Infinite Galois Theory

June 10, 2020

Why is $\overline{\mathbb{Q}}$ a union of <u>finite</u> Galois extensions?

If $[F:\mathbb{Q}] < \infty$, write $F = \mathbb{Q}(\alpha)$.

Let $f(x)$ be min poly of α over $\mathbb{Q}$,
let $\tilde{F}$ = splitting field of $f(x)$ over $\mathbb{Q}$

$\tilde{F} \supset F = \mathbb{Q}(\alpha) \supset \mathbb{Q}$, $\tilde{F}/\mathbb{Q}$ is Galois.

$$F = \mathbb{Q}(\sqrt[3]{2}) \rightsquigarrow \tilde{F} = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$$

Topology on Galois Groups and Galois correspondence

Let L/K be Galois. It is a union of finite Galois extensions of K. For $\sigma \in \mathrm{Gal}(L/K)$, a *basic open set* around σ is a coset $\sigma\,\mathrm{Gal}(L/F)$ for some finite extension F/K inside L, and this means

$$\sigma\,\mathrm{Gal}(L/F) = \{\tau \in \mathrm{Gal}(L/K) : \tau|_F = \sigma|_F\}.$$

Opens are unions of basic opens. The topology on $\mathrm{Gal}(L/K)$ is Hausdorff.

Last time: For Galois L/K and $K \subset E \subset L$, $\mathrm{Gal}(L/E)$ is closed. For all subgroups H, $\mathrm{Gal}(L/L^H) = \overline{H}$. Therefore $\mathrm{Gal}(L/L^H) = H$ when H is closed.

$= \overline{H}$

Theorem (Krull). For Galois L/K, $K \subset E \subset L$, and a *closed* subgroup H, $L^{\mathrm{Gal}(L/E)} = E$ and $\mathrm{Gal}(L/L^H) = H$.

Half of this has been done. Main remaining part is $L^{\mathrm{Gal}(L/E)} \subset E$. See lecture notes (Theorem 4.7). Proof needs finite Galois theory.

Some Consequences of Galois Correspondence

L
$|$
E
$|$
K

- Closed subgroups of $\mathrm{Gal}(L/K)$ are $\mathrm{Gal}(L/E)$ for $K \subset E \subset L$.
- Open subgroups of $\mathrm{Gal}(L/K)$ are $\mathrm{Gal}(L/F)$ where F/K is a finite extension. ($\mathrm{Gal}(L/F)$ has finite index)
- For $\sigma \in \mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/\sigma(E)) = \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$, so closed normal subgroups correspond to Galois E/K in L and open normal subgroups correspond to finite Galois F/K.

Last time someone asked: do *all* normal subgroups correspond to Galois extensions? I had said "no," but ...

Any subgp $H \longrightarrow L^H = L^{\overline{H}}$

$N \triangleleft G$: $L^N = L^{\overline{N}}$

Check: $N \triangleleft G \Rightarrow \overline{N} \triangleleft G$ for topological gp G

$\Rightarrow L^N/K$ is Galois!

Embedding Gal(L/K) into Product of Finite Galois Groups, I

Making F bigger makes Gal(L/F) smaller. Passing to a larger finite *Galois* extension of K, can focus on basic opens σ Gal(L/F) with F/K Galois, in which case σ Gal(L/F) is inverse image for a restriction homomorphism *to a finite group*:

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K), \text{ where } \sigma \mapsto \sigma|_F$$

σG_L — L, $\sigma G_{F'}$ — F', F, K Galois

Each $\sigma \in \mathrm{Gal}(L/K)$ is completely determined by *all* $\sigma|_F$, so we have an embedding

finite groups

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_F \mathrm{Gal}(F/K) \text{ by } \sigma \mapsto (\sigma|_F)_F,$$

where product runs over all finite Galois extensions F/K in L. Can think of the right side algebraically and topologically:

$$(\sigma|_F)_F(\tau|_F)_F = (\sigma\tau|_F)_F$$

Each $G(F/K)$ discrete
Give $\prod_F$ prod. top.
$\Rightarrow \prod_F$ compact

Embedding $\mathrm{Gal}(L/K)$ into Product of Finite Galois Groups, II

Theorem. For Galois L/K, the embedding

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_F \mathrm{Gal}(F/K) \text{ by } \sigma \mapsto (\sigma|_F)_F,$$

where F runs over finite Galois extensions of K in L, identifies $\mathrm{Gal}(L/K)$ with its image both algebraically and topologically (homeomorphism to image that has the subspace topology).

What *is* the image of $\mathrm{Gal}(L/K)$ in the product of finite groups?

$(g_F)_F \in \prod_F \mathrm{Gal}(F/K)$ is $(\sigma|_F)_F \iff g_F|_{F\cap F'} = g_{F'}|_{F\cap F'}$ $\forall F, F'$.

$F - F \cap F' - F'$

The image is *closed* and *compact*, so the Krull topology on $\mathrm{Gal}(L/K)$ is compact.

<u>Closed</u>: If $g_{F_0}|_{F_0\cap F_0'} \neq g_{F_0'}|_{F_0\cap F_0'}$ look at all $(h_F)_F$ with $h_{F_0} = g_{F_0}$,

$h_{F_0'} = g_{F_0'}$, $h_{F_0 \cap F_0'} = g_{F_0 \cap F_0'}$.

