

Galois representations and their deformations.

A. CONTI (3/225) andrea.conti@iwr.uni-heidelberg.de

Goal: study representations of Galois groups of p -adic or number fields with p -adic coefficients, by "deforming" representations with modulo p coefficients.

References:

- * Gouvêa, notes
- * Böckle, notes
- * Mazur's article "Deforming Galois representations"
- * Mézard, notes

01. Galois groups

K perfect field, L a normal extension of K . Define $\text{Gal}(L/K)$
 $= \{\sigma : L \rightarrow L \mid \sigma \text{ field automorphism}, \sigma|_K = \text{id}_K\}$

Topology:

- * if $L|K$ is finite then give $\text{Gal}(L|K)$ the discrete topology
- * if $L|K$ is infinite then give $\text{Gal}(L|K)$ the Krull topology:
 a basis of open neighborhoods of id_L is the collection of sets
 $\{\sigma \in \text{Gal}(L|K) \mid \sigma|_E = \text{id}_E\}$ where E varies over the finite
 subextensions $E|K$

As groups: $\text{Gal}(L|K) \cong \varprojlim_{\substack{E|K \text{ finite and normal} \\ E \subseteq L}} \text{Gal}(E|K)$

If $\text{Gal}(E|K)$ has the discrete topology, then this is an isomorphism of topological groups.

This makes $\text{Gal}(L|K)$ into a profinite group.

$\Rightarrow \text{Gal}(L|K)$ is compact and hausdorff.

\Rightarrow Open subgroups are the closed subgroups of finite index

Theorem. (**Galois correspondence**) The map

$$\begin{array}{ccc} \left\{ \text{subextensions } L \mid E \subset K \right\} & \longrightarrow & \left\{ \substack{\text{closed subgroups} \\ \text{of } \text{Gal}(L|K)} \right\} \\ E & \longmapsto & \text{Gal}(L|E) \end{array} \quad \text{is a bijection.}$$

The inverse is $H \mapsto E = L^H$.

This induces a bijection

$$\begin{array}{ccc} \left\{ \substack{L|E \subset K, \\ E \subset K \text{ finite}} \right\} & \longrightarrow & \left\{ \substack{\text{open subgroups} \\ \text{of } \text{Gal}(L|K)} \right\} \end{array}$$



When $L = K^{\text{alg}}$, we call $\text{Gal}(K^{\text{alg}}|K)$ the **absolute Galois group** of K , we write G_K .

Examples. * $K = \mathbb{F}_p$, we know that finite extensions are of the form \mathbb{F}_{p^n} and

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \quad \text{is an isomorphism.}$$

$$(x \mapsto x^p) \longmapsto 1$$

"Frobenius element"

$$\text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) = \varprojlim_{n \rightarrow \infty} \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\sim} \varprojlim_{n \rightarrow \infty} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}$$

$$\begin{aligned} (\text{the maps are } \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) &\longrightarrow \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \quad m \mid n \text{ with } m \mid n \\ d &\longmapsto d|_{\mathbb{F}_{p^m}} \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ x &\longmapsto x \bmod m \end{aligned}$$

The Frobenius of $\text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p)$ is mapped to $1 \in \hat{\mathbb{Z}}$.

* $k = \mathbb{Q}_p$; we denote by \mathbb{Q}_p^{ur} the maximal unramified extension of \mathbb{Q}_p .

(\hookrightarrow maximal extension for which p is still a uniformizer (generator of the maximal ideal of the valuation ring))

Valuation ring \mathbb{Z}_p^{ur} has residue field $\mathbb{Z}_p^{\text{ur}}/\mathfrak{p}\mathbb{Z}_p^{\text{ur}} \cong \mathbb{F}_p^{\text{alg}}$

There is a map $\text{Gal}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p) \rightarrow \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p)$

$$d \longmapsto d \bmod p$$

This map is a group isomorphism.

$$\begin{array}{c} \mathbb{Q}_p^{\text{alg}} \\ | \\ \mathbb{Q}_p \\ | \end{array} \xrightarrow{\quad \text{"Inertia group"} \quad} (\mathbb{I}_p) \\ \text{topologically generated by } \text{Frob}_p$$

* $K = \mathbb{Q}$, $\text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$, let p be prime.
 Choose an extension of the p -adic valuation on \mathbb{Q} to \mathbb{Q}^{alg} (not unique!)
 (\hookrightarrow choose an embedding $\mathbb{Q}^{\text{alg}} \rightarrow \mathbb{Q}_p^{\text{alg}}$)

Write a map $\text{Gal}(\mathbb{Q}_p^{\text{alg}}/\mathbb{Q}_p) \rightarrow \text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$

$$\sigma \mapsto \sigma|_{\mathbb{Q}^{\text{alg}}}$$

This map is an injective group homomorphism and it identifies $\text{Gal}(\mathbb{Q}_p^{\text{alg}}/\mathbb{Q}_p)$ with a subgroup $\mathcal{D}_p \subseteq \text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$

$$\mathcal{D}_p = \left\{ \sigma \in \text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q}) \mid v(\sigma^{-1}(x)) = v(x) \quad \forall x \in \mathbb{Q}^{\text{alg}} \right\}$$

We have injections

$$\mathbb{I}_p \subseteq \mathcal{D}_p \subseteq \text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$$

O2. Galois groups for extensions unramified outside a finite set.

K number field, S is a finite set of places of K .

Def. 1) K^S is the largest extension of K that is unramified at all places not in S .

$$2) G_{K,S} := \text{Gal}(K^S/K)$$

Remark. $v \notin S$, then we have $\text{Gal}(K_v^{\text{alg}}/K_v) \hookrightarrow \text{Gal}(K^{\text{alg}}/K) \rightarrow \text{Gal}(K^S/K)$

Answer: injection when $K = \mathbb{Q}$, $\#S \geq 2$

Injection?

Exercise. An open subgroup $H \subseteq G_{K,S}$ has the form G_{K_1, S_1} where $K_1 | K$ is finite and S_1 is a set of places of K_1 .

(places in S_1 have to lie over the places of S
 $\Rightarrow S_1$ finite)

Theorem. (Hasse-Minkowski) Let K, S as before.

Let $d \in \mathbb{N}_{>0}$. Then there are only finitely many extensions of K of degree d and unramified outside S .

Corollary. $\text{Hom}_{\text{cont}}(G_{K,S}, \mathbb{F}_p)$ is finite. (Morphisms of topological groups)

Corollary. For every open subgroup $H \leq G_{K,S}$, $\text{Hom}_{\text{cont}}(H, \mathbb{F}_p)$ is finite.

\Leftarrow Def. $G_{K,S}$ satisfies the " p -finiteness condition".

(\mathbb{F}_p has the discrete topology)

03. Galois representations

Let G be a profinite group and let A be a topological ring.

Def. A **continuous representation** of G with A -coefficients is a continuous group homomorphism $\rho: G \rightarrow GL_n(A)$ for some integer n .

Given representations $\rho_1, \rho_2: G \rightarrow GL_n(A)$, we say that they are equivalent iff. $\exists P \in GL_n(A): \rho_1 = P^{-1} \cdot \rho_2 \cdot P$

Another point of view: let M be a finite free A -module of rank n .

Then a continuous representation $\rho: G \rightarrow GL_n(A)$ gives a continuous action $G \curvearrowright M$

$$G \times M \rightarrow M$$

$$(g, m) \mapsto \rho(g)(m)_{i=1..n}$$

where $(m_i)_{i=1..n}$ are coordinates of m

Def.

We call ρ a **Galois representation** if G is:

- * $\text{Gal}(K^{\text{alg}}/K)$ for a finite extension $K \mid \mathbb{Q}_p$

- * $G_{K,S}$ for a number field K and a finite set of places S .

From now on G is one of those groups.

Choices of coefficient ring A :

1) $A = \mathbb{C}$

2) $A = \mathbb{F}_p$

3) $A = \mathcal{O}_E$ for $E \mid \mathbb{Q}_p$ finite

4) $A = E$, $E \mid \mathbb{Q}_p$ finite

① $A = \mathbb{C}$

Proposition. A representation $\rho: G \rightarrow GL_n(\mathbb{C})$ has finite image.

Proof. Consider an open neighborhood U of $\mathbb{1}_n \in GL_n(\mathbb{C})$. If U is sufficiently small, the

only subgroup $\subseteq U$ is $\{\mathbb{1}_n\}$ (Exercise). By continuity of ρ , $\exists V$ open neighborhood of $e \in G$ such that $\rho(V) \subseteq U$. We can choose V' a neighborhood of e which is an open subgroup of G and s.t. $V' \subseteq V$. Then $\rho(V') \subseteq \rho(V) \subseteq U$.

