra A and every lifting $\rho : \Pi \to \mathrm{GL}_N(A)$ of $\bar{\rho}$ to A, the relative functor $D_\rho : \mathcal{C}_\Lambda(A) \to Sets$ is nearly representable (in the sense of our definition 10)

For the full proof of this result we refer to [1] (cf. section 1.2 in particular).

Remark 15. In the assertion (ii) of the above theorem one can actually assume a weaker hypothesis, namely that the natural mapping $k \to \mathrm{End}_{k[\Pi]}(\bar{V})$ is an isomorphism, where $\bar{V} = k^N$ with Π acting on it via $\bar{\rho}$. This condition is clearly satisfied (by Schur's lemma) if $\bar{\rho}$ is absolutely irreducible, but it can also hold in other cases of interest. For instance it is satisfied by the (non necessarily irreducible!) degree 2 residual Galois representations attached to elliptic curves over p-adic fields with ordinary reduction.

In what follows, we try to explain where the p-finiteness of Π is needed in the proof of theorem 14. We will see that assuming the p-finiteness of Π is crucial to prove that $D_{\bar{\rho}}$ satisfies condition (H3) of theorem 9 and that D_ρ is nearly representable.

In the setting (and with the notation) of the above theorem we assume that we have proven (H1) and (H2) for the functor $D_{\bar{\rho}}$ and that hypothesis $(\mathbf{T}_A)$ holds for D_ρ. Then we know that $t_{\bar{\rho}} := t_{D_{\bar{\rho}}} = D(k[\varepsilon])$ is naturally a k-vector space (our Zariski tangent k-vector space) and that $t_\rho : t_{D_\rho} = D_\rho(A[\varepsilon])$ is naturally an A-module (our Zariski tangent A-module).

In order to prove the finiteness of t_ρ as A-module (note that the relative case contains the absolute case!) we will need a cohomological interpretation of such A-module. Let $V = A^N$ be the free A-module of rank N endowed with the A-linear action given via the composition of ρ with the natural action of $\mathrm{GL}_N(A)$ on V (we think of elements of V as column vectors and the action is right multiplication of matrices).

The action of Π on V induces the so-called adjoint action of Π on $\mathrm{End}_A(V)$ (a free A-module of rank N^2), given by

$$(g * e)(v) := \rho(g)(e(\rho(g)^{-1}(v)))$$

for all $g \in \Pi$, $e \in \mathrm{End}_A(V)$, $v \in V$. We write $\mathrm{End}_A(V) = Ad(\rho)$ when we think of $\mathrm{End}_A(V)$ as a Π-module with the above adjoint action. Equivalently $Ad(\rho)$ can be thought as the composition of ρ with the adjoint representation of $\mathrm{GL}_N(A)$ into its Lie algebra $\mathrm{Mat}_N(A)$.

The cohomology groups appearing in the following will always refer to the continuous cohomology of profinite groups.

Proposition 16. *There is a natural isomorphism of A-modules*

$$t_\rho \cong H^1(\Pi, Ad(\rho))$$

Sketch of the proof. Let $\Gamma := \mathrm{Ker}(GL_N(A[\varepsilon]) \to GL_N(A))$. The short exact sequence of groups

$$1 \to \Gamma \to \mathrm{GL}_N(A[\varepsilon]) \xrightarrow{\beta} \mathrm{GL}_N(A) \to 1$$

splits on the right via the obvious injection $\sigma : \mathrm{GL}_N(A) \hookrightarrow \mathrm{GL}_N(A[\varepsilon])$, proving that we can view $\mathrm{GL}_N(A[\varepsilon])$ as a semidirect product

$$\mathrm{GL}_N(A[\varepsilon]) = \Gamma \rtimes \mathrm{GL}_N(A)$$

Moreover $\Gamma \cong \mathrm{Mat}_N(A)$ as abelian groups (sending $1 + \varepsilon m \mapsto m$) and under this isomorphism we have that

$$\mathrm{GL}_N(A[\varepsilon]) \cong \mathrm{Mat}_N(A) \rtimes \mathrm{GL}_N(A) = \mathrm{End}_A(V) \rtimes \mathrm{GL}_N(A)$$

with $\mathrm{GL}_N(A)$ acting on $\mathrm{Mat}_N(A)$ via conjugation (in particular we have $\Gamma \cong \mathrm{Mat}_N(A) \cong Ad(\rho)$ also as Π-modules).

