LECTURES ON DEFORMATIONS OF GALOIS REPRESENTATIONS

Mark Kisin

Lecture 1: Deformations of Representations of pro-finite groups

(1.1) Throughout these notes p will be a rational prime and $\mathbb{F}$ a finite field of characteristic p. We will denote by G be a pro-finite group and $V_{\mathbb{F}}$ a finite dimensional $\mathbb{F}$-vector space equipped with a continuous action of G. We write $n = \dim_{\mathbb{F}} V_{\mathbb{F}}$.

For the first three lectures G will usually be an arbitrary pro-finite group sometimes satisfying a certain finiteness condition. Later we will consider the case where G is the Galois group of a number field or of a finite extension of $\mathbb{Q}_p$.

(1.1.1) Let $\mathfrak{AR}_{W(\mathbb{F})}$ denote the category of finite local, Artinian $W(\mathbb{F})$-algebras with residue field $\mathbb{F}$. If A is in $\mathfrak{AR}_{W(\mathbb{F})}$ then by a *deformation* of $V_{\mathbb{F}}$ to A we mean a finite free A-module V_A equipped with a continuous action of G, and a G-equivariant isomorphism $V_A \otimes_A \mathbb{F} \xrightarrow{\sim} V_{\mathbb{F}}$.

We define a functor $D_{V_{\mathbb{F}}}$ on $\mathfrak{AR}_{W(\mathbb{F})}$ by setting

$$D_{V_{\mathbb{F}}}(A) = \{\text{isomorphisms classes of deformations of } V_{\mathbb{F}} \text{ to A}\}.$$

Fix an $\mathbb{F}$-basis β of $V_{\mathbb{F}}$. A framed deformation of $V_{\mathbb{F}}$ to A is a deformation V_A of $V_{\mathbb{F}}$ to A together with a lift of the chosen $\mathbb{F}$-basis of $V_{\mathbb{F}}$ to an A-basis β_A of V_A. We define

$$D^{\square}_{V_{\mathbb{F}}}(A) = \{\text{isomorphism classes of framed deformations of } V_{\mathbb{F}} \text{ to } A\}$$

Remarks (1.1.2): (1) The fixed basis β allows us to view $V_{\mathbb{F}}$ as a representation

$$\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$$

Then $D^{\square}_{V_{\mathbb{F}}}(A)$ is the set of representations

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

lifting $\bar{\rho}$, while $D_{V_{\mathbb{F}}}(A)$ is the set of such representations modulo the action of $\ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$ acting by conjugation.

(2) As the definition suggests there are *categories* underlying these functors. Although we postpone the explanation of this, it will be important.

(1.2) A finiteness condition: We say that G satisfies the condition Φ_p if for all finite index subgroups $G' \subset G$ the maximal pro-p quotient of G' is topologically finitely generated. This is equivalent to asking that $\mathrm{Hom}(G, \mathbb{F}_p)$ is finite dimensional.

Examples of groups satisfying this condition include the absolute Galois group of a finite extension $K/\mathbb{Q}_p$, and the Galois group $\mathrm{Gal}(F_S/F)$ where F is a number field and F_S is a maximal extension of F unramified outside a finite set of primes S of F. Both these groups are frequently encountered in arithmetic applications.

The following proposition is due to Mazur [Ma].

Proposition (1.2.1). *Assume G satisfies Φ_p. Then*

1. *$D^{\square}_{V_{\mathbb{F}}}$ is pro-representable by a complete local (Noetherian) $W(\mathbb{F})$-algebra $R^{\square}_{V_{\mathbb{F}}}$.*
2. *If $\mathrm{End}_{\mathbb{F}[G]} V_{\mathbb{F}} = \mathbb{F}$ then $D_{V_{\mathbb{F}}}$ is a pro-representable by a complete local $W(\mathbb{F})$-algebra $R_{V_{\mathbb{F}}}$ called the universal deformation ring of $V_{\mathbb{F}}$.*

Remarks (1.2.2) (1) The condition Φ_p is not really necessary for the proposition by its suppression leads to non-Noetherian rings.

