The Galois Correspondence

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

Monday April 28, 2025

In this file: §4.1.5 of lecture notes.

1. The main theorem of Galois theory: the Galois Correspondence

Recall

Theorem

For a finite extension $K \subset L$ with $G = \mathrm{Aut}_K(L)$, the following are equivalent:

1. *$K \subset L$ is Galois, i.e., $|G| = [L : K]$;*
2. *$K = L^G$;*
3. *The extension $K \subset L$ is normal and separable;*
4. *L is a splitting field over K of some separable polynomial in $K[x]$.*

Let $K \subset L$ be a field extension, and let $G = \mathrm{Aut}_K(L)$.

Definition-Lemma.

- A subfield M of L containing K is called an intermediate field of $K \subset L$, and denoted as $\underline{K \subset M \subset L}$.
- For any intermediate field $K \subset M \subset L$, $\mathrm{Aut}_M(L)$ is a subgroup of G;
- For any subgroup H of G,

$$L^H \stackrel{\text{def}}{=} \{a \in L : \sigma(a) = a, \ \forall\, \sigma \in H\}$$

  is an intermediate field of $K \subset L$, called the fixed field of H.

$$\{K \subset \underline{M} \subset L\} \longleftrightarrow \{\underline{H} \subset G\}$$

For a field extension $K \subset L$ and $G = \mathrm{Aut}_K(L)$, have

$$\{\text{intermediate fields } K \subset M \subset L\} \underset{F}{\overset{\Gamma}{\rightleftarrows}} \{\text{subgroups } H \subset G\},$$

$$\Gamma(M) = \mathrm{Aut}_M(L) \quad \text{and} \quad F(H) = L^H = \{a \in L : \sigma(a) = a,\ \forall \sigma \in H\}.$$

Lemma. Both F and Γ are inclusion reversing:

$$M_1 \subset M_2 \implies \Gamma(M_1) \supset \Gamma(M_2),$$
$$H_1 \subset H_2 \implies F(H_1) \supset F(H_2).$$

Moreover, for all intermediate field M and subgroup H of G, one has

$$M \subset F(\Gamma(M)), \quad H \subset \Gamma(F(H)).$$

If H is a finite subgroup of G, Artin's Theorem gives $H = \Gamma(F(H))$

Proof.

Theorem (Fundamental Theorem of Galois Theory)

Let $K \subset L$ be a finite Galois extension. Then

1. *for any intermediate $K \subset M \subset L$, the extension $M \subset L$ is Galois;*
2. *the two maps Γ and F are inverses of each other;*
3. *for an intermediate field $K \subset M \subset L$, the extension $K \subset M$ is Galois if and only if $\Gamma(M) = \mathrm{Aut}_M(L)$ is a normal subgroup of $\mathrm{Aut}_K(L)$, and in this case,*

$$\mathrm{Aut}_K(M) = \mathrm{Aut}_K(L)/\mathrm{Aut}_M(L).$$

The correspondence between intermediate fields $K \subset M \subset L$ and subgroups fof G is called the The Galois Correspondence.

Proof of Fundamental Thm. of Galois Theory. Let $K \subset L$ be finite Galois.

1. L is splitting field over K of a separable $f \in K[x]$. Then L is also a splitting field over M of the separable $f \in M[x]$. Thus $M \subset L$ is Galois.

2. Already know that $H = \Gamma(F(H))$ by Artin's Theorem. For any intermediate $K \subset M \subset L$, by (i), $M \subset L$ is Galois, so $M = F(\Gamma(M))$.

3. Assume first that $K \subset M$ is Galois.
   - M is the splitting field of some $g(x) \in K[x]$, so $M = K(R_g)$.
   - $\sigma(R_g) = R_g$ for every $\sigma \in \mathrm{Aut}_K(L)$, so $\sigma(M) = M$. Thus have the group homomorphism

     $$\phi : \mathrm{Aut}_K(L) \longrightarrow \mathrm{Aut}_K(M), \sigma \longmapsto \sigma|_M$$

     with $\ker \phi = \mathrm{Aut}_M(L)$. Thus $\mathrm{Aut}_M(L)$ is a normal subgroup of $\mathrm{Aut}_K(L)$.

Proof continued:

- Have injective group homomorphism
$$[\phi] : \ \mathrm{Aut}_K(L)/\mathrm{Aut}_M(L) \longrightarrow \mathrm{Aut}_K(M).$$
- As both $K \subset L$ and $K \subset M$ are Galois,
$$|\mathrm{Aut}_K(L)/\mathrm{Aut}_M(L)| = \frac{|\mathrm{Aut}_K(L)|}{|\mathrm{Aut}_M(L)|} = \frac{[L : K]}{[L : M]} = [M : K]$$
$$= |\mathrm{Aut}_K(M)|.$$
Thus $[\phi]$ is a group isomorphism.

