01

Mittwoch, 18. April 2018 14:17

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 id_L is the collection of sets $\{\sigma \in \mathrm{Gal}(L/K) \mid \sigma|_E = \mathrm{id}_E\}$ where E 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.

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

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

Mittwoch, 18. April 2018 14:35

Theorem. (Galois correspondence) The map

$$\{\text{subextensions } L \mid E \mid K\} \longrightarrow \{\text{closed subgroups of } \mathrm{Gal}(L \mid K)\}$$

$$E \longmapsto \mathrm{Gal}(L \mid E)$$

is a bijection.

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

This induces a bijection

$$\{L \mid E \mid K,\ E \mid K \text{ finite}\} \longrightarrow \{\text{open subgroups of } \mathrm{Gal}(L \mid K)\}$$

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

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

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

"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 $\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_{p^m} / \mathbb{F}_p)$ 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 $\mathbb{Q}_p$.
(⟷ 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 $\mathrm{Gal}(\mathbb{Q}_p^{ur} / \mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_p^{alg} / \mathbb{F}_p)$

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

This map is a group isomorphism.

$\mathbb{Q}_p^{alg}$

|) "Inertia group" (I_p)

$\mathbb{Q}_p^{ur}$

|) $Gal = \hat{\mathbb{Z}}$ (topologically generated by $Frob_p$)

$\mathbb{Q}_p$

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

Wrik a map $Gal(\mathbb{Q}_p^{alg}/\mathbb{Q}_p) \to Gal(\mathbb{Q}^{alg}/\mathbb{Q})$

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

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

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

We have injections $I_p \leq D_p \subseteq Gal(\mathbb{Q}^{alg}/\mathbb{Q})$

Mittwoch, 18. April 2018 15:03

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. $v \notin S$, 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 $G \curvearrowright M$

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

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

Def.
We call ρ 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 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 $Gal(K \mid \mathbb{Q}) \hookrightarrow GL_n(\mathbb{C})$.

② Proposition. If $\rho: G \to GL_n(\overline{\mathbb{F}_p})$ 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 $\mathbb{Q}_p$. ∎

Proof of the last Proposition.

Look at $\rho(G) \leq GL_n(\overline{\mathbb{Q}}_p)$. 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)

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

($\forall n \in \mathbb{N}$: there are only finitely many $E/\mathbb{Q}_p$ s.t. $[E:\mathbb{Q}_p] = n$)

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/E finite such that $\rho(G) \leq GL_n(F)$ (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 $\rho: G \longrightarrow GL_n(K)$ is a continuous representation with coefficients in $K/\mathbb{Q}_p$ finite, then there exists a continuous representation $\rho': G \longrightarrow GL_n(\mathcal{O}_K)$ such that if $\iota: GL_n(\mathcal{O}_K) \longrightarrow GL_n(K)$ is the inclusion $\rho \overset{\text{equivalent}}{=} \iota \circ \rho'$

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 $\mathrm{Stab}(L) = \{g \in GL_n(K) \mid g(L) \subseteq L\}$ is an open subgroup of $GL_n(K)$. Ex

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

Choose a set $\{g_1, \dots, g_m\}$ of representatives for $G/\rho^{-1}(\mathrm{Stab}(L))$.

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

(G-stable: $\rho(g)\,L' \subseteq L' \quad \forall g \in G$)

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

By construction $\iota \circ \rho' \sim \rho$

Start with $\rho : G \to GL_n(K)$ continuous representation.

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

Then we can reduce modulo the maximal ideal $\mathfrak{m}_K \lhd \mathcal{O}_K$ and we obtain a "residual" representation $\bar{\rho} : G \to GL_n(\underbrace{\mathcal{O}_K/\mathfrak{m}_K}_{= \mathbb{F}_p^m})$ 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 (A: field) such that M_i/M_{i-1} is an irreducible $A[G]$-module.