(2) Recall that (pro-)representability (for example for $D^{\square}_{V_{\mathbb{F}}}$ means that there exists an isomorphism

$$D^{\square}_{V_{\mathbb{F}}}(A) \xrightarrow{\sim} \mathrm{Hom}_{W(\mathbb{F})}(R^{\square}_{V_{\mathbb{F}}}, A)$$

which is functorial in A.

In particular, the identity map in $\mathrm{Hom}(R^{\square}_{V_{\mathbb{F}}}, R^{\square}_{V_{\mathbb{F}}})$ gives rise to a universal framed deformation over $R^{\square}_{V_{\mathbb{F}}}$.

(3) Note that when the conditions in (2) of the Proposition hold the map of local $W(\mathbb{F})$-algebras $R_{V_{\mathbb{F}}} \to R^{\square}_{V_{\mathbb{F}}}$ is formally smooth, thus the singularities of these two rings are in some sense equivalent.

In general even if $D_{V_{\mathbb{F}}}$ is not representable there is a sense in which it has an intrinsic geometry. However this is best formulated in terms of groupoids and we postpone it till later.

Proof. Proof of (i). Let $G' = \ker(\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F}))$. For any lift $\rho_A : G \to \mathrm{GL}_n(A)$ of $\bar{\rho}$, $\rho_A|_{G'}$ factors through $\ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$ which is a pro-p group, and hence $\rho_A|_{G'}$ factors through the maximal pro$-p$ quotient of G'. Write this quotient as G'/H for H a normal subgroup of G', which is also normal in G.

By assumption, G'/H is topologically finitely generated and hence so is G/H. Let $\gamma_1, \dots, \gamma_s$ be topological generators of G/H. Then $R^{\square}_{V_{\mathbb{F}}}$ is a quotient of $W(\mathbb{F})[\![X_i^{j,k}]\!]$ where $i = 1, \dots, s$ and $k, j = 1, \dots, n^2$. and the universal deformation is given by

$$\gamma_i \mapsto (X_i^{j,k}) + [\rho](\gamma_i)$$

where $[\rho](\gamma_i) \in \mathrm{GL}_n(W(\mathbb{F}))$ denotes the matrix whose entries are the Teichmïler representatives of the entries of $\rho(\gamma_i)$.

The second part of the proposition will be proved later. We will give a somewhat different proof to the original one of Mazur which uses Schlessinger's representability criterion. To explain the idea let $\widehat{\mathrm{PGL}}_n$ denote the completion of the group PGL_n over $W(\mathbb{F})$ along its identity section. Then $\widehat{\mathrm{PGL}}_n$ acts on the functor $D^{\square}_{V_{\mathbb{F}}}$ by conjugation and hence it acts on the formal scheme $\mathrm{Spf}\, R^{\square}_{V_{\mathbb{F}}}$. The condition $\mathrm{End}_{\mathbb{F}[G]} V_{\mathbb{F}} = \mathbb{F}$ implies that this action is free, and the idea is to define

$$\mathrm{Spf}\, R_{V_{\mathbb{F}}} = \mathrm{Spf}\, R^{\square}_{V_{\mathbb{F}}} / \widehat{\mathrm{PGL}}_n$$

(1.3) Tangent Spaces: Let $\mathbb{F}[\epsilon] = \mathbb{F}[X]/X^2$ denote the dual numbers.

Lemma (1.3.1).

(1) *There is a canonical isomorphism*

$$D_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon]) \xrightarrow{\sim} H^1(G, \mathrm{ad}V_{\mathbb{F}})$$

where $\mathrm{ad}V_{\mathbb{F}}$ *denotes the* G*-representation* $\mathrm{End}_{\mathbb{F}}V_{\mathbb{F}}$.

