Galois representations

$G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

$G_{\mathbb{Q}} \longrightarrow GL(V)$ $\quad V/K \quad K$: field

Recall: L/K ext'n of fields

L/K is Galois if algebraic and the subfield of L fixed by all automorphism of

$(\forall \alpha \in L,\ K(\alpha)/K$ finite$)$

$$\mathrm{Aut}(L/K) = \{\text{field automorphisms } \sigma \text{ of } L \mid \sigma|_K = \mathrm{id}_K\}$$

is exactly K.

If L/K is Galois, $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$.

If L/K is Galois

$H \le Gal(L/K)$

denote $L^H = \{ \alpha \in L : \sigma(\alpha) = \alpha \ \ \forall \sigma \in H \}$ subfield of L.

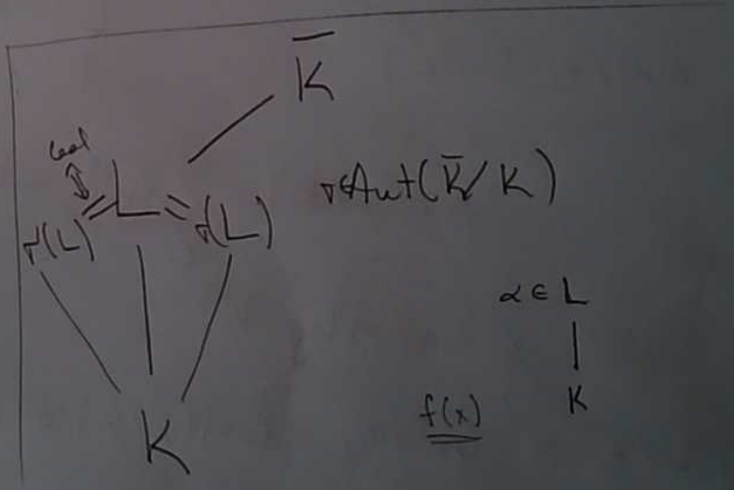
$L^{Gal(L/K)} = K$.

If L/K is finite, $\# Aut(L/K) \le [L:K]$

with equality iff L/K is Galois.

$\overline{\mathbb{Q}}/\mathbb{Q}$, $\overline{\mathbb{F}_p}/\mathbb{F}_p$

$G_{\mathbb{Q}}$ $G_{\mathbb{F}_p}$



Thm (Fundamental Thm of finite Gal. Thy).

Let L/K be finite Galois, with $G = \mathrm{Gal}(L/K)$.

We have an inclusion-reversing bijection

$$\left\{ \begin{array}{c} \text{subgroups} \\ H \leq G \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subextensions} \\ L/M/K \end{array} \right\}$$

$$H \longmapsto L^H$$

$$\mathrm{Gal}(L/M) \longleftarrow\!\shortmid\; M$$

which restricts to

$$\left\{ \begin{array}{c} \text{normal subgps} \\ H \leq G \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Galois subextns} \\ L/M/K \end{array} \right\}$$

$\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K)$

$H' \subseteq H$

$\Updownarrow$

$L^{H'} \supseteq L^H$

$$\begin{tikzcd} L \arrow[d, dash, "\mathrm{Gal}"'] \arrow[dr, dash, "\mathrm{Gal}"] & \\ K \arrow[r, dash] & M \end{tikzcd}$$

$$\begin{tikzcd} L = K(\alpha) \arrow[d, dash, "n"', "\text{sep.}"] \\ K \end{tikzcd}$$

$f(x)$: minl poly of α

deg n

$\alpha \longmapsto \beta$ β: root of f.

Fact:

$$\begin{tikzcd} L \arrow[r, dashed] & \overline{K} \\ K \arrow[u, hook, "\text{alg}"] \arrow[ur] & \end{tikzcd}$$

To define topology of $G_{\mathbb{Q}}$, need inverse limit.

<u>Defn</u>

(1) Let I be a partially ordered set ($\leq$). An inverse system indexed by I is a collection THINGS $\{A_i\}_{i\in I}$ together with THING-maps

$$\varphi_{ij} : A_i \longrightarrow A_j \qquad (j \leq i)$$

such that $\varphi_{ii} = \mathrm{id}_{A_i} \quad \forall i \in I$

$$\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik} \quad \forall\, k \leq j \leq i$$

(transition maps).

$I = \mathbb{N}$

$$\begin{tikzcd} A_4 \arrow[r] & A_3 \arrow[r] \arrow[rr, bend right] & A_2 \arrow[r] & A_1 \end{tikzcd}$$

(2) The inverse limit of $(\{A_i\}_{i\in I}, \{\varphi_{ij}\}_{j\leq i})$ is the THING

THINGS $\in$ {sets, grps, rings, topological spaces}

$$\varprojlim_i A_i = \left\{ (a_i)_{i\in I} \in \prod_{i\in I} A_i \;:\; \varphi_{ij}(a_i) = a_j \quad \forall j \leq i \right\}$$

(with the subspace topology when THING = top. sp.).

Examples

(1) $I = \mathbb{N}$

$A_i = \mathbb{Z}/p^i\mathbb{Z}$ w/ discrete top.

