MATH 5020

Galois Representations $G_{\mathbb{Q}}$

SPRING 2022

MARCH 29
2022

Ω/F Galois, algebraic extension

$\mathrm{Gal}(\Omega/F) = \mathrm{Aut}(\Omega/F)$ with Krull topology.

Thm (FTIGT)

Let Ω/F be Galois, algebraic ext'n, w/ $G = \mathrm{Gal}(\Omega/F)$.

$$\left\{\begin{array}{c}\text{closed subgps}\\ H \text{ of } G\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{intermediate fields}\\ F \subseteq M \subseteq \Omega\end{array}\right\}$$

$$H \longmapsto \Omega^H$$

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

ex. Subfields of $\mathbb{Q}(\zeta_{p^\infty})$.

ex Let $\overline{\mathbb{F}_p} / \mathbb{F}_p$ where $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

Then $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z}$

$$\cong \hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$$

Fix q prime, $H = \prod_{p \neq q} \mathbb{Z}_p \Rightarrow \hat{\mathbb{Z}}/H \cong \prod \mathbb{Z}_p \Big/ \prod_{p \neq q} \mathbb{Z}_p \cong \mathbb{Z}_q$

What is $\overline{\mathbb{F}_p}^H$?

$$\mathbb{F}_p \overset{q}{—} \mathbb{F}_{p^q} \overset{q}{—} \mathbb{F}_{p^{q^2}} — \cdots \quad \mathbb{F}_{p^{q^\infty}} \subseteq \overline{\mathbb{F}_p}$$

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{q}} \subseteq \mathbb{F}_{p^{q^2}} \subseteq \cdots$$

ex

$$L = \mathbb{Q}(\{\sqrt{d} : d \in \mathbb{Z}\}) = \mathbb{Q}(\{i, \sqrt{2}, \sqrt{3}, \dots, \sqrt{p}, \dots\})$$

$$= \mathbb{Q}(\{\sqrt{p_n}\}_{n \geq 0} : \ p_n \text{ nth prime}_{n \geq 1}, \ p_0 = -1)$$

Then $\mathrm{Gal}(L/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\{\sqrt{p_n} : 0 \leq n \leq m\}) \cong \varprojlim (\mathbb{Z}/2\mathbb{Z})^{m+1}$

$$\cong \prod_{n \geq 0} (\mathbb{Z}/2\mathbb{Z})$$

Krull top. = prod. topology.

s.t. $\prod_{n \geq 0} (\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\pi_k} \mathbb{Z}/2\mathbb{Z}$ continuous.

Closed subgps of finite index $\to$ open

$$\pi_m : \prod_{n \geq 0} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

$H_1 = \pi_m^{-1}(\{id\})$ of index 2 $\to$ fixed field $\mathbb{Q}(\sqrt{p_m})$

$H_2 = \pi_t^{-1}(\{id\}) \cap \pi_s^{-1}(\{id\})$ $\to$ fixed field $\mathbb{Q}(\sqrt{p_t}, \sqrt{p_s})$

$$\pi_{s,t} : \prod (\mathbb{Z}/2\mathbb{Z}) \longrightarrow \underbrace{\mathbb{Z}/2\mathbb{Z}}_{s} \times \underbrace{\mathbb{Z}/2\mathbb{Z}}_{t}$$

$H_3 = \pi_{s,t}^{-1}(\{(0,0),(1,1)\})$ $\to$ fixed field $\mathbb{Q}(\sqrt{p_s p_t})$

$$\prod (\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\pi} \underbrace{\prod_{k=1}^{n} \underbrace{(\mathbb{Z}/2\mathbb{Z})}_{i_k}}_{\tilde{H}}$$

$\pi^{-1}(\tilde{H}) = H$ closed subgp of finite index

Closed subgps of infinite index:

$$\begin{tikzcd} & L = \mathbb{Q}(\{\sqrt{d}\}) \arrow[dl, dash, "H"'] \arrow[ddr, dash] & \\ K \arrow[drr, dash, "\text{inf.}"'] & & \\ & & \mathbb{Q} \end{tikzcd}$$

$K/\mathbb{Q}$ infinite

$\alpha_k \in \mathbb{Z}$

$$K = \mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_k}, \dots)$$

s.t. $\langle \alpha_1, \dots, \alpha_k, \dots \rangle \mathbb{Q}^{\times 2} / \mathbb{Q}^{\times 2}$ is an ∞ subgp of $\mathbb{Q}^{\times} / \mathbb{Q}^{\times 2}$

K corresponds to $\underbrace{\bigcap_{k \geq 1} H_k}_{\text{closed.}}$ s.t. H_k fixes $\mathbb{Q}(\sqrt{\alpha_k})$

Any subgp. $\overset{H}{\vee}$ of index 2 in $\prod \mathbb{Z}/2\mathbb{Z}$ is the kernel of a hom:

$\phi : \prod \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, $H = \operatorname{Ker}\phi$.

