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

## 01. Galois groups

$K$ perfect field, $L$ a normal extension of $K$. Define $\mathrm{Gal}(L/K)$

$= \{ \sigma : L \to L \mid \sigma \text{ field automorphism}, \ \sigma|_K = \mathrm{id}_K \}$

· Topology:
* if $L|K$ is finite then give $\mathrm{Gal}(L|K)$ the discrete topology
* if $L|K$ is infinite then give $\mathrm{Gal}(L|K)$ the Krull topology:

a basis of open neighborhoods of $\mathrm{id}_L$ is the collection of sets

$$\{ \sigma \in \mathrm{Gal}(L/K) \mid \sigma|_E = \mathrm{id}_E \} \text{ where } E \text{ varies over the finite}$$

subextensions $E|K$

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

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

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

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

$\Rightarrow$ Open subgroups are the closed subgroups of finite index

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

$$\left\{ \begin{matrix} \text{subextensions} \\ L \mid E \mid K \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{closed subgroups} \\ \text{of } \mathrm{Gal}(L \mid K) \end{matrix} \right\}$$

$$E \longmapsto \mathrm{Gal}(L \mid E) \qquad \text{is a bijection.}$$

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

This induces a bijection

$$\left\{ \begin{matrix} L \mid E \mid K, \\ E \mid K \text{ finite} \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{open subgroups} \\ \text{of } \mathrm{Gal}(L \mid K) \end{matrix} \right\}$$

When $L = K^{alg}$, we call $\mathrm{Gal}(K^{alg} \mid K)$ 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

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

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

"Frobenius element"

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

(the maps are $\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p) \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^m} / \mathbb{F}_p)$ $\quad m, n$ with $m \mid n$

$$\sigma \longmapsto \sigma|_{\mathbb{F}_{p^m}}$$

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$x \longmapsto x \bmod m$$

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

* $K = \mathbb{Q}_p$; we denote by $\mathbb{Q}_p^{ur}$ the maximal unramified extension of $\mathbb{Q}_p$.
($\longleftrightarrow$ 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 $\mathbb{Z}_p^{ur} / p\mathbb{Z}_p^{ur} \cong \mathbb{F}_p^{alg}$

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

$$\sigma \longmapsto \sigma \text{ modulo } p$$

This map is a group isomorphism.

$$\begin{array}{l} \mathbb{Q}_p^{alg} \\ \big| \Big) \text{ "Inertia group" } (I_p) \\ \mathbb{Q}_p^{ur} \\ \big| \Big) \mathrm{Gal} = \hat{\mathbb{Z}} \quad \text{(topologically generated by } \mathrm{Frob}_p) \\ \mathbb{Q}_p \end{array}$$

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

($\leftrightarrow$ choose an embedding $\mathbb{Q}^{alg} \to \mathbb{Q}_p^{alg}$)

Write a map

$$\mathrm{Gal}(\mathbb{Q}_p^{alg}/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q})$$
$$\sigma \longmapsto \sigma|_{\mathbb{Q}^{alg}}$$

This map is an injective group homomorphism and it identifies $\mathrm{Gal}(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$ with a subgroup $D_p \leq \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q})$

$$D_p = \{\sigma \in \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q}) \mid v(\sigma^{-1}(x)) = v(x) \quad \forall x \in \mathbb{Q}^{alg}\}$$

We have Injections

$$I_p \leq D_p \leq \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q})$$

# 02. 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) $G_{K,S} := \mathrm{Gal}(K^S/K)$

Remark. $v \in S$, then we have $\mathrm{Gal}(K_v^{alg}/K_v) \hookrightarrow \mathrm{Gal}(K^{alg}/K) \to \mathrm{Gal}(K^S/K)$

Injection ?

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

Exercise. An open subgroup $H \leq G_{K,S}$ 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. $\mathrm{Hom}_{cont}(G_{K,S}, \mathbb{F}_p)$ is finite. (Morphisms of topological groups)

Corollary. For every open subgroup $H \leq G_{K,S}$, $\mathrm{Hom}_{cont}(H, \mathbb{F}_p)$ is finite.
$\overset{\text{Def.}}{\Longleftrightarrow}$ $G_{K,S}$ 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 $\rho : G \longrightarrow GL_n(A)$ for some integer $n$.

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

---

Another point of view: let $M$ be a finite free $A$-module of rank $n$. Then a continuous representation $\rho : G \longrightarrow GL_n(A)$ gives a continuous action $G \curvearrowright M$

$$G \times M \longrightarrow M$$
$$(g, m) \longmapsto \rho(g)\,(m_i)_{i=1..n}$$

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

Def.

We call $\rho$ a Galois representation if $G$ is:

* $Gal(K^{alg}/K)$ for a finite extension $K \mid \mathbb{Q}_p$
* $G_{K,S}$ for a number field $K$ and a finite set of places $K$.

From now on $G$ is one of those groups.

Choices of coefficient ring $A$:

1) $A = \mathbb{C}$
2) $A = \mathbb{F}_{p^n}$
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 $\rho : G \longrightarrow GL_n(\mathbb{C})$ has finite image.

Proof. Consider an open neighborhood $\overset{\mathcal{U}}{\vee}$ of $\mathbb{1}_n \in GL_n(\mathbb{C})$. If $\mathcal{U}$ is sufficiently small, the only subgroup $\subseteq \mathcal{U}$ is $\{\mathbb{1}_n\}$ (Exercise). By continuity of $\rho$, $\exists\, V$ open neighborhood of $e \in G$ such that $\rho(V) \subseteq \mathcal{U}$. We can choose $V'$ a neighborhood of $e$ which is an open subgroup of $G$ and s.t. $V' \subseteq V$. Then $\rho(V') \subseteq \rho(V) \subseteq \mathcal{U}$.

$\Rightarrow \rho(V') = \{\mathbb{1}_n\}$. 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 $Gal(K/\mathbb{Q}) \hookrightarrow GL_n(\mathbb{C})$.

# 06

Mittwoch, 18. April 2018 15:39

② Proposition. If $\rho : G \to GL_n(\mathbb{F}_p^{alg})$ is a continuous representation,
$GL_n(\mathbb{Q}_p)$

then it factors through $\rho' : G \to GL_n(\mathbb{F}_{p^m})$ for some finite extension
$\to GL_n(E)$

$\mathbb{F}_{p^m} / \mathbb{F}_p$

$E / \mathbb{Q}_p$

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