$A_i = \mathbb{Z}/p^i\mathbb{Z} \xrightarrow{\text{mod } p^j} \mathbb{Z}/p^j\mathbb{Z} = A_j$ $\qquad j \le i$

$$\cdots \longrightarrow \mathbb{Z}/p^3 \longrightarrow \mathbb{Z}/p^2 \longrightarrow \mathbb{Z}/p$$

$$\varprojlim_i \mathbb{Z}/p^i\mathbb{Z} = \left\{ (a_i) \in \prod_{i \ge 1} \mathbb{Z}/p^i\mathbb{Z} \;:\; a_i \text{ mod } p^j = a_j \quad \forall j \le i \right\}$$

$\|?$

$\mathbb{Z}_p$

as rings <u>and</u> topo. spaces. $\mathbb{Z}_p \supseteq U_n = \{x \in \mathbb{Z}_p : v_p(x) \ge n\}$ $\quad \left\| \frac{1}{6} \right\| = 3$

$\|6\|_3 = \frac{1}{3}$

$d(a,b) = |a - b|$

$\mathbb{Q} \xrightarrow[\text{complete w.r.t.}]{\|\cdot\|_p} \mathbb{Q}_p$

$\cup\!|$

$\mathbb{Z}_p$

$\left\| \frac{a}{b} \right\|_p = p^{-v_p(a/b)}$ $\qquad p$ prime

$\|3\|_3 = \frac{1}{3}$ $\qquad \|9\|_3 = \frac{1}{9}$

(2) R ring, $I = \mathbb{N}$

$A_i = R[x]/(x^i)$ discrete top.

$$\cdots \longrightarrow R[x]/(x^3) \xrightarrow{\text{mod } x^2} R[x]/(x^2) \xrightarrow{\text{mod } x} R[x]/(x)$$

$$\varprojlim_i R[x]/(x^i) = \left\{ (f_i) \in \prod_i R[x]/(x^i) \;;\; f_i \text{ mod } x^j = f_j \;\; \forall j \le i \right\}.$$

$\|?$

$R[[x]]$

(3) Let L/K be Galois.

$$I = \{ L/M/K \ : \ M/K \text{ finite Gal.} \}$$

$A_M = \underline{\mathrm{Gal}(M/K)}$ disc. top.

$N \subseteq M$

$$\begin{array}{ccc} A_M & \longrightarrow & A_N \\ \parallel & & \parallel \\ \mathrm{Gal}(M/K) & \xrightarrow{\mathrm{res}_N} & \mathrm{Gal}(N/K) \\ \sigma & \longmapsto & \sigma|_N \end{array}$$

$$\varprojlim_{\substack{L/M/K \\ M \text{ fn Gal}}} \mathrm{Gal}(M/K) = \left\{ (\sigma_M) \in \prod_M \mathrm{Gal}(M/K) \ : \ \sigma_M|_N = \sigma_N \quad \forall N \subseteq M \right\}$$

$$L = \bigcup_{\substack{L/M/K \\ \text{fn. Gal}}} M \qquad \cong \mathrm{Gal}(L/K) \qquad !!!$$

$$\parallel$$

$$\mathrm{Aut}(L/K) = \left\{ \sigma \text{ field automorphisms of } L : \ \sigma|_K = \mathrm{id}_K \right\}$$

Thm Let L/K be Galois with gp $\mathrm{Gal}(L/K)$.

Then the map

$$\begin{aligned} \mathrm{Gal}(L/K) &\xrightarrow{\Theta} \varprojlim_M \mathrm{Gal}(M/K) \\ \sigma &\longmapsto (\sigma|_M)_M \end{aligned}$$

is an isomorphism

Pf. Θ has image in $\varprojlim \mathrm{Gal}(M/K)$: ✓

Injectivity: $1 \neq \sigma \in \mathrm{Gal}(L/K) \Longrightarrow \sigma(x) \neq x$ for some $x \in L$

Taking M/K containing x, we have $\sigma|_M \neq 1$

$\Longrightarrow \Theta(\sigma) \neq 1$.

Surj: Let $(\sigma_M) \in \varprojlim \mathrm{Gal}(M/K)$. Define $\sigma \in \mathrm{Gal}(L/K)$ by

$\sigma(x) = \sigma_M(x)$ for some M/K containing x.

$\sigma_M(x) = \sigma_{M \cap M'}(x) = \sigma_{M'}(x)$ for any choices of M, M'

Check: σ is an aut. of L

$\Theta(\sigma) = (\sigma_M)$. ∎

Rmk. This puts a topology on $\mathrm{Gal}(L/K)$.

$H \leq \mathrm{Gal}(L/K)$ closed subgp / open

$H \leq \mathrm{Gal}(L/K)$ open $\Longrightarrow$ also closed.

Thm (Fund. Thm of ~~?~~ Galois thy). Let L/K be Galois, $G = \mathrm{Gal}(L/K)$

There is an inclusion-reversing bijection

$$\left\{\begin{matrix}\text{closed subgps}\\ H \leq G\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subextns}\\ L/M/K\end{matrix}\right\}$$

$$H \longmapsto L^H$$

$$\mathrm{Gal}(L/M) \longmapsfrom M$$

which restricts to bijections

$$\left\{\begin{matrix}\text{normal closed}\\ H \leq G\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{Gal. subextns}\\ L/M/K\end{matrix}\right\}$$

$$\left\{\begin{matrix}\text{open subgps}\\ H \leq G\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{finite subextns}\\ L/M/K\end{matrix}\right\}$$