$V = \prod_{n \geq 0} \mathbb{Z}/2\mathbb{Z}$ is an ∞-dim'l vectorspace

How to pick a basis of V??

- Start w/ $\{e_0, e_1, e_2, \dots\}$ $\quad e_i = (0, \dots, 0, \overset{i\text{th}}{1}, 0, \dots, \dots)$

$(1,1,1,\dots,1,\dots) \notin \langle e_1, \dots, e_i, \dots \rangle$

- ZORN'S LEMMA $\Rightarrow$ there is a basis of V, $B = \{v_i\}_{i \in I}$

Define $\overset{\text{hom}}{\vee}$ ϕ by $\phi(v_i) = a_i \in \{0, 1 \bmod 2\}$, at least one $\phi(v_i) \neq 0$.

Let $H = \operatorname{Ker}\phi \Rightarrow [G : H] = 2$.

What ϕ gives me H s.t. $L^H = \mathbb{Q}(i)$

$$\phi : \prod \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} = \pi_0$$

(Q: define this one in terms of $\mathcal{B}$)

Pick $\phi(v_i) = a_i$, * suppose * H is closed
$\phi \neq 0$ $\quad$ " $\ker\phi$

$\Rightarrow L^H/\mathbb{Q}$ is of deg 2 $\Rightarrow L^H = \mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{p_{i_1} \cdots p_{i_m}})$

$\Rightarrow H \xrightarrow{\pi_k} \mathbb{Z}/2\mathbb{Z}$ $\quad k \neq i_1, \dots, i_m$ is surjective.

Suppose $\mathcal{B}$ extends can. basis.

Assume $\phi(e_i) = 1$ for ∞ly many i's.

H contains $J = \{(\dots, b_i, \dots) : b_i = 0$ for $i = i_1, \dots i_m\}$ $\quad$ fix every $\sqrt{p_{ij}}$ $\rightarrow$ fix $\sqrt{p_{i_1} \cdots p_{i_m}}$

but $\exists\ \infty$'ly many $e_i \in J \Rightarrow \overset{\infty\text{ly}}{e_i} \in J \leq H \Rightarrow \overset{\infty\text{ly}}{e_i} \in H$ but $\phi(e_i) \neq 0$

$\Rightarrow e_i \notin \ker\phi = H$ ✗

$\Rightarrow$ Hence $L^H = \mathbb{Q}(\sqrt{\alpha})$ is impossible.

Galois Theory $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$

in general if $L/\mathbb{Q}$ is NOT Galois $p\mathcal{O}_L = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$

Let $L/\mathbb{Q}$ be Galois, finite, p prime.

$$\begin{array}{ccc} L & \mathcal{O}_L & p\mathcal{O}_L = (\mathfrak{p}_1\cdots\mathfrak{p}_r)^e \\ | & | & | \\ \mathbb{Q} & \mathbb{Z} & (p) \end{array}$$

$\sigma \rightsquigarrow \tilde{\sigma} : \mathcal{O}_L/\mathfrak{p}_1 \to \mathcal{O}_L/\mathfrak{p}_1$

$$\begin{tikzcd}[row sep=small] L \arrow[d, dash] \arrow[ddd, dash, bend right] \\ L^I \arrow[d, dash] \\ L^D \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Then: $[L:\mathbb{Q}] = efr$ where $f = [\mathcal{O}_L/\mathfrak{p}_1 : \mathbb{Z}/p\mathbb{Z}]$.

$G = \mathrm{Gal}(L/\mathbb{Q}) \supseteq D(\mathfrak{p}_1|p) = \{\sigma \in G : \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = D$ DECOMPOSITION SUBG.

