Infinite Galois Theory

June 9, 2020

Review: Failure of Galois Correspondence

Let $L_n = \mathbf{Q}(\zeta_{2^n})$, so $\mathrm{Gal}(L_n/\mathbf{Q}) \cong (\mathbf{Z}/2^n\mathbf{Z})^\times$ by $\sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a$.

$$\begin{array}{ccc}
\mathbf{Q}(\zeta_{2^\infty}) & = & L \\
\vdots & & \\
\mathbf{Q}(\zeta_8) & & \\
| & & \\
\mathbf{Q}(\zeta_4) & = & \mathbf{Q}(i) \\
| & & \\
\mathbf{Q}(\zeta_2) & = & \mathbf{Q}
\end{array}$$

In $(\mathbf{Z}/2^n\mathbf{Z})^\times$, 5 and 13 each generate $\{a \bmod 2^n : a \equiv 1 \bmod 4\}$. It has index 2 and fixed field $\mathbf{Q}(i)$ ($a \equiv 1 \bmod 4 \Leftrightarrow i^a = i$) for $n \geq 2$.

Every number in $\mathbf{Q}(\zeta_{2^\infty})$ is in some $\mathbf{Q}(\zeta_{2^n})$, so $\langle \sigma_5 \rangle$ and $\langle \sigma_{13} \rangle$ in $\mathrm{Gal}(\mathbf{Q}(\zeta_{2^\infty})/\mathbf{Q})$ have fixed field $\mathbf{Q}(i)$ even though $\langle \sigma_5 \rangle \neq \langle \sigma_{13} \rangle$.

For odd b, $\langle b \bmod 2^n \rangle = \{a \bmod 2^n : a \equiv 1 \bmod 4\}$ for $n \geq 2$ if $b \equiv 1 \bmod 4$ & $b \not\equiv 1 \bmod 8$, so $\langle \sigma_b \rangle$ has fixed field $\mathbf{Q}(i)$ in $\mathbf{Q}(\zeta_{2^\infty})$.

What Happened?

$$\begin{array}{ccc} L & \longleftrightarrow & \{id.\} \\ | & & | \\ E & \longleftrightarrow & H \\ | & & | \\ K & \longleftrightarrow & G \end{array}$$

For an infinite-degree Galois extension L/K, the mappings

$$E \mapsto \mathrm{Gal}(L/E), \quad H \mapsto L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

have $L^{\mathrm{Gal}(L/E)} = E$ (uses Zorn's lemma!) but $\mathrm{Gal}(L/L^H) \supset H$ and $\mathrm{Gal}(L/L^H)$ could be larger than H.

The group $\mathrm{Gal}(L/K)$ has a topology with the following properties:

- multiplication and inversion on $\mathrm{Gal}(L/K)$ are continuous,
- for finite L/K, the topology on $\mathrm{Gal}(L/K)$ is discrete,
- if $K \subset E \subset L$ then $\mathrm{Gal}(L/E)$ is *closed* in $\mathrm{Gal}(L/K)$.
- for subgroups $H \subset \mathrm{Gal}(L/K)$, $L^H = L^{\overline{H}}$ and $\mathrm{Gal}(L/L^H) = \overline{H}$.

So $\mathrm{Gal}(L/L^H) = H \Leftrightarrow H$ is closed. The Galois correspondence is a bijection between all intermediate fields and closed subgroups.

Intuition for Topology on Galois Groups

Idea behind the topology: $\sigma, \tau \in \mathrm{Gal}(L/K)$ are "close" if they agree on a "big" finite subextension F/K in L.

$$\begin{tikzcd} & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ F' \arrow[dr, dash] & & F \arrow[dl, dash] \\ & K & \end{tikzcd}$$

σ, τ

$\sigma = \tau$ on F

Example: $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)/\mathbf{Q})$. When do elements of $\prod\{\pm 1\}$ agree as automorphisms on $\mathbf{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$ or on $\mathbf{Q}(\sqrt{6})$?

signs on $\rightarrow$ $\sqrt{-1} \quad \sqrt{2} \quad \sqrt{3} \quad \sqrt{5} \quad \sqrt{7} \quad \ldots$

$\checkmark \quad \checkmark \quad \checkmark$

[EQUAL]

Example: $\mathrm{Gal}(\mathbf{Q}(\zeta_{2^\infty})/\mathbf{Q})$. When do two 2-adic units agree as automorphisms on $\mathbf{Q}(\zeta_8)$, or on $\mathbf{Q}(\zeta_{2^n})$?