$\Rightarrow \rho(V') = \{\mathbb{1}_n\}$. Since V' is of finite index in G , $\rho(V')$ is of finite index in $\rho(G)$.

Expl. Take $K \mid \mathbb{Q}$ Galois, finite. Then $\text{Gal}(K \mid \mathbb{Q}) \hookrightarrow GL_n(\mathbb{C})$. □

② Proposition. If $\rho: G \rightarrow \mathrm{GL}_n(\mathbb{F}_p^{\text{alg}})$ is a continuous representation,
 $(\mathrm{GL}_n(\mathbb{Q}_p))$
then it factors through $\rho': G \rightarrow \mathrm{GL}_n(\mathbb{F}_{p^m})$ for some finite extension
 $\mathbb{F}_{p^m} / \mathbb{F}_p$
 E / \mathbb{Q}_p

Proof. Similar for \mathbb{F}_p , more difficult for \mathbb{Q}_p . □

07

Proof of the last Proposition.

Look at $\rho(G) \subseteq GL_n(\bar{\mathbb{Q}_p})$. It is a compact Hausdorff topological group

\Rightarrow Baire's Lemma holds for $\rho(G)$.

(Baire's Lemma: a countable union of nowhere dense closed subspaces of X is nowhere dense in X .)

Nowhere dense: it does not contain any open set of X)

$$GL_n(\bar{\mathbb{Q}_p}) = \bigcup_{\substack{E/\mathbb{Q}_p \\ \text{finite}}} GL_n(E) \quad \text{countable union of closed subsets.}$$

($\forall n \in \mathbb{N}$: there are only finitely many E/\mathbb{Q}_p st. $|E : \mathbb{Q}_p| = n$)

Write $\rho(G) = \bigcup_{\substack{E/\mathbb{Q}_p \\ \text{finite}}} (GL_n(E) \cap \rho(G))$. Either there exists E/\mathbb{Q}_p finite such

that $GL_n(E) \cap \rho(G)$ has finite index in $\rho(G)$

\Rightarrow We can choose $F \subseteq E$ finite such that $\rho(G) \subseteq GL_n(F)$ (finite index -)

Or for every E/\mathbb{Q}_p finite, $GL_n(E) \cap \rho(G)$ has infinite index in $\rho(G)$

$\Rightarrow GL_n(E) \cap \rho(G)$ is nowhere dense in $\rho(G)$ (Basis of open subgroups
 \Rightarrow open subgroups in compact spaces are of finite index)

Now $\rho(G)$ is a countable union of nowhere dense sets \Rightarrow Contradicts Baire's Lemma. □

Lemma. If $\rho: G \rightarrow GL_n(K)$ is a continuous representation with coefficients in K/\mathbb{Q}_p

finite, then there exists a continuous representation $\rho': G \rightarrow GL_n(\mathcal{O}_K)$ such that

if $i: GL_n(\mathcal{O}_K) \rightarrow GL_n(K)$ is the inclusion $\rho' \stackrel{\text{equivalent}}{\equiv} i \circ \rho$

Proof. Recall: an \mathcal{O}_K -lattice in K^n is a free \mathcal{O}_K -module L of rank n such that $L \otimes_{\mathcal{O}_K} K \cong K^n$.

Choosing a basis for K^n we obtain a continuous action of G on K^n via ρ .

Let L be any lattice in K^n . For $g \in GL_n(K)$ let $g(L) := \{g(x) \mid x \in L\}$

Exercise: $g(L)$ is a lattice, and $\text{Stab}(L) = \{g \in GL_n(K) \mid g(L) \subseteq L\}$ is an open subgroup of $GL_n(K)$. Ex

Look at $\underbrace{\rho^{-1}(\text{Stab}(L))}_{\substack{\text{open} \\ \subseteq GL_n(K)}} \subseteq G \Rightarrow \underbrace{\rho^{-1}(\text{Stab}(L))}_{G \text{ compact}}$ has finite index in G .

08

Choose a set $\{g_1, \dots, g_m\}$ of representatives for $\frac{G}{\tilde{g}^{-1}(\text{stab}(L))}$.

Then define

$$L' := \sum_{i=1}^m g(g_i)(L). \quad \text{We check that the lattice } L' \text{ is } G\text{-stable.}$$

$$(G\text{-stable: } g(g)L' \subseteq L' \quad \forall g \in G)$$

Choose an \mathcal{O}_K -basis for the lattice L' , then the action of G on L' gives a (continuous) representation $\rho': G \rightarrow \text{GL}_n(\mathcal{O}_K)$

$$\text{By construction } \iota \circ \rho' \sim \rho \quad \blacksquare$$

Start with $\rho: G \rightarrow \text{GL}_n(K)$ continuous representation.

Then by the Lemma we can choose a conjugate of ρ with values in $\text{GL}_n(\mathcal{O}_K)$.

Then we can reduce modulo the maximal ideal $m_K \subset \mathcal{O}_K$ and we obtain a "residual" representation $\bar{\rho}: G \rightarrow \text{GL}_n(\underbrace{\mathcal{O}_K/m_K}_{=\mathbb{F}_p})$ attached to ρ .

Def. If G acts on a finite free module M . Choose a filtration $M \supseteq M_n \supseteq \dots \supseteq \{0\}$

in G -stable A -modules such that $\frac{M_i}{M_{i-1}}$ is an irreducible $A[G]$ -module.
(A : field)

(Does not admit any G -stable submodule)

Then the semi-simplification of M is the $A[G]$ -module $\bigoplus_{i=1}^n \frac{M_i}{M_{i-1}}$.

$$\text{Example: If } \rho(g) = \begin{pmatrix} \chi_1(g) & \delta(g) \\ 0 & \chi_2(g) \end{pmatrix} \rightarrow \bar{\rho}^{\text{ss}}(g) = \begin{pmatrix} \chi_1(g) & 0 \\ 0 & \chi_2(g) \end{pmatrix}$$

χ_1, χ_2 : Character of ρ

Remark: the representation $\bar{\rho}^{\text{ss}}$ attached to ρ is well-defined up to equivalence.

$$K \longrightarrow \mathcal{O}_K \longrightarrow \mathbb{F}_{p^m}$$

* - - - - -

Idea: fix $\bar{\rho}: G \rightarrow \mathrm{GL}_n(\mathbb{F}_{p^m})$ and look at $\rho: G \rightarrow \mathrm{GL}_n(\mathcal{O}_K)$
 (with $\mathcal{O}_K/m_K = \mathbb{F}_{p^m}$) such that $\rho \bmod m_K = \bar{\rho}$.

Example of p -adic Galois representation. (" p -adic cyclotomic character")
 (p prime, $n \in \mathbb{N}_{\geq 1}$)

$$\chi_n: G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times (= \mathrm{GL}_1(\mathbb{Z}/p^n\mathbb{Z}))$$

This representations are compatible with the maps $(\mathbb{Z}/p^m\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ for $m \geq n$.

$$\chi_m \bmod p^n = \chi_n.$$

We can take $\varprojlim_n \chi_n : G_{\mathbb{Q}} \rightarrow \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$

$$\text{Write } \mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$$

We call χ_{cyc} the p -adic cyclotomic character. χ_{cyc} factors through

$$G_{\mathbb{Q}, p^\infty} \longrightarrow \mathbb{Z}_p^\times. \text{ It also factors through } G_{\mathbb{Q}}^{\mathrm{ab}} \longrightarrow \mathbb{Z}_p^\times.$$

Theorem: (Kronecker-Weber) The product of all cyclotomic characters gives an isomorphism

$$G_{\mathbb{Q}}^{\mathrm{ab}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p^\times.$$

Look at "deformation functors". $=: h_R$

* \mathcal{C} -category, $R \in \mathcal{C}$, then $\mathrm{Hom}_{\mathcal{C}}(R, -): \mathcal{C} \rightarrow \underline{\mathrm{Set}}$ is the functor

$$A \mapsto \mathrm{Hom}_{\mathcal{C}}(R, A), \quad f \in \mathrm{Mor}_{\mathcal{C}}(A, B) \mapsto \begin{cases} \mathrm{Hom}_{\mathcal{C}}(R, A) \rightarrow \mathrm{Hom}_{\mathcal{C}}(R, B) \\ g \mapsto f \circ g \end{cases}$$

We will work with some categories of rings.