(Does not admit any G-stable submodule)

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

Example: If $\rho(g) = \begin{pmatrix} \chi_1(g) & \delta(g) \\ 0 & \chi_2(g) \end{pmatrix} \to \bar{\rho}^{ss}(g) = \begin{pmatrix} \chi_1(g) & 0 \\ 0 & \chi_2(g) \end{pmatrix}$ $\quad g \in G$

χ_1, χ_2: Character of ρ

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

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

Idea: fix $\bar{\rho}: G \longrightarrow GL_n(\mathbb{F}_{p^m})$ and look at $\rho: G \longrightarrow GL_n(\mathcal{O}_K)$ (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, $n \in \mathbb{N}_{\geq 1}$)

$$\chi_n: G_{\mathbb{Q}} \longrightarrow Gal\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \left(= GL_1\left(\mathbb{Z}/p^n\mathbb{Z}\right)\right)$$

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

$$\chi_m \text{ modulo } p^n = \chi_n.$$

We can take $\underbrace{\varprojlim_n \chi_n}_{=: \chi_{cyc}}: G_{\mathbb{Q}} \longrightarrow \varprojlim_n Gal\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) = \varprojlim_n \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times = \mathbb{Z}_p^\times$

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

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

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

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

* $\mathcal{C}$ category, $R \in \mathcal{C}$, then $Hom_{\mathcal{C}}(R, \cdot): \mathcal{C} \longrightarrow \underline{Set}$ is the functor

$A \longmapsto Hom_{\mathcal{C}}(R,A)$, $f \in Mor_{\mathcal{C}}(A,B) \longmapsto \begin{cases} Hom_{\mathcal{C}}(R,A) \longrightarrow Hom_{\mathcal{C}}(R,B) \\ g \longmapsto f \circ g \end{cases}$

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.

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

$\wr$

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

* $\exists$ 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 $\mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n} = \mathbb{F}_{p^n}$

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

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

x modulo p^m $\longmapsto$ $\mathrm{Frob}_p(x)$ modulo p^m

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

$\wr$

$\mathbb{F}_{p^n}[\![T]\!]$

DEFORMATION FUNCTORS

Fix $n \geq 1$.

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

$\bar{\rho}: G \longrightarrow GL_n(k)$.

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

$\rho: G \longrightarrow GL_n(A)$ such that ρ modulo $m_A = \bar{\rho}$.

We say that $\rho_1, \rho_2 : G \longrightarrow GL_n(A)$ are strictly equivalent iff. $\exists M \in \ker(GL_n(A) \to GL_n(k))$ such that $M^{-1}\rho_1 M = \rho_2$.

Remark: if $A \xrightarrow{f} B$ is a morphism in $\hat{\mathcal{C}}_k$ and $\rho_1, \rho_2 : G \to GL_n(A)$ are strictly equivalent representations, then $f\rho_1, f\rho_2 : G \to GL_n(B)$ are strictly equivalent.

We define $D_{\bar{\rho}} : \hat{\mathcal{C}}_k \longrightarrow \underline{Set}$ as the functor

* $D_{\bar{\rho}}(A) := \left\{ \begin{array}{c} \text{deformations of} \\ \bar{\rho} \text{ to } A \end{array} \right\} /$ strict equivalence

* $D_{\bar{\rho}}(f)$ maps a deformation $\rho : G \to GL_n(A)$ to the class of $f \circ \rho$ ($f : A \to B$ morphism in $\hat{\mathcal{C}}_k$)

(We obtain a functor $\mathcal{C}_k \longrightarrow \underline{Set}$ by restricting $D_{\bar{\rho}}$ to $\mathcal{C}_k$)

Goal: show that D_ρ is "pro-represented" by some $R \in \hat{\mathcal{C}}_k$, in the sense that $D_{\bar{\rho}} \cong \mathrm{Hom}_{\hat{\mathcal{C}}_k}(R, \cdot)$