The set of deformations $t_\rho = D_\rho(A[\varepsilon])$ is the set of strict equivalence classes of group homomorphisms $\rho' : \Pi \to \mathrm{GL}_N(A[\varepsilon]$ such that $\beta \circ \rho' = \rho$, where recall that ρ' is equivalent to ρ'' if they are conjugate to each other via an element of $\Gamma = \mathrm{Ker}(\beta)$.

Let ρ_0 be the homomorphism $\rho_0 = \sigma \circ \rho$, which certainly defines a class in t_ρ. If ρ' is another lifting of ρ we define the difference cocycle $c_{\rho'} : \Pi \to \Gamma \cong Ad(\rho)$ as

$$c_{\rho'}(g) := \rho'(g) \cdot \rho_0(g)^{-1} \quad \text{for all } g \in \Pi.$$

Note that this is well-defined, i.e. $c_{\rho'}(g)$ actually lies in Γ and it holds

$$c_{\rho'}(g_1 g_2) = c_{\rho'}(g_1) \cdot (g_1 * c_{\rho'}(g_2))$$

Then one checks that sending the class of ρ' in t_ρ to the class of $c_{\rho'}$ in $H^1(\Pi, Ad(\rho))$ defines the required bijection (we omit the details here). □

Remark 17. It is also possible to interpret the elements of the A-module $H^1(\Pi, Ad(\rho))$ as isomorphism classes of (continuous) Γ-torsors, sending the deformation represented by a certain lifting ρ' to the isormorphism class of the torsor given by $\Gamma \cong \mathrm{End}_A(V)$ with regular right Γ-action and left Π-action given by

$$g \cdot_{\rho'} (1 + \varepsilon m) := \rho'(g)(1 + \varepsilon m)\rho_0(g)^{-1}$$

for every $g \in G$ and $m \in \mathrm{Mat}_N(A) = \mathrm{End}_A(V)$.

Proposition 18. *Let A be a coefficient Λ-algebra. Then the Zariski tangent A-module t_ρ is finite over A.*

Sketch of the proof. We will assume that A is artinian. For the proof in the general case we refer to [2], proposition 21.2b.

By the above theorem it is enough to show that $H^1(\Pi, Ad(\rho))$ is a finite A-module. Since A is artinian, the kernel of ρ is an open subgroup of Π, that we denote by Π_0. In this simple situation the inflation-restriction exact sequence for (continuous) group cohomology looks like

$$1 \to H^1(\Pi/\Pi_0, Ad(\rho)) \to H^1(\Pi, Ad(\rho)) \to \mathrm{Hom}_{cont}(\Pi_0, Ad(\rho))^{\Pi/\Pi_0} \to \dots$$

and we have that $H^1(\Pi/\Pi_0, Ad(\rho))$ is finite since Π/Π_0 is a finite group and $Ad(\rho)$ is finite, while $\mathrm{Hom}_{cont}(\Pi_0, Ad(\rho)$ is finite because Π satisfy the p-finiteness condition and $\mathrm{End}_A(V)$ is a finite abelian p-group. The thesis follows. □

5 Presentations of the deformation rings

In this section we work under the assumptions $\Lambda = W(k)$ and $A = k$. In this case we simply denote the category $\hat{\mathcal{C}}_\Lambda(k)$ (resp. $\mathcal{C}_\Lambda(k)$) by $\hat{\mathcal{C}}$ (resp. $\mathcal{C}$). As usual we let

$$\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$$

be a residual representation of our profinite group Π. Assuming that Π satisfies the p-finiteness condition and that $\bar{\rho}$ is absolutely irreducible, we know by theorem 14 that the functor $D_{\bar{\rho}}$ is pro-representable, i.e. there is a unique complete local noetherian ring $R = R(\bar{\rho})$ with residue field k and a deformation represented by a lifting $\rho^{univ} : \Pi \to \mathrm{GL}_N(R)$ of $\bar{\rho}$, such that for all objects A in $\mathcal{C}$ (and actually in $\hat{\mathcal{C}}$) it holds

$$\mathrm{Hom}_{\hat{\mathcal{C}}}(R, A) \cong D_{\bar{\rho}}(A) \qquad f \mapsto [\tilde{f} \circ \rho^{univ}]$$