Fix a field k . We denote by \mathcal{C}_k the category whose objects are Artinian, local rings with residue field k and morphisms are local ring morphisms, that induce the identity on k .

10

Examples. * If $k = \mathbb{F}_p$, then $\mathbb{Z}_{p^n} \in \mathcal{C}_{\mathbb{F}_p}$ $\forall n \in \mathbb{N}_{>0}$.

$$\mathbb{F}_p[[T]] / T^n$$

* \exists unique degree n unramified extension of \mathbb{Q}_p , we will denote it

by \mathbb{Q}_{p^n} . We write \mathbb{Z}_{p^n} for its valuation ring, then $\mathbb{Z}_{p^n}/p \mathbb{Z}_{p^n} = \mathbb{F}_{p^n}$

$\forall m \in \mathbb{N}_{>0}$: $\mathbb{Z}_{p^n}/p^m \mathbb{Z}_{p^n} \in \mathcal{E}_{\mathbb{F}_{p^m}}$

$\mathbb{Z}_{p^n}/p^m \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}/p^m \mathbb{Z}_{p^n}$ This is not a morphism in $\mathcal{C}_{\mathbb{F}_{p^m}}$ if $m \geq 2$.

$x \pmod{p^m} \mapsto \text{Frob}_p(x) \pmod{p^m}$

Let $\hat{\mathcal{E}}_k$ be the category whose objects are complete local Noetherian rings with residue field k , morphisms are local ring morphisms that induce the identity on k .

Example. $\mathbb{Z}_{p^n} \in \hat{\mathcal{E}}_{\mathbb{F}_{p^n}}$ | An object of \mathcal{E}_k is also an object in $\hat{\mathcal{E}}_k$
 $\mathbb{F}_{p^n}[[T]]$ | (same for morphisms)

DEFORMATION FUNCTORS

Fix $n \geq 1$.

Let G be a profinite group, k a finite field. Fix a continuous representation

$$\bar{\rho}: G \rightarrow \text{GL}_n(k).$$

Def. For $A \in \hat{\mathcal{E}}_k$, a deformation (of $\bar{\rho}$ to A) is a continuous representation

$$\rho: G \rightarrow \text{GL}_n(A) \text{ such that } \rho \pmod{m_A} = \bar{\rho}.$$

We say that $\rho_1, \rho_2: G \rightarrow \text{GL}_n(A)$ are strictly equivalent iff. $\exists M \in \text{ker}(\text{GL}_n(A) \rightarrow \text{GL}_n(k))$

$$\text{such that } M^{-1} \rho_1 M = \rho_2.$$

Remark: if $A \xrightarrow{f} B$ is a morphism in $\hat{\mathcal{E}}_k$ and $\rho_1, \rho_2: G \rightarrow \text{GL}_n(A)$ are strictly equivalent representations, then $f \circ \rho_1, f \circ \rho_2: G \rightarrow \text{GL}_n(B)$ are strictly equivalent.

11

We define $\hat{D}_{\bar{g}} : \hat{\mathcal{E}}_k \rightarrow \underline{\text{Set}}$ as the functor

* $\hat{D}_{\bar{g}}(A) := \left\{ \begin{array}{l} \text{deformations of} \\ \bar{g} \text{ to } A \end{array} \right\}$
strict equivalence

* $\hat{D}_{\bar{g}}(f)$ maps a deformation $g : G \rightarrow GL_n(A)$ to the class of $f \circ g$
 $f : A \rightarrow B$ morphism in $\hat{\mathcal{E}}_k$

(We obtain a functor $D_{\bar{g}} : \mathcal{E}_k \rightarrow \underline{\text{Set}}$ by restricting $\hat{D}_{\bar{g}}$ to \mathcal{E}_k)

Goal: show that $D_{\bar{g}}$ is "pro-represented" by some $R \in \hat{\mathcal{E}}_k$, in the sense

that $D_{\bar{g}} \cong \text{Hom}_{\hat{\mathcal{E}}_k}(R, \cdot)$

02.05.18

Fix any $\Lambda \in \hat{\mathcal{E}}_k$. We define \mathcal{E}_Λ as the category of local Artinian Λ -algebras with residue field k and local morphisms of Λ -algebras (that induce the identity on k)

* $\hat{\mathcal{E}}_\Lambda =$ category of complete local Noetherian Λ -algebras with residue field k . Morphisms as above.

The natural choice for Λ (when working in $\text{char } k = 0$) is the ring of Witt vectors $W(k)$ of k .
(= unique complete discrete valuation ring with residue field k and uniformizer p).
(Mézard's notes, Serre "Local fields")

We only need

$W(\mathbb{F}_{p^n}) = \mathbb{Z}_{p^n}$ ring of integers in \mathbb{Q}_{p^n}

$\hat{\mathcal{E}}_{\mathbb{Z}_{p^n}} \ni \mathbb{Z}_{p^n}, \quad \mathbb{F}_{p^n}[[T]] \in \hat{\mathcal{E}}_{\mathbb{F}_{p^n}}, \text{ but } \notin \hat{\mathcal{E}}_{\mathbb{Z}'_{p^n}}$

Deformation functors Fix $\bar{g} : G \rightarrow GL_n(k)$; We defined $D_{\bar{g}} : \mathcal{E}_k \rightarrow \underline{\text{Set}}$, $\hat{D}_{\bar{g}} : \hat{\mathcal{E}}_k \rightarrow \underline{\text{Set}}$.
one defines

$D_{\bar{g}, \Lambda} : \mathcal{E}_\Lambda \rightarrow \underline{\text{Set}}$ by $D_{\bar{g}, \Lambda}(A) = \left\{ \begin{array}{l} \text{deformations of} \\ \bar{g} \text{ to } A \end{array} \right\}$
strict equivalence

$\hat{D}_{\bar{g}, \Lambda} : \hat{\mathcal{E}}_\Lambda \rightarrow \underline{\text{Set}}$ in the same way.

Representable Functors.

Let \mathcal{C} be any category, $F: \mathcal{C} \rightarrow \underline{\text{Set}}$ any functor.

* F is called representable : $\Leftrightarrow \exists A \in \mathcal{C}: F \cong \text{Hom}_{\mathcal{C}}(A, \cdot)$, as functors.

For our categories $\mathcal{E}_k, \hat{\mathcal{E}}_k, \dots$ we define the following:

* $F: \mathcal{E}_1 \rightarrow \underline{\text{Set}}$ is pro-representable : $\Leftrightarrow \exists R \in \hat{\mathcal{E}}_1$ and an isomorphism of functors

$$\begin{aligned} \text{Hom}_{\hat{\mathcal{E}}_1}(R, \cdot) &\longrightarrow F \\ (\text{as a functor} \\ \mathcal{E}_1 \rightarrow \underline{\text{Set}}) \end{aligned}$$

Why representability?

Assume $D_{\bar{S}, 1}$ is (pro-)representable by some R in $\hat{\mathcal{E}}_1$: means that there is a

bijection $\text{Hom}_{\hat{\mathcal{E}}_1}(R, A) \rightarrow D_{\bar{S}, 1}(A)$ for every $A \in \mathcal{E}_1$.

Take $A = R$. Then there is a strict equivalence class ρ_R in $D_{\bar{S}, 1}(R)$ corresponding to id_R .

Then the bijection

$$\begin{aligned} \text{Hom}_{\hat{\mathcal{E}}_1}(R, A) &\longrightarrow D_{\bar{S}, 1}(A) \\ (f: R \rightarrow A) &\longmapsto \text{class of} \\ f \circ \rho_R: G &\rightarrow GL_n(A) \end{aligned}$$

We call (R, ρ_R) a universal couple, R is the universal deformation ring of \bar{S} , ρ_R is the universal deformation of $\bar{\rho}$.

(pro-)

Properties of representable functors $\mathcal{E}_1 \xrightarrow{F} \underline{\text{Set}}$. In this section F is a pro-representable

- left exact
- $F(k) = \{*\}$, since the only

element of $\text{Hom}_{\hat{\mathcal{E}}_1}(R, k)$ is $R \xrightarrow{\sim} R/m_R \cong k$

one fixed identification

- ~~F is continuous (later)~~

- F behaves well with respect to fiber products

$$k[\varepsilon] = \frac{k[T]}{T^2}, \quad \varepsilon = T \quad (\text{ring with } \varepsilon^2=0)$$

$$k[\varepsilon] = \{a+b\varepsilon \mid a, b \in k\}, \quad \varepsilon^2=0$$

- $F(k[\varepsilon])$ is a finite dimensional k -vector space.