$a = a_0 + 2a_1 + 4a_2 + 8a_3 + \cdots$

$b = b_0 + 2b_1 + 4b_2 + 8b_3 + \cdots$

$a_i, b_j \in \{0, 1\}$

$\zeta_8^a = \zeta_8^{a_0 + 2a_1 + 4a_2}$

$\zeta_8^b = \zeta_8^{b_0 + 2b_1 + 4b_2}$

$\zeta_8^a = \zeta_8^b \iff \underline{a \equiv b \bmod 8}$

$$a \equiv b \bmod 8 \iff \begin{array}{l} a_0 = b_0 \ (=1) \\ a_1 = b_1 \\ a_2 = b_2 \end{array}$$

That's all!

$$\sigma_a = \sigma_b \text{ on } \mathbb{Q}(\zeta_{2^n}) \iff a \equiv b \bmod 2^n$$

$$a_j = b_j \text{ for } j = 0, \ldots, n-1$$

Definition of Topology on Galois Groups

Definition. Let L/K be Galois.
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.
A subset U of $\mathrm{Gal}(L/K)$ is called *open* if each element of U is contained in a basic open set that's inside of U: for each $\sigma \in U$, $\sigma\,\mathrm{Gal}(L/F) \subset U$ for some finite extension F/K in L.

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

Since $F \subset F' \Rightarrow \sigma\,\mathrm{Gal}(L/F') \subset \sigma\,\mathrm{Gal}(L/F)$, making F bigger (but still finite over K!) shrinks the basic open set around σ.

What does $\sigma\,\mathrm{Gal}(L/F)$ really mean? It's the same thing as the set of all τ where $\boxed{\tau|_F = \sigma|_F}$ so a "basic open set" is all the automorphisms that agree on a specified (finite) extension F/K. This implies* $\mathrm{Gal}(L/F)$ has finite index in $\mathrm{Gal}(L/K)$.

$\forall \alpha \in F,\ \tau(\alpha) = \sigma(\alpha) \iff \sigma^{-1}\tau(\alpha) = \alpha \ (\forall \alpha \in F)$
$\iff \sigma^{-1}\tau \in \mathrm{Gal}(L/F)$
$\iff \tau \in \sigma\,\mathrm{Gal}(L/F)$

* See Lemma 4.1 in notes

Examples of Basic Open Sets in Galois Groups

Example. In $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)/\mathbf{Q}) = \prod\{\pm 1\}$, sequences with specified relations among signs in finitely many components and no constraints in remaining components form a basic open set.

Just like basic opens for prod. top. on $\prod_{n \geq 1} \{\pm 1\}$

Example. In $\mathrm{Gal}(\mathbf{Q}(\zeta_{5^\infty})/\mathbf{Q})$, a compatible sequence

$$(a_1 \bmod 5, a_2 \bmod 5^2, a_3 \bmod 5^3, \ldots), \qquad a_1 \not\equiv 0 \bmod 5$$

$a_n \equiv a_{n-1} \bmod 5^{n-1}$

with specified values for one $a_n \bmod 5^n$ and no constraints for later components is a basic open set.