Then $(h_F)_F$ is not in image of $Gal(L/K)$, so complement of image is open: $\{g_{F_0}\} \times \{g_{F_0'}\} \times \{g_{F_0 \cap F_0'}\} \times \prod_{F \neq F_0, F_0', F_0 \cap F_0'} \{*\}$ is open for prod top.

Closed $\subset$ cpt $\Rightarrow$ cpt, so

$Gal(L/K)$ is cpt for Krull top.

Embedding Gal(L/K) into Product of Finite Galois Groups, III

The embedding

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_F \mathrm{Gal}(F/K) \quad \text{by } \sigma \mapsto (\sigma|_F)_F$$

lets us topologize Gal(L/K) as subset of product of finite (discrete) groups using the subspace topology for the product topology.

This gives new approach to Krull topology and explains many things as special cases of *general theorems* about topological groups: why topology is (1) Hausdorff, (2) totally disconnected, and (3) discrete if $[L : K] < \infty$.

- Each Gal(F/K) is Hausdorff, tot. disconnected

$\{X_i\}$ all Hausdorff $\Rightarrow \prod X_i$ is Hausdorff

$\{X_i\}$ all tot. disconn $\Rightarrow \prod X_i$ is tot. discon

Subset of Hausdorff/tot disconn has same property

Can **Z** be a Galois group? **R**? S^1?

$\mathbb{Z}$) NO: Infinite compact Hausdorff spaces are uncountable.

$\mathbb{R}$) NO: 1) $\mathbb{R}$ not compact (usual)

2) $\mathbb{R}$ has no finite quotient grp besides $\{0\}$.

($\mathbb{R}$ is divisible group)

S^1) No: S^1 is divisible group.

Infinite Groups as Galois Groups

An infinite Galois group G has many finite quotient groups: the identity of G has a *neighborhood basis* of open (normal) subgroups. Think about neighborhood basis for groups like $\mathbf{R}$ and S^1.

$\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ for finite Galois $F/K \subset L$.

The group G is "well-approximated" by its finite quotient groups G/N ($N =$ open normal subgroup). A new category of groups:

1. compact,
2. Hausdorff,
3. totally disconnected.

Topological groups that are **compact, Hausdorff** and **totally disconnected** are called *profinite* groups (projective limit of finite groups). If finite quotients are all cyclic, call it a *pro-cyclic* group. If finite quotients are all p-groups, call it a *pro-p* group.

Theorem. Every profinite group is the Galois group of some Galois extension. $\longrightarrow$ no control over base field

Inverse Galois problem: is every finite group G a Galois group over $\mathbb{Q}$: is it a quotient group of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$? Expect "yes", open.

$$\left.\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array}\right] Gal(K/\mathbb{Q}) \overset{?}{=} G$$

For profinite groups, "no"

$Card(Gal(\bar{\mathbb{Q}}/\mathbb{Q})) < Card(G)$

for some profinite G.

Good conjecture here?

Making p-adic integers a Galois group over Q

Let's make $\mathbf{Z}_5$ a Galois group over $\mathbf{Q}$, using 5-power cyclotomic extensions.

$$\mathbb{Z}_5 = \{a_1 \bmod 5,\ a_2 \bmod 25,\ a_3 \bmod 125 \ldots\}$$

<u>Earlier</u>

$$(\mathbb{Z}/25)^\times = \mu_4 \times \langle 1+5 \rangle$$

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_{25}) & & \{1\} \\
5\ \big| & & 5\ \big| \\
\mathbb{Q}(\zeta_5) & K_1 & \{a \bmod 25 : a \equiv 1 \bmod 5\} \\
4\ \big| & & 4\ \big| \\
\mathbb{Q} & & (\mathbb{Z}/25)^\times
\end{array}$$

$\langle 7 \bmod 25 \rangle$

4

5

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{Q}(\zeta_{5^{n+1}}) \arrow[dddl, dash] \\
K_n \arrow[urr, dash, "4"] & & \\
 & & \\
 & \mathbb{Q} \arrow[uul, dash, "5^n"] &
\end{tikzcd}$$

Gal$(K_n/\mathbb{Q})$ cyclic of order 5^n

$$\begin{tikzcd}[column sep=small]
 & & \{1\} \arrow[dddl, dash] \\
\mu_4 \arrow[urr, dash, "4"] & & \\
 & & \\
 & (\mathbb{Z}/5^{n+1})^\times \arrow[uul, dash, "5^n"] &
\end{tikzcd}$$

$$\underset{4}{\mu_4} \times \underset{5^n}{\langle 1+5 \rangle} \cong (\mathbb{Z}/5^{n+1})^\times$$

$$\begin{tikzcd}[column sep=small, row sep=small]
 & & & K_3 \cdots \\
 & & K_2 \arrow[ur, dash] & \\
 & K_1 \arrow[ur, dash] & & \\
\mathbb{Q} \arrow[ur, dash] & & &
\end{tikzcd}$$

$K_\infty = \bigcup_{n \geq 1} K_n$ is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathbb{Z}_5$.

cyclotomic $\mathbb{Z}_5$-ext^n of $\mathbb{Q}$.