Remark: fiber products don't always exist in $\hat{\mathcal{C}}_A$ $A = W(k)$

Example $A = k[[X, Y]], \quad C = k[[X]], \quad B = k$

maps

$$\begin{array}{ccc} A \rightarrow C & , & B \rightarrow C \\ Y \mapsto 0 & & \\ k \hookrightarrow k[[X]] & & \end{array}$$

Check: the fiber product $A \times_B C$ is not in the category $\hat{\mathcal{C}}_A$ (the fiber product as rings is not Noetherian ... this argument should not work)

Fiber products exist in $\hat{\mathcal{C}}_A$.

F has the Mayer-Vietoris property if the map $F(A \times_B C) \rightarrow F(A) \times_{F(B)} F(C)$ is a bijection.

Remark: F pro-representable $\Rightarrow F$ has the Mayer-Vietoris - property.

- $F(k[\varepsilon])$ is a k -vector space:

Why is it a k -vector space? It is when the map $F(k[\varepsilon] \times_k k[\varepsilon])) \xrightarrow{\sim} F(k[\varepsilon]) \times_{F(k)} F(k[\varepsilon])$ is a bijection. (induced by $k[\varepsilon] \xrightarrow{\sim} k \xleftarrow{\sim} k[\varepsilon]$)

k -scalar multiplication is induced by

$$\begin{aligned} k \times k[\varepsilon] &\longrightarrow k[\varepsilon] \\ (\lambda, a+b\varepsilon) &\mapsto (a+\lambda b)\varepsilon \end{aligned}$$

; addition is induced by

$$\begin{cases} k[\varepsilon] \times_k k[\varepsilon] \longrightarrow k[\varepsilon] \\ (a+b\varepsilon, c+d\varepsilon) \mapsto a+(b+c)\varepsilon \end{cases}$$

14

In this case we call $F(k[\epsilon])$ the tangent space of F . Why?

When F is pro-representable, $F \cong \text{Hom}_{\mathcal{C}_k}(R, \cdot)$ then there is an isomorphism of k -vector spaces

$$t_R \longrightarrow F(k[\epsilon])$$

Recall: for R a local Noetherian A -algebra with maximal ideal m_R , then

$t_R^* = \frac{m_R}{(m_R^2, m_R)}$ is the cotangent space of R , $t_R = \text{Hom}_R(t_R^*, k)$.

Idea of proof: $f \in F(k[\epsilon]) = \text{Hom}_{\mathcal{C}_k}(R, k[\epsilon])$

$$\text{then } f(r) = \bar{r} + f'(r) \in$$

for $r \in R \quad \begin{matrix} \text{image} \\ \text{mod } m_R \end{matrix}$

Criteria for representability:

Criterion. (Grothendieck) Let $F: \mathcal{C}_k \rightarrow \underline{\text{Set}}$ be a functor such that $F(k) = \{*\}$.

Then F is pro-representable if and only if the following hold:

- i) F has the Mayer-Vietoris property
- ii) $F(k[\epsilon])$ is a finite dimensional vector space $/k$.

We will use a refined version:

Criterion. (Schlessinger)

Def. If $R, S \in \mathcal{C}_k$, $f: R \rightarrow S$ a morphism. We say that f is small if it is surjective and if $\ker f$ is annihilated by m_R ($m_R \cdot \ker f = 0$) (Exp.: $k[\epsilon] \xrightarrow{\epsilon \mapsto 0} k$)

We introduce the Schlessinger conditions. $R_0, R_1, R_2 \in \mathcal{C}_k$, $\varphi_1: R_1 \rightarrow R_0$, $\varphi_2: R_2 \rightarrow R_0$, $R_3 := R_1 \times_{R_0} R_2 \dots$; $(*) : F(R_3) \rightarrow F(R_1) \times_{F(R_0)} F(R_2)$

The conditions are:

- H1: If $\varphi_2 : R_2 \rightarrow R_0$ is small, then $(*)$ is surjective
- H2: If $R_0 = k$, $R_2 = k[\epsilon]$ with $R_2 \xrightarrow{\epsilon \mapsto 0} R_0$, then $(*)$ is bijective
- H3: $F(k[\epsilon])$ is finite-dimensional over k .
- H4: If $R_1 = R_2$, $\varphi_1 = \varphi_2$ is small, then $(*)$ is bijective.

Theorem of Schlessinger: If $F(k) = \{*\}$ and it satisfies H1-H4, then F is pro-representable.

09.05.18

CONTINUITY OF FUNCTORS

$F : \hat{\mathcal{C}}_A \rightarrow \underline{\text{Set}}$ functor. We say that F is continuous if the natural map

$$F(A) \longrightarrow \varprojlim_n F(A/m_A^n) \quad \text{is a bijection } \forall A \in \hat{\mathcal{C}}_A$$

Exercise: * F representable $\Rightarrow F$ continuous

* $\hat{D}_{\bar{P}, A}$ is continuous

* If we extend $D_{\bar{P}, A}$ by continuity ($D_{\bar{P}, A}(A) := \varprojlim_n D_{\bar{P}, A}(A/m_A^n)$ for $A \in \hat{\mathcal{C}}_A$), we get $\hat{D}_{\bar{P}, A}$

* If $D_{\bar{P}, A}$ is pro-represented by some $R \in \hat{\mathcal{C}}_A$, then $\hat{D}_{\bar{P}, A} \cong \text{Hom}_{\hat{\mathcal{C}}_A}(R, \cdot)$

EXISTENCE OF UNIVERSAL DEFORMATION PAIRS

$G, R, A \in \hat{\mathcal{C}}_k$, fix $\bar{p} : G \rightarrow GL_n(k)$

We want to show $D_{\bar{P}, A}$ is pro-representable, by proving it satisfies H1-H4 of Schlessinger's criterion.

Theorem. Assume G satisfies the p -finiteness condition

(ϕ_p) $\text{Hom}_{\text{cont}}(H, \mathbb{Z}_{p\mathbb{Z}})$ is a finite set \forall open subgroups $H \leq G$

Then $D_{\bar{\rho}, 1} : \mathcal{E}_1 \rightarrow \underline{\text{Set}}$ satisfies H1, H2, H3. of Schlessinger's criterion.

Let $C_k(\bar{\rho}) = \text{Hom}_{\bar{\rho}}(k^n, k^n) \left(= \left\{ M \in M^{n \times n}(k) \text{ s.t. } \bar{\rho} \cdot M = M \cdot \bar{\rho} \right\} \right)$

If $C_k(\bar{\rho}) = k$ (matrices) then $D_{\bar{\rho}, 1}$ also satisfies H4.

(Mazur proved Theorem for $\bar{\rho}$ abs. irreducible, Ramakrishna proved for $C_k(\bar{\rho}) = k$)

Corollary. If G satisfies p -finiteness and $C_k(\bar{\rho}) = k$ then $D_{\bar{\rho}, 1}$ is pro-representable:

there exists a couple $(R^{\text{univ}}, \rho^{\text{univ}})$ with the following universal property:
 $\mathcal{E}_1 \xrightarrow{\quad} R^{\text{univ}} \quad | \quad$
 $\quad : G \rightarrow \text{GL}_n(R^{\text{univ}})$

$\forall A \in \mathcal{E}_1$ and every deformation $\rho : G \rightarrow \text{GL}_n(A)$ of $\bar{\rho}$, there exists an unique 1-algebra morphism $f_\rho : R^{\text{univ}} \rightarrow A$ s.t. $\rho \underset{\substack{\text{str.} \\ \text{equiv.}}}{\cong} f_\rho \circ \rho^{\text{univ}}$

Remarks: 1) When is $C_k(\bar{\rho}) = k$? Schur's Lemma \Rightarrow condition holds for $\bar{\rho}$ abs. irreducible $\Leftrightarrow \bar{\rho} : G \rightarrow \text{GL}_n(k)$

Take $\bar{\rho}(g) = \begin{pmatrix} \chi_1(g) & * \\ 0 & \chi_2(g) \end{pmatrix}$, χ_1, χ_2 distinct characters $G \rightarrow k^\times$, $* \neq 0$ $\boxed{\text{GL}_2(k)}$ irred.

Then $C_k(\bar{\rho}) = k$.

2) What to do when $C_k(\bar{\rho}) \neq k$?

* Look at "versal" deformations

* Look at "framed" deformations

Versal deformations:

Def. Let $F, G : \mathcal{C}_1 \rightarrow \underline{\text{Set}}$ be functors s.t. $F(k) = \{*\}, G(k) = \{*\}$.