$\cup|$

$I = I(\mathfrak{p}_1|p) = \{\sigma \in G : \sigma$ induces a trivial action on $\mathcal{O}_L/\mathfrak{p}_1\}$

$$\begin{tikzcd}
L \arrow[dr, dash, "e"'] \arrow[ddr, dash, bend left=60, "|D| = ef"] \arrow[ddd, dash, "efr"'] & \\
& L^I \arrow[d, dash, "f"'] \\
& L^D \arrow[dl, dash, "r"] \\
\mathbb{Q} &
\end{tikzcd}$$

$|I| = e$

$$\begin{tikzcd}
(\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e \arrow[d, dash] \\
\mathfrak{p}_{I,1} \cdots \mathfrak{p}_{I,r} \arrow[d, dash] \\
\mathfrak{p}_{D,1} \cdots \mathfrak{p}_{D,r} \arrow[d, dash] \\
(p)
\end{tikzcd}$$

ramification.

residue fields grow

splitting

$$\begin{tikzcd}
& \text{"}L\mathbb{Q}_p\text{"} \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & \mathbb{Q}_p \\
& \mathbb{Q} \arrow[ur, "\text{"}\subseteq\text{"}", hook] &
\end{tikzcd}$$

"$L\mathbb{Q}_p$" = (1) $L_{\mathfrak{p}_1}$ the completion of L at $\mathfrak{p}_1$

(2) $L = \mathbb{Q}(\alpha)$, $f(\alpha) = 0$

extend $\mathbb{Q}_p$ adjoin a root in $\overline{\mathbb{Q}_p}$ of $f(x) = 0$

$$\begin{tikzcd} & L^D \arrow[r] & L^D\mathbb{Q}_p \arrow[dr, dash, "?"] & \\ L^D \arrow[ur, phantom] & & & \mathbb{Q}_p \\ & \mathbb{Q} \arrow[ul, dash] \arrow[urr] & & \end{tikzcd}$$

$$\begin{tikzcd} K \arrow[d, dash, "efr"'] \\ \mathbb{Q}_p \end{tikzcd} \qquad \begin{tikzcd} \mathcal{O}_K \arrow[d, dash] \\ \mathbb{Z}_p \end{tikzcd} \qquad \begin{tikzcd} p\mathcal{O}_K = \mathfrak{p}^e = (\pi^e) \arrow[d, dash] \\ (p) \end{tikzcd}$$

$\underline{\underline{r=1.}}$

where $(\pi) = \mathfrak{p}$.

$$\begin{tikzcd} K \arrow[dd, dash] \arrow[dr, dash, "I"] & \\ & k^I \arrow[dl, dash] \\ \underline{\underline{\mathbb{Q}_p = k^D}} & \end{tikzcd}$$

Decomp. locally $=$ $\mathrm{Gal}(K/\mathbb{Q}_p)$

$\sigma \in G$ s.t. $\sigma(\mathfrak{p}) = \mathfrak{p} \to \sigma \in D.$

$\underbrace{K/\mathbb{Q}_p}_{r=1}$ finite $\underset{e=1}{\text{unramified}}$ $[K : \mathbb{Q}_p] = efr = f$

fin. unramified $\Longleftrightarrow$ $[K : \mathbb{Q}_p] = [k : \mathbb{F}_p]$

where $k = \mathcal{O}_K/(\pi)$, $\mathbb{F}_p \cong \mathbb{Z}_p/(p) \cong \mathbb{Z}/p\mathbb{Z}$

ex $L = \mathbb{Q}(\sqrt{2})$ $\quad p = 5$ <u>inert</u> $\quad 5\mathcal{O}_L = \text{prime} = \mathfrak{p}$

$$\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$$

$$\text{"}L\mathbb{Q}_5\text{"} \longrightarrow \mathbb{Q}_5(\sqrt{2})$$

$$\text{"}L\mathbb{Q}_5\text{"} \longrightarrow \text{complete } \mathbb{Z}[\sqrt{2}] \text{ at } \mathfrak{p} = 5\mathcal{O}_L$$