Moreover we have canonical identifications

$$\mathrm{Hom}_k(\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR), k) \cong \mathrm{Hom}_{\hat{\mathcal{C}}}(R, k[\varepsilon]) \cong D_{\bar{\rho}}(k[\varepsilon]) = t_{\bar{\rho}} \cong H^1(\Pi, Ad(\bar{\rho})).$$

One can expect that (some) obstructions to the existence of deformations might lie in the group $H^2(\Pi, Ad(\bar{\rho}))$. In order to see this we let $A_1 \to A_0$ be a surjective map in $\mathcal{C}$ with kernel I annihilated by $\mathfrak{m}_{A_1}$ (i.e. I endowed with the structure of k-vector space, in particular $I^2 = 0$).

Assume that we are given a deformation ρ_0 represented by a lifting $\rho_0 : \Pi \to \mathrm{GL}_N(A_0)$ of $\bar{\rho}$ (note the abuse of notation here!).

Lemma 19. *With the above notation, there exists an obstruction class*

$$\mathcal{O}(\rho_0) \in H^2(\Pi, Ad(\bar{\rho})) \otimes I = H^2(\Pi, I \otimes Ad(\bar{\rho}))$$

which depends only upon the strict equivalence class of ρ_0 and which vanishes if and only if there exists a deformation $\rho_1 : \Pi \to \mathrm{GL}_N(A_1)$ of $\bar{\rho}$, which when projected to A_0 yields the deformation ρ_0.

Sketch of the proof. A cocycle $c(\rho_0)$ representing the class $\mathcal{O}(\rho_0)$ can be formed setting:

$$c(\rho_0)(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} \in 1 + I \otimes \mathrm{Mat}_N(k) \cong I \otimes Ad(\bar{\rho})$$

for every $g_1, g_2 \in \Pi$, where $\gamma : \Pi \to \mathrm{GL}_N(A_1)$ is any set theoretic map that when projected to $\mathrm{GL}_N(A_0)$ gives a homomorphism in the strict equivalence class of our ρ_0 and where we note that

$$1 + I \otimes \mathrm{Mat}_N(k) = \mathrm{Ker}(\mathrm{GL}_N(A_1) \to \mathrm{GL}_N(A_0)).$$

One can check that $c(\rho_0)$ is indeed a 2-cocycle and that its cohomology class $\mathcal{O}(\rho_0)$ only depends on the strict equivalence class of ρ_0. Assuming this, it trivially follows that if ρ_1 as above exists, then $\mathcal{O}(\rho_0)$ vanishes.

Conversely, assuming that $c(\rho_0)$ is a coboundary, i.e.

$$c(\rho_0)(g_1, g_2) = g_1 * f(g_2) \cdot f(g_1 g_2)^{-1} f(g_1)$$

for a set-theoretic function $f : \Pi \to 1 + I \otimes \mathrm{Mat}_N(k)$, then we leave to the reader the task of checking that

$$\rho_1 : \Pi \to \mathrm{GL}_N(A_1) \qquad g \mapsto f(g) \cdot \gamma(g)$$

is indeed the required lifting (the only thing to check is that with our definition ρ_1 is a group homomorphism!). □

Set $h^i := \dim_k H^i(\Pi, Ad(\bar{\rho}))$ in what follows. We can now state and prove our last result.