A natural transformation $\eta : F \rightarrow G$ is formally smooth $\Leftrightarrow \forall A, B \in \mathcal{C}_1$

\forall surjections $A \rightarrow B$ the natural map $F(A) \rightarrow F(B) \times_{G(B)} G(A)$ is surjective.

Proposition.

If F, G are pro-representable,

$F = \text{Hom}(R_F, \cdot), G = \text{Hom}(R_G, \cdot)$ for some $R_F, R_G \in \hat{\mathcal{E}}_1$

then:

a transformation $F \rightarrow G$ is formally smooth

\Leftrightarrow it is induced by a morphism $R_G \rightarrow R_F$ that makes R_F a ring of formal power series over R_G .

$$(R_F = R[[T_1, \dots, T_n]])$$

$$\left(\begin{array}{ccc} F(A) & & n_A \\ \downarrow & & \downarrow \\ F(B) & \swarrow & \downarrow \\ & n_B & \\ & \downarrow & \\ & G(B) & \end{array} \right)$$

Proved in Mézard's notes, in Schlessinger's paper (Lemma 2.5) □

Def. We say that a functor $F : \mathcal{C}_1 \rightarrow \underline{\text{Set}}$ admits a versal deformation

if there exists a couple (R, p) such that the morphism of functors

$$\hat{\mathcal{E}}_1 \xrightarrow{F(R)}$$

$$\text{Hom}_{\hat{\mathcal{E}}_1}(R, A) \rightarrow F(A) \text{ defined for } A \in \hat{\mathcal{E}}_1 \quad (f : R \rightarrow A) \mapsto F(f)(p)$$

is formally smooth.

$$(R^{\text{ver}}, p^{\text{ver}})$$

Theorem. (Schlessinger) Assume G satisfies ϕ_p . Then $D_{\bar{p}, 1}$ admits a versal deformation
This means that for $\forall A \in \hat{\mathcal{E}}_1$ and \forall deformations p of \bar{p} to A there exists $f_p \in \text{Hom}_{\hat{\mathcal{E}}_1}(R^{\text{ver}}, A)$
st. $f_p \circ \tilde{p} \underset{\text{str.}}{\approx} p$, but f_p is not uniquely determined.

Framed deformations:

Define a framed deformation functor $\mathcal{D}_{\bar{P}, 1}^{\square} : \mathcal{C}_1 \rightarrow \underline{\text{Set}}$ as

$$\mathcal{D}_{\bar{P}, 1}^{\square}(A) = \left\{ \begin{array}{l} \text{set of deformations} \\ \text{of } \bar{P} \text{ to } p : G \rightarrow GL_n(A) \end{array} \right\}$$

Deformations as actions on A-modules

See $\bar{P} : G \rightarrow GL_n(k)$ as datum of:

- * a continuous action of G on a n -dimensional k -vector space $V_{\bar{P}}$
- * a choice of basis β for $V_{\bar{P}}$

We call a deformation of \bar{P} the datum of
(framed deformation)

(1) a continuous action of G on a free A -module V_A of rank n

such that $V_A \otimes_A k \underset{G\text{-modules}}{\cong} V_{\bar{P}}$

(2) a choice of a lift of the basis β of $V_{\bar{P}}$ to an A -basis of V_A

(same as choosing a lift of \bar{P} to $p : G \rightarrow GL_n(A)$)

$\mathcal{D}_{\bar{P}, 1}^{\square}(A) = \text{set of choices of (1)}$,

$\mathcal{D}_{\bar{P}, 1}^{\square}(A) = \text{set of choices of (1) and (2).}$

Theorem. Assume G has property ϕ_p . Then the framed deformation functor $\mathcal{D}_{\bar{P}, 1}^{\square}$ is pro-representable. (No need of Schlessinger)

Proposition. The transformation of functors $\mathcal{D}_{\bar{P}, 1}^{\square} \rightarrow \mathcal{D}_{\bar{P}, 1}$ defined by

$$(p : G \rightarrow GL_n(A)) \mapsto [p]_{\text{str. equivalence}}$$

is formally smooth.

19

Proof. exercise. $D_{\bar{P}, \Lambda}^{\square}(A) \rightarrow D_{\bar{P}, \Lambda}^{\square}(B) \times_{D_{\bar{P}, \Lambda}^{\square}(B)} D_{\bar{P}, \Lambda}^{\square}(A)$ (surjection $A \rightarrow B$) \blacksquare

Corollary. if $\mathcal{E}_k(\bar{P}) = k$ ($\rightarrow D_{\bar{P}, \Lambda}^{\square}$ and $D_{\bar{P}, \Lambda}$ are represented as $\text{Hom}_{\widehat{\mathcal{E}}_k}(\text{R}_{\text{univ}}, \cdot)$, $\text{Hom}_{\widehat{\mathcal{E}}_k}(\text{R}_{\text{univ}}, \cdot)$), then $\text{R}_{\text{univ}}^{\square} = \text{R}_{\text{univ}}[[T_1, \dots, T_n]]$.

Proof of pro-representability of $D_{\bar{P}, \Lambda}^{\square}$.

We look for an object $R \in \widehat{\mathcal{E}}_k$ such that $D_{\bar{P}, \Lambda}^{\square}(A) = \text{Hom}_{\widehat{\mathcal{E}}_k}(R, A) \quad \forall A \in \widehat{\mathcal{E}}_k$.

1) We prove the result for G finite. (fix $p: G \rightarrow GL_n(k)$)

Define Λ -algebra $\Lambda[G, n]$ by giving

* generators: $X_{ij}^g, g \in G, i, j \in \{1, \dots, n\}$

* relations: $X_{ij}^{gh} = \sum_{e=1}^n X_{ie}^g X_{ej}^h \quad \forall g, h \in G \quad \forall i, j \in \{1, \dots, n\} \quad (e \in G \text{ unity})$

$$X_{ij}^e = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{if } i \neq j \end{cases}$$

Then there is a bijection, for every Λ -algebra A

$$\begin{aligned} b_A: \text{Hom}_{\Lambda}(\Lambda[G, n], A) &\rightarrow \text{Hom}_{\text{Grp}}(G, GL_n(A)) \\ f &\mapsto (g \mapsto (f(X_{ij}^g))_{i,j}) \end{aligned}$$

Check: this is a bijection. ($\Lambda[-, n] \rightarrow GL_n$)

Consider $\bar{p} \in \text{Hom}_{\text{Grp}}(G, GL_n(k))$, then $b_k^{-1}(\bar{p}) =: f_{\bar{p}}$ is a Λ -algebra-morphism

$\Lambda[G, n] \rightarrow k$. Set $m_{\bar{p}} = \ker f_{\bar{p}}$.

Set $R := m_{\bar{p}}$ -adic completion of $\Lambda[G, n] = \varprojlim_n \frac{\Lambda[G, n]}{m_{\bar{p}}^n}$

Show that R has the universal property: take a deformation $p: G \rightarrow GL_n(A)$ of \bar{p} to some $A \in \widehat{\mathcal{E}}_k$. Then $f_p := b_A^{-1}(p): \Lambda[G, n] \rightarrow A$, then $f_p(m_{\bar{p}}) \subseteq m_A$.

In particular f_p can be extended by continuity to $f_p: R \rightarrow A$. Then one checks

$$\begin{array}{ccc} G & \xrightarrow{p^{\text{univ}}} & GL_n(R) \\ & \downarrow \pi & \downarrow f_p \\ & p & GL_n(A) \end{array} \quad \left| \begin{array}{l} \text{define } p^{\text{univ}} \text{ as the homomorphism} \\ G \rightarrow GL_n(R) \text{ attached to} \\ \Lambda[G,n] \rightarrow R \text{ by } b_R \end{array} \right.$$

Also, f_p with this property is unique.

$\Rightarrow (R, p^{\text{univ}})$ is an universal deformation couple for \bar{p}

2) G profinite, then $G = \varprojlim_{\substack{H \trianglelefteq G \\ G/H \text{ finite} \\ H \in \ker \bar{p}}} G/H$

(are exactly the H 's such that \bar{p} factors through $\bar{p}_H: G/H \rightarrow GL_n(k)$)

For each such H there is a representing pair $(R_{\bar{p}_H}, \bar{p}_H)$ for the functor $D_{\bar{p}_H, 1}^\square$. The set $\{R_{\bar{p}_H}\}_H$ is a projective system, and

$R_{\bar{p}} := \varprojlim_H R_{\bar{p}_H}$ is in the category $\hat{\mathcal{E}}_1$. (uses ϕ_p -assumption on G !)