(2) *If* G *satisfies* Φ_p *then* $D_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon])$ *is a finite dimensional* $\mathbb{F}$*-vector space and satisfies*

$$\begin{aligned}\dim_{\mathbb{F}} D^{\square}_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon]) &= \dim_{\mathbb{F}} D_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon]) + n^2 - \dim_{\mathbb{F}}(\mathrm{ad}V_{\mathbb{F}})^G \\ &= n^2 + H^1(G, \mathrm{ad}V_{\mathbb{F}}) - H^0(G, \mathrm{ad}V_{\mathbb{F}}).\end{aligned}$$

Proof. An element of $D_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon])$ $V_{\mathbb{F}[\epsilon]}$ gives rise to an extension

$$0 \to V_{\mathbb{F}} \to V_{\mathbb{F}[\epsilon]} \to V_{\mathbb{F}} \to 0$$

where we have identified $\epsilon \cdot V_{\mathbb{F}[\epsilon]}$ with $V_{\mathbb{F}}$. Thus we obtain a class in

$$\mathrm{Ext}^1_G(V_{\mathbb{F}}, V_{\mathbb{F}}) \xrightarrow{\sim} H^1(G, \mathrm{ad}V_{\mathbb{F}}).$$

Conversely an element of $H^1(G, \mathrm{ad}V_{\mathbb{F}})$ gives rise to an extension of one copy of $V_{\mathbb{F}}$ by another $V_{\mathbb{F}}$, and such an extension can be viewed as an $F[\epsilon]$-module, with multiplication by ϵ identifying the two copies of $V_{\mathbb{F}}$.

To prove the second part of the lemma, fix a deformation of $V_{\mathbb{F}}$ to $\mathbb{F}[\epsilon]$ $V_{\mathbb{F}[\epsilon]}$. The set of $\mathbb{F}[\epsilon]$-bases of $V_{\mathbb{F}[\epsilon]}$ lifting a fixed basis of $V_{\mathbb{F}}$ is an $\mathbb{F}$-vector space of dimension n^2. Let β', β'' be two such lifted bases. Then there is an isomorphism of framed deformations

$$(V_{\mathbb{F}[\epsilon]}, \beta') \xrightarrow{\sim} (V_{\mathbb{F}[\epsilon]}, \beta'')$$

if and only if there is an automorphism of $V_{\mathbb{F}[\epsilon]}$ which is the identity mod ϵ and takes β' to β''. That is, the fibres of

$$D^{\square}_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon]) \to D_{V_{\mathbb{F}}}(\mathbb{F}[\epsilon])$$

are $\mathrm{ad}V_{\mathbb{F}}/(\mathrm{ad}V_{\mathbb{F}})^G$ torsors. The lemma follows. □

(1.4) Traces: Absolutely irreducible representations of finite groups are determined by their trace functions. A result of Carayol [Ca] and Mazur [Ma] says that the analogous result holds also for deformations:

Theorem (1.4.1). *(Mazur, Carayol): Suppose that* $V_{\mathbb{F}}$ *is absolutely irreducible. If* A *is in* $\mathfrak{AR}_{W(\mathbb{F})}$ *and* $V_A, V'_A \in D_{V_{\mathbb{F}}}(A)$ *are deformations such that* $\mathrm{tr}(\sigma|V_A) = \mathrm{tr}(\sigma|V'_A)$ *for all* $\sigma \in G$*, then* V_A *and* V'_A *are isomorphic deformations.*

Proof. We give (one of) Carayol's argument(s).

Fix bases for V_A and V'_A and extend the resulting representations to A-linear maps

$$\rho_A, \rho'_A : A[G] \to M_n(A).$$

We have to show that the bases can be chosen so that $\rho_A = \rho'_A$.

Let $\mathfrak{m}_A$ be the radical of A, and $I \subset A$ an ideal such that $I \cdot \mathfrak{m}_A = 0$. By induction on the length of A, we may assume that $\rho_A = \rho'_A$ modulo I, and write $\rho_A = \rho'_A + \delta$ where for $\sigma \in A[G]$, $\delta(\sigma) \in M_n(I)$ has trace 0.