Proposition 20. *In the above setting and with the above notation we have that the Krull dimension of $R = R(\bar{\rho})$ satisfies*

$$h^1 - h^2 \leq \dim(R/pR) \leq h^1$$

In particular if $h^2 = 0$ (i.e. if the lifting problem for $\bar{\rho}$ is unobstructed), then it holds $\dim(R/pR) = h^1$ and R is isomorphic to the ring of power series in h^1 variables over $W(k)$. If $h^2 > 0$ we can still find a surjective ring homomorphism

$$\pi : F := W(k)[\![X_1, \ldots, X_{h^1}]\!] \twoheadrightarrow R$$

and given any such π one has a canonical injection of k-vector spaces

$$\mathrm{Hom}_k(\mathrm{Ker}(\pi)/\mathfrak{m}_F \mathrm{Ker}(\pi), k) \hookrightarrow H^2(\Pi, Ad(\bar{\rho})$$

so that $\mathrm{Ker}(\pi)$ is can be generated by at most h^2 elements.

Proof. Denote by D_F the functor on $\mathcal{C}_k$ pro-represented by D_F, so that the Zariski tangent space t_{D_F} is a k-vector space of dimension h_1. One can clearly define a continuous coefficient $W(k)$-algebra homomorphism $\pi : F \to R$ inducing an isomorphism $t_{\bar{\rho}} \cong t_{D_F}$ (just send the variables $X_1, \ldots, X_{h^1}$ to elements of the maximal ideal $\mathfrak{m}_R$ of R generating $\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR)$ as k-vector space).

Since such π will induce the identity at the level of residue fields, one easily sees that it must be surjective. Let $J := \mathrm{Ker}(\pi)$ so that we have an exact sequence

$$0 \to J/\mathfrak{m}_F J \to F/\mathfrak{m}_F J \to R \to 0.$$

One can construct an obstruction class $\vartheta := \mathcal{O}(\rho^{univ}) \in H^2(\Pi, Ad(\bar{\rho})) \otimes J/\mathfrak{m}_F J$ (viewing $A_1 = F/\mathfrak{m}_F J$, $A_0 = R$ and $I = J/\mathfrak{m}_F J$ in the previous lemma). Let $V = \mathrm{Hom}_k(J/\mathfrak{m}_F J, k)$ be the k-dual of $J/\mathfrak{m}_F J$. Then we define a k-linear map

$$V \to H^2(\Pi, AD(\bar{\rho})) \qquad f \mapsto (id \otimes f)(\vartheta)$$

and we claim that it is injective. Note that if this is true then the proof of the proposition is complete.

Assume by contradiction that there exists $f \in V$ non-zero such that $(id \otimes f)(\vartheta) = 0$ and let $J' = (J/\mathfrak{m}_F J)/\mathrm{Ker}(f)$, which is a k-vector space of dimension one fitting in the exact sequence

$$0 \to J' \to R' \xrightarrow{\tilde{\pi}} R \to 0$$

where $R' = (F/\mathfrak{m}_F J)/\mathrm{Ker}(f)$. Then, by construction, the obstruction to have a lifting of ρ^{univ} to R' vanishes and we get a deformation $\rho' \in D_{\bar{\rho}}(R')$, which by universality yields a morphism $\sigma : R \to R'$ such that $\tilde{\pi} \circ \sigma = id_R$ (again by universality), so in particular σ is injective. By our construction of the original π it follows that $\tilde{\pi}$ induces isomorphisms on the tangent spaces $t_{\bar{\rho}} \cong t_{D_{R'}}$, so that σ does the same. Since σ induces the identity on residue fields and R, R' are complete noetherian local rings, this implies that σ must be surjective, i.e. an isomorphism. Then $\tilde{\pi}$ would be an isomorphism, contradicting the fact that $J' = \mathrm{Ker}(\tilde{\pi}) \neq 0$. This finishes the proof. □

References

[1] Barry Mazur. Deforming Galois representations. In *Galois groups over* **Q** *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 385–437. Springer, New York, 1989.

[2] Barry Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 243–311. Springer, New York, 1997.

[3] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[4] Michael Schlessinger. Functors of Artin rings. *Trans. Amer. Math. Soc.*, 130:208–222, 1968.