Then $R_{\bar{p}}$ pro-represents $D_{\bar{p}, 1}^\square$:

$$\begin{aligned} D_{\bar{p}, 1}^\square(A) &= \varprojlim_H D_{\bar{p}_H, 1}^\square(A) = \varprojlim_H \text{Hom}(R_{\bar{p}_H}, A) \\ &\cong \text{Hom}(\varprojlim_H R_{\bar{p}_H}, A) \\ &= \text{Hom}(R_{\bar{p}}, A). \end{aligned}$$

Representability of $D_{\bar{p}}$ when $C_R(\bar{p}) = k$. Need to check H1-H4 in Schlessinger's criterion.

Objects $R_0, R_1, R_2 \in \hat{\mathcal{E}}_A$ with morphisms $R_1 \rightarrow R_0$; set $R_3 := R_1 \times_{R_0} R_2$
 $R_2 \rightarrow R_0$

$$b: D_{\bar{p}}(R_3) \longrightarrow D_{\bar{p}}(R_1) \times_{D_{\bar{p}}(R_0)} D_{\bar{p}}(R_2)$$

E_i : set of all deformations $p: G \rightarrow GL_n(R_i)$ of \bar{p} .

$$D_{\bar{p}}(R_i) = E_i / \begin{matrix} \text{strict equiv.} \\ \Gamma_n(R_i) \end{matrix} = E_i / \Gamma_n(R_i) \quad (\Gamma_n(R_i) := \ker(GL_n(R) \rightarrow GL_n(k)))$$

Then write

$$b: E_3 / \Gamma_n(R_3) \longrightarrow E_1 / \Gamma_n(R_1) \times_{E_0 / \Gamma_n(R_0)} E_2 / \Gamma_n(R_2)$$

H1: if $R_2 \xrightarrow[\text{small}]{} R_0 \Rightarrow b$ surjective

Proof. Take p_1, p_2 representatives of classes in $E_1 / \Gamma_n(R_1)$, $E_2 / \Gamma_n(R_2)$. Assume that the images of p_1 and p_2 via $\begin{matrix} R_1 \\ R_2 \end{matrix} \xrightarrow{\quad} R_0$ are in the same class.

$$\begin{matrix} p_{10}: G \rightarrow GL_n(R_0) \\ p_{20}: G \rightarrow GL_n(R_0) \end{matrix} \quad \text{Then } \exists M_0 \in \Gamma_n(R_0) \text{ s.t. } M_0^{-1} p_{20} M_0 = p_{10}.$$

Since $R_2 \rightarrow R_0$ is surjective, $\Gamma_n(R_2) \rightarrow \Gamma_n(R_0)$ is surjective. So we can choose a lift M_2 of M_0 in $\Gamma_n(R_2)$. Then the representations $M_2^{-1} p_2 M_2$ and p_1 give the same representations in $GL_n(R_0)$. They glue to a representation $p_3: G \rightarrow GL_n(R_3)$

$$(p_3(\cdot)) = (p_1(\cdot), M_2^{-1} p_2(\cdot) M_2) \in GL_n(R_1 \times_{R_0} R_2)$$

□

H2, H4: similar strategies (see Gaïevar)

H3: $D_{\bar{p}}(\frac{k[E_3]}{k[X]})$ is a finite-dimensional k -vector space.

Proof. $G_0 = \ker \bar{p}$ ($\rightsquigarrow (G:G_0) < \infty$); $R \in \hat{\mathcal{E}}_A$ and $p: G \rightarrow GL_n(R)$ a lift of \bar{p} .

Then $p|_{G_0}$ takes values in $\Gamma_n(k)$. This is a pro-p group.

Take $R = k[\varepsilon]$. Then $\Gamma_n(k[\varepsilon]) = 1 + \underbrace{\mathbb{Z}_{p^n}(k)}_{p\text{-elementary finite group}}$

A lift $p: G \rightarrow GL_n(k[\varepsilon]) \circ \bar{p}$ defines a homomorphism

$$G_0 \rightarrow \Gamma_n(k[\varepsilon]), \quad (p|_{G_0} = p'|_{G_0} \Leftrightarrow p \sim p' \text{ strictly equiv.})$$

but $\Gamma_n(k[\varepsilon])$ is a finite sum of \mathbb{Z}_{p^n} 's ($\Leftrightarrow p\text{-elementary finite}$)

By p -finiteness $\text{Hom}_{\text{cont}}(G_0, \Gamma_n(k[\varepsilon]))$ is finite.

By Schlessinger, \exists universal deformation couple $(R_{\bar{p}}^{\text{univ}}, p^{\text{univ}})$ for \bar{p} .

Proof of Schlessinger's criterion gives a surjection $\Lambda[[T_1, \dots, T_d]] \rightarrow R_{\bar{p}}^{\text{univ}}$

By looking at tangent spaces, one sets, for the minimal d : $d = \dim_k t_{R_{\bar{p}}^{\text{univ}}} \Rightarrow \dim_k D_{\bar{p}}(k[\varepsilon])$

* Can we give d in terms of \bar{p} ?

* $R_{\bar{p}}^{\text{univ}} = \Lambda[[T_1, \dots, T_d]] / I$, we will describe $\dim R_{\bar{p}}^{\text{univ}}$ in terms of \bar{p} .

Explicit case: $n=1$.

Fix $\bar{p}: G \rightarrow k^\times = GL_1(k)$. We describe the universal deformation couple for \bar{p} . There is a lift $p: G \rightarrow W(k)^\times$ given by $(W(\mathbb{F}_{p^n}) = \mathbb{Z}_{p^n})$ the Teichmüller lift $k^\times \rightarrow W(k)^\times$.

Take another lift $p: G \rightarrow A^\times$ for $A \in \mathcal{E}_\lambda$. (one has a map $W(k)^\times \rightarrow A^\times$)

Then $\bar{p}^{-1} \circ p: G \rightarrow A^\times$ takes values in $1 + m_A$.
 $\bar{p}^{-1}(g) = p(g)^{-1}$. $\hookrightarrow \circ \text{not} \circ$

$1 + m_A$ is a pro-p-group, so $\bar{p}^{-1} \circ p$ factors through the pro-p-completion Γ of G .

$(\Gamma := \varprojlim H$
 $H \text{ quotient of } G \text{ that is finite } p\text{-group})$

23

$$\rho_0 \circ p: G \rightarrow 1 + m_A$$

$\downarrow \gamma^n$

$\exists f_p$ continuous
group hom.

By continuity f_p can be extended to

$$f_p: \Lambda[\Gamma] \rightarrow A, \text{ 1-af. hom.}$$

$$\Lambda[\Gamma] = \varprojlim_{\substack{\Gamma' \text{ open normal} \\ \Gamma' \text{ subgrp. of } \Gamma}} \Lambda[\Gamma/\Gamma']$$

1 group-algebra

Remark. * $\Lambda[\Gamma] \in \Sigma_1$.

One checks that

G satisfies p -finiteness $\Rightarrow \Gamma$ is top. f.g. $\Rightarrow \Lambda[\Gamma]$ is a quotient of $\Lambda[x_1, \dots, x_n]$
by x_1, \dots, x_n

Proposition. The universal deformation couple for \bar{p} is
 $(\Lambda[\Gamma], p^{\text{univ}})$, where $p^{\text{univ}} = p_0 \circ [\gamma]$

Where $[\gamma]$ is the composition $G \rightarrow \Gamma \rightarrow \Lambda[\Gamma]^x$

Proof. We already defined a 1-algebra morphism $f_p: \Lambda[\Gamma] \rightarrow A$ (for any deformation $p: G \rightarrow A^x$)
We check: for $g \in G$

$$f_p \circ p^{\text{univ}}(g) = f_p(p_0(g)[\gamma(g)]) = p_0(g) f_p([\gamma(g)]) = \underbrace{p_0(g) \bar{p}_0(g)}_{=1} p_0(g) = p(g).$$

Check that f_p is unique.

□

Remark. * $R_{\bar{p}}^{\text{univ}}$ is independent of \bar{p} .

Take any $\bar{p}: G \rightarrow \text{GL}_n(k)$ (with $S_k(\bar{p}) = k$). Then there is a universal def. couple $(R_{\bar{p}}^{\text{univ}}, p^{\text{univ}})$. Look at $\det \circ p^{\text{univ}}: G \rightarrow R_{\bar{p}}^{\text{univ}, x}$. It is a deformation of $\det \circ \bar{p}$.