$$\text{"}L\mathbb{Q}_5\text{"} = L_5$$

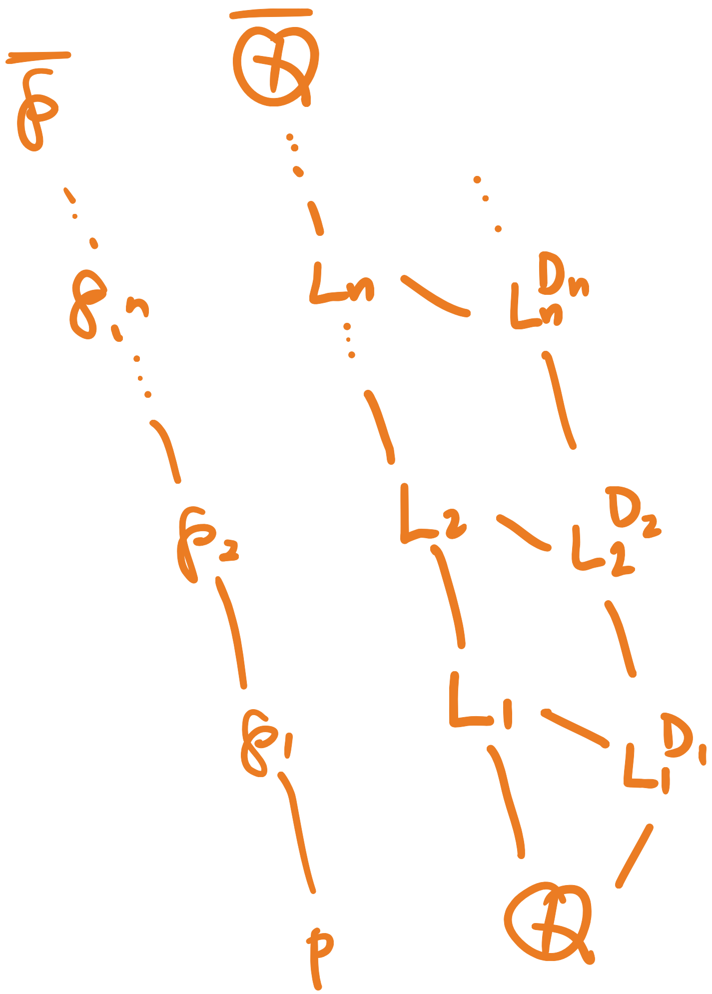
$$\mathcal{O}_{L_5} = \varprojlim \mathbb{Z}[\sqrt{2}]/(5)^n$$

$$\begin{array}{ccc} \mathbb{Q}_5(\sqrt{2}) & & \mathbb{Q}_5(\sqrt{5}) \\ \Big| \ \text{unramified } f=2 & \qquad & \Big| \ \text{ramified } e=2 \\ \mathbb{Q}_5 & & \mathbb{Q}_5 \end{array}$$

$$
\begin{tikzcd}[row sep=small, column sep=small]
L \arrow[dash, dddd] \arrow[dash, dr] \arrow[rdd, bend left=60, dash, "D"] & \\
& L^{I} \arrow[dash, d] \\
& L^{D} \arrow[dash, dl] \\
& \\
\mathbb{Q} &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[row sep=small, column sep=small]
L_{\mathfrak{P}_1} \arrow[dash, dr] \arrow[dr, bend left=60, dash, "D"] & \\
& \mathbb{Q}_p \arrow[dl, phantom, "\|" description] \\
\mathbb{Q}_p &
\end{tikzcd}
$$

$$D(\mathfrak{P}_1 | p) \rightsquigarrow \mathrm{Gal}(L_p / \mathbb{Q}_p) \cong D(\mathfrak{P}_1 | p)$$

Tower:



$$\begin{array}{ccc} D_n & \longrightarrow & D_{n-1} \\ \| & & \| \\ D(\mathfrak{P}_n \mid p) & \longrightarrow & D(\mathfrak{P}_{n-1} \mid p) \end{array}$$

by restriction.

$\mathfrak{P}_{n-1} = \mathfrak{P}_n \cap \mathcal{O}_{L_{n-1}}$

$$D(\overline{\mathfrak{P}} \mid p) := \varprojlim D(\mathfrak{P}_n \mid p)$$

$\overline{\mathfrak{P}} \cap \mathcal{O}_L = \mathfrak{P}$

$$D(\overline{\mathfrak{P}} \mid p) := \varprojlim_{\substack{L/\mathbb{Q} \\ \text{fin. Galois}}} D(L/\mathbb{Q}, \mathfrak{P} \mid p) \subseteq \mathrm{Gal}(L/\mathbb{Q})$$

$$D(\overline{\mathfrak{P}} \mid p) \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

$$\begin{tikzcd}[column sep=small] L_n \arrow[dr, dash, "D_n"] \arrow[ddr, dash] & \\ & L^{D_n} \arrow[d, dash] \\ & \mathbb{Q} \end{tikzcd} \quad \rightsquigarrow \quad \begin{tikzcd} L_n\mathbb{Q}_p \arrow[d, dash] \\ L^{D_n}\mathbb{Q}_p = \mathbb{Q}_p \end{tikzcd} \qquad \mathrm{Gal}(L_n\mathbb{Q}_p/\mathbb{Q}_p) \cong D_n$$

$$\begin{tikzcd} D(\bar{\mathfrak{p}}|p) \arrow[d, phantom, sloped, "\cong"] & \subseteq & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \\ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) & \text{“}\subseteq\text{''} & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \end{tikzcd}$$