As ρ_A, ρ'_A are multiplicative we find that for $\sigma_1, \sigma_2 \in A[G]$

$$\delta(\sigma_1\sigma_2) = \bar{\rho}(\sigma_1)\delta(\sigma_2) + \delta(\sigma_1)\bar{\rho}(\sigma_2).$$

If $\sigma_2 \in \ker \bar{\rho}$, we get $\delta(\sigma_1\sigma_2) = \bar{\rho}(\sigma_1)\delta(\sigma_2)$ for all $\sigma \in A[G]$, so $\mathrm{tr}(\bar{\rho}(\sigma_1)\delta(\sigma_2)) = 0$ for all $\sigma_1 \in A[G]$. But by Burnside's theorem $\bar{\rho}(\mathbb{F}[G]) = M_n(\mathbb{F})$ as $\bar{\rho}$ is absolutely irreducible. Hence $\mathrm{tr}(X\delta(\sigma_2)) = 0$ for any $X \in M_n(\mathbb{F})$, so $\delta(\sigma_2) = 0$.

It follows that δ may be regarded as a *derivation*

$$\delta : M_n(\mathbb{F}) \to M_n(I) := M_n(\mathbb{F}) \otimes_{\mathbb{F}} I$$

on $M_n(\mathbb{F})$. Such a derivation is always *inner*:

$$\exists U \in M_n(I) \text{such that} \delta(\sigma) = \bar{\rho}(\sigma)U - U\bar{\rho}(\sigma).$$

Hence $\rho'_A = (1 - U)\rho_A(1 + U)$. $\square$

(1.5) Exercises:

Exercise 1: Show that the following are equivalent:

(1) For all open subgroups $G' \subset G$ the maximal pro-p quotient of G' is topologically finitely generated
(2) For all $G' \subset G$ as above $\mathrm{Hom}(G', \mathbb{F}_p)$ is finite dimensional over $\mathbb{F}_p$.
(3) For all $G' \subset G$ as above, and all continuous representations of G' on a finite dimensional $\mathbb{F}$-vector space W, $H^1(G', W)$ is finite dimensional

Exercise 2: Show that

$$\mathrm{Ext}^1_G(V_{\mathbb{F}}, V_{\mathbb{F}}) \xrightarrow{\sim} H^1(G, \mathrm{ad}V_{\mathbb{F}}).$$

Exercise 3:

(1) Give an example where $V_{\mathbb{F}}$ is not absolutely irreducible and there exist non-isomorphic deformations $V_A, V'_A \in D_{V_{\mathbb{F}}}(A)$ with the same traces. (Hint: Consider two character $\chi_1, \chi_2 : G \to F^\times$ with $\dim_{\mathbb{F}} \mathrm{Ext}^1(\chi_1, \chi_2) > 1$.)
(2) Show that if $\chi_1, \chi_2 : G \to \mathbb{F}^\times$ are distinct characters with such that $\mathrm{Ext}^1(\chi_1, \chi_2)$ are 1-dimensional, and $V_{\mathbb{F}}$ is an extension of chi_1 by χ_2 then the analogue of Carayol's theorem hold for $V_{\mathbb{F}}$: any deformation of $V_{\mathbb{F}}$ is determined by its trace.

Exercise 4: Suppose $R_{V_{\mathbb{F}}}$ pro-represents $D_{V_{\mathbb{F}}}$. Let $E/W(\mathbb{F})[1/p]$ be a finite extension and $x : R_{V_{\mathbb{F}}}[1/p] \to E$ am E-valued point such that the ideal $\ker x$ has residue field E. Specializing the universal representation over $R_{V_{\mathbb{F}}}$ by x produces a representation of G on a finite dimensional E-vector space V_x.

Let $\widehat{R}_x$ denote the complete local ring at the point $\ker x \in \mathrm{Spec}\, R_{V_{\mathbb{F}}}[1/p]$. Show that $\widehat{R}_x$ is the universal deformation ring of V_x.

Formulate and prove the analogous statement for $R^{\square}_{V_{\mathbb{F}}}$.

References

[Ca] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), Contemp. Math., 165,, Amer. Math. Soc., 1994, pp. 213-237.

[Ma] B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ. 16, Springer, New York-Berlin, pp. 395-437, 1989.