$\det \circ \bar{p}$ \Rightarrow There exists a 1-af. morphism $\Lambda[\Gamma] \rightarrow R_{\bar{p}}^{\text{univ}}$
inducing $\det \circ p^{\text{univ}}$

It is a special case of "functoriality".

* Take any algebraic morphism $\text{GL}_m \xrightarrow{\delta} \text{GL}_n$. (of algebraic groups)Take $\bar{p}_m: G \rightarrow \text{GL}_m(k)$, then we get $\bar{p}_n: G \rightarrow \text{GL}_n(k) := \delta_k \circ \bar{p}_m$.

Assume \bar{P}_m, \bar{P}_n are absolutely irreducible. Then $\frac{\delta}{R_{\bar{P}_n}} \circ P_n^{\text{univ}}$ is a deformation of \bar{P}_m . By the universal property we get $R_{\bar{P}_m}^{\text{univ}} \xrightarrow{r(\delta)} R_{\bar{P}_n}^{\text{univ}}$ s.t. $r(\delta) \circ P_m^{\text{univ}} = P_n^{\text{univ}}$

* $m = n$, $GL_n/\lambda \xrightarrow{\delta} GL_n/\lambda$ given by conjugation with fixed $g \in GL_n(\lambda)$.

Take $\bar{p}_m : G \rightarrow GL_m(k)$, then \exists a morphism $R_{\bar{p}_m \otimes \bar{p}_n} \rightarrow R_{\bar{p}_m} \hat{\otimes}_{\Lambda} R_{\bar{p}_n}$

Dimension of the deformation rings

$$\lambda \left[T_1, \dots, T_d \right] \equiv R_{\overline{P}}^{\text{univ}}$$

Reinhold : Group cohomology

* G pro-finite group, M topological abelian group with a continuous action of G .
 (G, \cdot) $(M, +)$

Can define a functor $M \mapsto \underline{M^G} = \{m \in M \mid gm = m \text{ } \forall g \in G\}$

$H^0(G, M) = M^G$, $H^i(G, M) \rightarrow$ Right-derived functor of $M \mapsto M^G$.

We will compute cohomology with the following complex.

$$M \rightarrow K^1 \xrightarrow{d^1} K^2 \xrightarrow{d^2} \dots \rightarrow K^i \xrightarrow{d^i} \dots$$

with $K^i := \{f: G^i \rightarrow M \text{ continuous functions}\}$ with $d^i f(g_1, \dots, g_{i-1})$

$$= g_1 f(g_{21} - \sum_{j=1}^{i-1} (-1)^j f(g_{11} - g_{ij} g_{j+11} + g_{i1}))$$

$$\text{Explicitly: } H^0(G, M) = M^G$$

$$z^1(G, M) = \{ f: G \rightarrow M \mid f(g_1g_2) = g_2 f(g_1) + f(g_2) \}$$

$$\mathcal{B}^1(G, M) = \{ f: G \rightarrow M \mid \exists m \in M \text{ s.t. } f(g) = (g^{-1})m \quad \forall g \in G \}$$

Cohomological interpretation of the tangent space.

Fix $\bar{p}: G \rightarrow GL_n(k)$ ($C_k(\bar{p}) = k$). We said that $d = \dim_k D_{\bar{p}}(k[\varepsilon])$
 $= \dim_k t_{R_{\bar{p}}^{univ}}$

$$(t_{R_{\bar{p}}^{univ}} = \text{Hom}_\Lambda(R_{\bar{p}}^{univ}, k[\varepsilon]))$$

Start with $p: G \rightarrow GL_n(k[\varepsilon])$ a deformation of \bar{p} . Then $\forall g \in G$:

$$p(g) = \bar{p}(g)(1 + c_g \varepsilon) \quad (\Lambda \hookrightarrow k[\varepsilon] = k + \varepsilon k)$$

check: p homomorphism

$$M_n(k)$$

$\Rightarrow c: G \rightarrow M_n(k), g \mapsto c_g$ is a 1-cocycle for the adjoint

action $G \curvearrowright M_n(k)$ of \bar{p} .

Adjoint representation: $G \curvearrowright M_n(k)$

$$g \cdot m := \bar{p}(g)^{-1} m \bar{p}(g). \text{ Write } \text{Ad}_{\bar{p}}$$

Proposition: The previous construction gives an isomorphism (of vector spaces)

$$D_{\bar{p}}(k[\varepsilon]) \xrightarrow{\sim} H^1(G, \text{Ad}_{\bar{p}})$$

Corollary. $d = \dim_k (H^1(G, \text{Ad}_{\bar{p}}))$.

23.05.18

Obstructions Take $R_0, R_1 \in \hat{\mathcal{E}}_\Lambda$ with a morphism of Λ -algebras $R_1 \xrightarrow{\varphi} R_0$ surjective
 $I := \ker \varphi$. and $\text{ker } \varphi \cdot M_{R_1} = 0$.

Fix $\bar{p}: G \rightarrow GL_n(k)$. Consider a deformation $p_0: G \rightarrow GL_n(R_0)$ of \bar{p} .

Can we lift p_0 to $p_1: G \rightarrow GL_n(R_1)$?

$$\begin{array}{ccc}
 GL_n(R_1) & \xrightarrow{\varphi} & GL_n(R_0) \\
 \downarrow p_1 & \nearrow p_0 & \\
 G & &
 \end{array}$$

Take σ any map (of sets) $G \xrightarrow{\sigma} GL_n(R_1)$ inducing
 p_0 . For $g_1, g_2 \in G$ set
 $c_\sigma(g_1, g_2) = \sigma(g_1 g_2) \sigma(g_2)^{-1} \sigma(g_1)^{-1}$.

We know σ lifts p_0 , so $c_\sigma(g_1g_2) \equiv 1 \pmod{I}$ \rightsquigarrow we can write

$$c_\sigma(g_1g_2) = 1 + d_\sigma(g_1, g_2)$$

\cap
 $M_n(I)$

Check: $G \times G \rightarrow I$ defines a cocycle in $H^2(G, \text{Ad}_{p_I})$
 $(g_1, g_2) \mapsto d_\sigma(g_1, g_2)$

$I \cdot m_{R_1} = 0 \Rightarrow I$ has a k -vector space structure ($\exists k \rightarrow I$)

p_I = composition of \bar{p} with $k \rightarrow I$

$\text{Ad}_{p_I} = G$ acting on $M_n(I)$ via conjugation with p_I .

If σ' is another set-theoretic lift $G \rightarrow GL_n(R_1)$ of p_0 , then $d_\sigma(g_1, g_2) d_{\sigma'}(g_1, g_2)$ is a coboundary.

\rightarrow The class $\mathcal{O}(p_0)$ of d_σ in $H^2(G, \text{Ad}_{p_I})$ only depends on p_0 .

If \exists a group homomorphism $\sigma: G \rightarrow GL_n(R_1)$ lifting p_0 , then $\mathcal{O}(p_0)$ is trivial.

If $\mathcal{O}(p_0)$ is trivial, then p_0 admits a lift $G \rightarrow GL_n(R_1)$ (group homomorph. !)

Conclusion: p_0 admits a lift to $R_1 \Leftrightarrow \mathcal{O}(p_0) = 0$.

Remark: if $H^2(G, \text{Ad}_{\bar{p}}) = 0$, then $H^2(G, \text{Ad}_{p_I}) = 0$
 SII

$$H^2(G, \text{Ad}_{\bar{p}}) \otimes_k I$$

\Rightarrow for any $R_1 \xrightarrow{\Psi} R_0$ and any p_0 there exists a lift of p_0 to R_1 .

When $H^2(G, \text{Ad}_{\bar{p}}) = 0$ we say that the deformation problem is unobstructed.

Interpretation of obstructions via group extensions

Same situation: $R_1 \xrightarrow{\varphi} R_0$, $I = \ker \varphi$, $I \cdot m_{R_1} = 0$.

$\text{Ad}_{\tilde{\rho}_I}$ is a G -module. In general: Take a G -module A . Then there is a group isomorphism $\Omega^1(G, A) \rightarrow H^2(G, A)$

* $\Theta_{\text{pext}}(G, A)$ is the set of A -extensions of G :

$1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$ exact sequence of groups up to isomorph.

$$E' \xrightarrow{h} E$$

E, E' are isomorphic if $\exists h: E \rightarrow E'$ isomorph-
making the diagrams commute.