Ex: $\{(a_n)_{n \geq 1} : a_2 \equiv 12, 19, 7 \bmod 25\}$

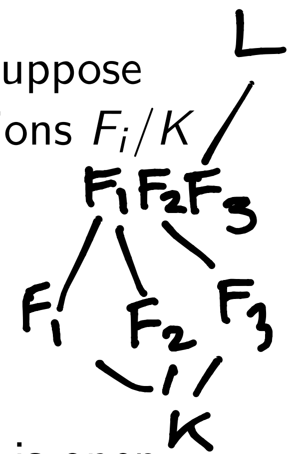
Example. In $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, all σ such that $\sigma(i) = i$ and $\sigma(\sqrt{2}) = -\sqrt{2}$ are a basic open set in this mysterious group.

$\{\sigma \in G(\overline{\mathbb{Q}}/\mathbb{Q}) \mid \text{on } \mathbb{Q}(\sqrt{2}, i),\ \sigma \text{ fixes } i,\ \sigma(\sqrt{2}) = -\sqrt{2}\}$

Open Sets are a Topology

Cosets $\sigma\,\mathrm{Gal}(L/F)$ for varying σ and F are a basis for a topology on $\mathrm{Gal}(L/K)$, like role of open balls to define open sets in a metric space. This is the Krull topology on $\mathrm{Gal}(L/K)$.

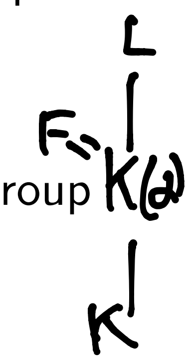
Example. For nonempty open $U_1, \ldots, U_n$ in $\mathrm{Gal}(L/K)$, suppose $\sigma \in \bigcap_i U_i$. Then $\sigma\,\mathrm{Gal}(L/F_i) \subset U_i$ for some finite extensions F_i/K in L. Passing to the finite extension $F := F_1 \cdots F_n$,



$$\underbrace{\sigma\,\mathrm{Gal}(L/F)}_{\text{basic open}} \subset \bigcap_i \sigma\,\mathrm{Gal}(L/F_i) \subset \bigcap_i U_i.$$

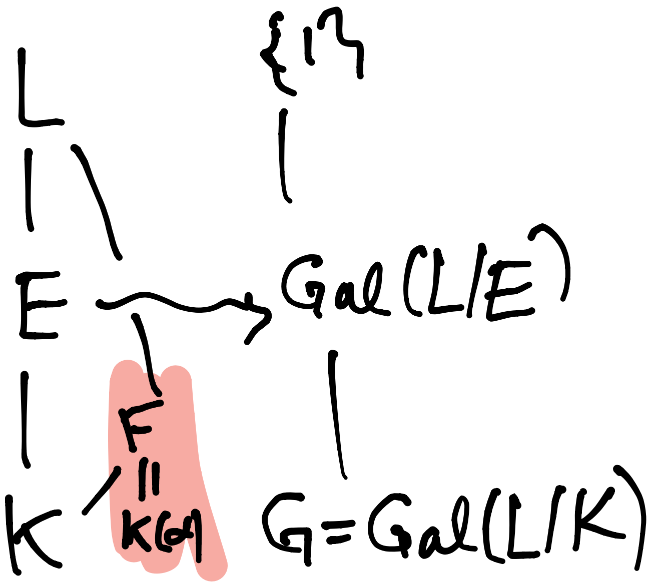
So all elements of $\bigcap_i U_i$ are in basic open in $\bigcap U_i$: $\bigcap_i U_i$ is open.

Example. For $\sigma \neq \tau$, there is $\alpha \in L$ with $\sigma(\alpha) \neq \tau(\alpha)$. For $F = K(\alpha)$, $\sigma|_F \neq \tau|_F$, so $\sigma\,\mathrm{Gal}(L/F) \neq \tau\,\mathrm{Gal}(L/F)$. In fact, $\sigma\,\mathrm{Gal}(L/F) \cap \tau\,\mathrm{Gal}(L/F) = \emptyset$ since different cosets of a subgroup are *disjoint*. Thus the topology on $\mathrm{Gal}(L/K)$ is Hausdorff.



Closed Subgroups

Theorem. For $K \subset E \subset L$, $\mathrm{Gal}(L/E)$ is closed.



↳ Show $\mathrm{Gal}(L/K) - \mathrm{Gal}(L/E)$ is open.

Pick $\sigma \in \mathrm{Gal}(L/K) - \mathrm{Gal}(L/E)$

For some $\alpha \in E$ s.t. $\sigma(\alpha) \neq \alpha$.

Let $F = K(\alpha)$, so $[F:K] < \infty$

Consider $\sigma\mathrm{Gal}(L/F)$.

It's basic open and is $\{\tau \in \mathrm{Gal}(L/K) : \tau|_F = \sigma|_F\}$.

So τ in here has $\tau(\alpha) = \sigma(\alpha) \neq \alpha$.

All of $\mathrm{Gal}(L/E)$ fixes α. So $\sigma\mathrm{Gal}(L/F) \cap \mathrm{Gal}(L/E) = \emptyset$

Closure of a Subgroup

Theorem. For a subgroup H of $\mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/L^H) = \overline{H}$.

$\mathrm{Gal}(L/L^H) = \{\tau : \tau \text{ fixes everything that } H \text{ fixes}\} \supset H.$

Saw this is closed on previous slide.

So $H \subset \mathrm{Gal}(L/L^H) = \text{closed} \Rightarrow \boxed{\overline{H} \subset \mathrm{Gal}(L/L^H)}$

Here, want equality

Pick $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \notin \overline{H}$. Show $\sigma \notin \mathrm{Gal}(L/L^H)$

$\sigma \notin \overline{H} = \text{closed} \Rightarrow \underbrace{\sigma\, \mathrm{Gal}(L/F)}_{\{\tau : \tau = \sigma \text{ on } F\}} \subset \underbrace{\mathrm{Gal}(L/K) - \overline{H}}_{\text{open}}$.

By enlarging F (splitting field over K) we can suppose F/K is $\boxed{\text{Galois}}$ and $\boxed{\text{still finite}}$: doing this (Increase F) shrinks $Gal(L/F)$, so we can assume our basic open $\sigma Gal(L/F)$ has F/K Galois.

Compare σ on F to H on F.

$\sigma Gal(L/F)$ disjoint from $\overline{H}$ $\Rightarrow$ nothing in $\overline{H}$ looks like σ on F.

Claim: There is some $\alpha \in F$ s.t. $\sigma(\alpha) \neq \alpha$ while $h(\alpha) = \alpha$ $\forall h \in H$.

If not, then $\boxed{\text{for all } \alpha \in F, \; h(\alpha) = \alpha \; \forall h \in H \Rightarrow \sigma(\alpha) = \alpha}$.

So σ fixes the fixed field of H inside F $\hookrightarrow L^H \cap F$

That says in $Gal(F/K)$, the fixed field of $\sigma|_F$ contains fixed field of $H|_F$. Then by finite Galois Theory, $\sigma|_F$ is contained in $H|_F$: some $h \in H$ looks like σ on F. Then $h|_F = \sigma|_F \Rightarrow h \in \sigma Gal(L/F)$. But $\sigma Gal(L/F)$ is disjoint from $\overline{H}$, and thus is disjoint from H: contradiction! That proves the claim.

From the claim, an $\alpha \in F$ with $\sigma(\alpha) \neq \alpha$ and $h(\alpha) = \alpha\ \forall\, h \in H$ is an element of L^H moved by σ, so $\sigma \notin \mathrm{Gal}(L/L^H)$.

Thus each $\sigma \in \mathrm{Gal}(L/K) - \overline{H}$ is not in $\mathrm{Gal}(L/L^H)$ too, so $\boxed{\mathrm{Gal}(L/L^H) \subset \overline{H}}$. We showed at the start that $\mathrm{Gal}(L/L^H) \supset \overline{H}$, so we have equality:

$$\mathrm{Gal}(L/L^H) = \overline{H}.$$