* Baer sum: gives $\text{Opext}(G, A)$ an abelian group structure.

* $E \in \text{Opext}(G, A)$ maps to $\text{OEH}^2(G, A) \leftrightarrow E$ is a split extension.

Back to $R_1 \xrightarrow{\varphi} R_0$, $\underbrace{\ker \varphi}_{=: I} \cdot m_{R_1} = 0$. Then Ad_{P_I} is a G -module.

Choose $\rho_0 : G \rightarrow GL_n(R_0)$

$$\text{identifg } \text{Ad}_{P_+} \cong 1 + \text{Ad}_{P_+} \quad (1+a)(1+b) = 1+a+b+\frac{ab}{\infty \text{ since}} \quad (1)$$

$$1 \rightarrow \text{Ad}_{P_{\mathbb{F}}} \hookrightarrow \text{GL}_n(R_A) \rightarrow \text{GL}_n(R_0) \rightarrow 1$$

\uparrow \uparrow \uparrow_{P}

$$1 \rightarrow \text{Ad}_{P_\mathbb{C}} \rightarrow G \times_{GL_n(R_\mathbb{C})} GL_n(R_\Lambda) \rightarrow G \rightarrow 1 \quad (*)$$

This $\text{Ad}_{P_{\mathbb{I}}}$ -extension of G gives a class $\Theta(p_0) \in H^2(G, \text{Ad}_{P_{\mathbb{I}}})$

Remark: The extension $(*)$ splits $\Leftrightarrow \exists$ repres. $p_1: G \rightarrow \mathrm{GL}_n(R_\lambda)$ lifting p_0 .

Proof: if (*) splits and $s: G \rightarrow G \times_{GL_n(R_2)} GL_n(R_1)$ is a section, then define

$$\rho_1 := \pi_2 \circ s$$

↑ projection to $GL_n(\mathbb{R})$

if p_1 exists then $s(g) := (g, p_1(g))$ is a section for $(*)$

We get: p_1 exists $\Leftrightarrow \mathcal{O}(p_0) = 0$.

Exercise: find something similar for H^1 .

Theorem. (Mazur) $d_1 := \dim_k H^1(G, \text{Ad}_{\bar{\rho}})$, $d_2 := \dim_k H^2(G, \text{Ad}_{\bar{\rho}})$

Then:

$$\dim_{\text{Krull}} \left(\frac{R_{\bar{\rho}}^{\text{univ}}}{m_{\lambda} R_{\bar{\rho}}^{\text{univ}}} \right) \geq d_1 - d_2$$

In particular, in the unobstructed case ($d_2 = 0$), $R_{\bar{\rho}}^{\text{univ}} \cong \Lambda[[T_1, \dots, T_{d_1}]]$.

Proof.

$$R = R_{\bar{\rho}}^{\text{univ}}$$

$$\Lambda[[T_1, \dots, T_{d_1}]] \rightarrow R \rightarrow 0 \quad \text{modulo } m_{\lambda}$$

$$0 \rightarrow J \rightarrow \underbrace{-k[[T_1, \dots, T_{d_1}]]}_{\substack{\text{defined} \\ \text{as kernel}}} \rightarrow \frac{R}{m_{\lambda} R} \rightarrow 0$$

Goal: prove that J has at most d_2 generators. $m_F := \text{max. ideal of } F$, reduce the sequence mod $m_F J$.

$$0 \rightarrow J/m_F J \rightarrow F/m_F J \rightarrow \frac{R}{m_{\lambda} R} \rightarrow 0$$

\uparrow
still an isomorphism on tangent spaces.

Consider p' the image of the universal deformation p^{univ} modulo $m_{\lambda} R$.

$$G \rightarrow \text{GL}_n(R/m_{\lambda} R)$$

By the previous construction, one associates to p' a class

$$\mathcal{O}(p') \in H^2(G, \text{Ad}_{\bar{\rho}}) \otimes_k \frac{J}{m_F J}.$$

Show \exists injection $\text{Hom}_k(\frac{J}{m_F J}, k) \hookrightarrow H^2(G, \text{Ad}_{\bar{\rho}})$ (then we are done).

$$f \longmapsto (1 \otimes f)(\mathcal{O}(p'))$$

2.9 Prove that it is an injection: Assume $f \neq 0$, consider $\ker f \leq J/m_p J$. galrep

Reduce modulo $\ker f$:

$$0 \rightarrow \underbrace{(J/m_p J)}_{\ker f} \rightarrow \underbrace{(F/m_p F)}_{\ker f} \rightarrow R/m_n R \rightarrow 0$$

* $A \rightarrow R/m_n R$ is still an isomorphism of tangent spaces.

* the image of $\mathcal{O}(p')$ in $H^2(G, \text{Ad}\bar{\rho}) \otimes (J/m_p J)_{/\ker f}$ is trivial.

$\Rightarrow p'$ admits a lift to A

\Rightarrow the exact sequence splits by the univ. prop. of p' .

$$\Rightarrow \ker f = J/m_p J \quad \xrightarrow{\text{to } f \neq 0.}$$

□

In many cases we have " $=$ " $\Leftrightarrow \dim_{\text{Gal}}(R/m_n R) = d_1 - d_2$.

Dimension conjecture: " $=$ " always holds.

Mazur calls this "generalized Leopoldt's conjecture".

Statement we use today: take K a number field, S set of places,

$S \ni p$ -adic and infinite places, $G_{K,S}$.

$r_1 = \#$ real embeddings of K , $r_2 = \frac{1}{2} \#$ complex embeddings

Leopoldt's conjecture \Leftrightarrow the number of \mathbb{Z}_p extensions of K unramified is $\sim_{\text{Gal}} \mathbb{Z}_p$

$$r_2 + 1 = \#\text{Hom}_{\text{cont}}(G_{K,S}, \mathbb{Z}_p)$$

\Leftrightarrow outside S is $r_2 + 1$.

Example: K total real, K has a \mathbb{Z}_p -extension (p -adic cyclotomic ext.),

Leopoldt's \Rightarrow it's the only \mathbb{Z}_p -extension.

30

Show: Dimension conjecture \Rightarrow Leopoldt's conjecture



$$\dim(\mathbb{R}/m_n \mathbb{R}) = d_1 - d_2$$

For every place $v \in S$ of K , write $G_v \subseteq G_{K,S}$ for a decomp. group at v

Proposition. For $\bar{\rho}: G_{K,S} \rightarrow \mathrm{GL}_n(k)$, we have $d_1 - d_2 = 1 + dn^2 - \sum_{v \in S^\infty} \dim_k H^0(G_v, \mathrm{Ad}\bar{\rho})$
 with $d = [K:\mathbb{Q}]$ ↑ infinite places

"Proof": Tate's Global Euler char. formula:

take M a finite $G_{K,S}$ -Module, then: (assume $\#M$ is an S -unit)

$$\frac{\# H^0(G_{K,S}, M) - \# H^2(G_{K,S}, M)}{\# H^1(G_{K,S}, M)} = \frac{\prod_{v \in S^\infty} \# H^0(G_v, M)}{\# M^d}$$

Apply it to $M = \mathrm{Ad}\bar{\rho}$. (We assumed $C_k(\bar{\rho}) = K$)

$$d_0 = \dim_k H^0(G_{K,S}, \mathrm{Ad}\bar{\rho})$$

$$\rightsquigarrow d_0 + d_2 - d_1 = \sum_{v \in S^\infty} \dim_k H^0(G_v, \mathrm{Ad}\bar{\rho}) - n^2 d$$

Apply to special cases:

1) $n=1$, any $\bar{\rho}: G_{K,S} \rightarrow k^\times$

For every $v \in S^\infty$ $H^0(G_v, \mathrm{Ad}\bar{\rho}) = 1$.

$$d_1 - d_2 = 1 + d - \underbrace{\#S^\infty}_{= r_1 + r_2} \quad d = r_1 + 2r_2$$

$$= 1 + r_2$$

What is $d_1 - d_2 \geq ?$ By the dimension conjecture $d_1 - d_2 = \dim \mathbb{R}_{\bar{\rho}}^{univ}/m_n \mathbb{R}_{\bar{\rho}}^{univ}$

$$\text{use } \mathbb{R}_{\bar{\rho}}^{univ} = \Lambda \mathbb{E} \hat{G}_{K,S}^{(p)} \mathbb{I} = \#\mathrm{Hom}_{\mathrm{cont}}(G_{K,S}, \mathbb{Z}_p)$$