Assume now that $\mathrm{Aut}_M(L)$ is a normal subgroup of $\mathrm{Aut}_K(L)$.

- Let $\sigma \in G$. For any $a \in M$ and $\tau \in \mathrm{Aut}_M(L)$, have
$$\sigma^{-1}\tau\sigma \in \mathrm{Aut}_M(L),$$
so $(\sigma^{-1}\tau\sigma)(a) = a$, i.e., $\tau(\sigma(a)) = \sigma(a)$, so $\sigma(a) \in F(\Gamma(M))$. By (ii), $F(\Gamma(M)) = M$, so $\sigma(a) \in M$.

Proof continued:

- Thus again have group homomorphism
$$\phi : \mathrm{Aut}_K(L) \longrightarrow \mathrm{Aut}_K(M), \sigma \longmapsto \sigma|_M,$$
and injective group homomorphism
$$[\phi] : \ \mathrm{Aut}_K(L)/\mathrm{Aut}_M(L) \longrightarrow \mathrm{Aut}_K(M).$$
- Since $|\mathrm{Aut}_K(M)| \leq [M : K]$, one has $|\mathrm{Aut}_K(M)| = [M : K]$. Thus $K \subset M$ is Galois.
- End of proof.

Corollary

A finite Galois extension $K \subset L$ has finitely many intermediate subfields.

Example. $\mathbb{F}_p \subset \mathbb{F}_{p^n}$:

- $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is Galois because $\mathbb{F}_{p^n}$ is a splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$;
- $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, generated by the Frobenius isomorphism $\sigma : a \mapsto a^p$.
- One subgroup of G of order m for each $m|n$, generated by σ^d, where $d = n/m$.
- The fixed field of $\langle \sigma^d \rangle$ is the subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^n}$.

Example. $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{(2\pi i)/3}$.

- Know that $|G = \mathrm{Aut}(\mathbb{Q})(L)| = .[L : \mathbb{Q}] = 6$.
- f has exactly three roots, namely
$$r_1 = \sqrt[3]{2}, \qquad r_2 = \omega\sqrt[3]{2}, \qquad r_3 = \omega^2\sqrt[3]{2},$$
so $G \cong S_3$, permutation group of the three roots.
- Every $g \in G$ must satisfy
$$g(\omega) \in \{\omega, \omega^2\}, \qquad g(\sqrt[3]{2}) \in \{r_1, r_2, r_3\}.$$
- Define $\sigma, \tau \in G$ by
$$\sigma(\omega) = \omega, \qquad \sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \qquad \tau(\omega) = \omega^2, \qquad \tau(\sqrt[3]{2}) = \sqrt[3]{2}.$$
Then $\sigma^3 = \tau^2 = \mathrm{Id}$, and
$$G = \{e,\ \sigma,\ \sigma^2,\ \tau,\ \tau\sigma,\ \sigma\tau = \tau\sigma^2\}.$$

Among the 6 intermediate fields:

- the extensions

$$\mathbb{Q} \subset \mathbb{Q}, \qquad \mathbb{Q} \subset \mathbb{Q}(\omega), \qquad \mathbb{Q} \subset L = \mathbb{Q}(\omega, \sqrt[3]{2})$$

  are Galois, corresponding to the three normal subgroups

$$\{e\}, \qquad \{e, \sigma, \sigma^2\}, \qquad G;$$

- the other three extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}), \qquad \mathbb{Q} \subset \mathbb{Q}(\omega\sqrt[3]{2}), \qquad \mathbb{Q} \subset \mathbb{Q}(\omega^2\sqrt[3]{2})$$

  are not Galois.

$$\begin{tikzcd}[column sep=small]
 & \{e\} \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] \arrow[drrr, dash] & & & \\
\langle\sigma\rangle \arrow[dr, dash] & & \langle\tau\rangle \arrow[dl, dash] & \langle\tau\sigma\rangle \arrow[dll, dash] & \langle\sigma\tau\rangle = \mathrm{Aut}_M(L) \arrow[dlll, dash] \\
 & \langle\sigma,\tau\rangle = \mathrm{Aut}_{\mathbb{Q}}(L) & & &
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt[3]{2},\omega) \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] \arrow[drrr, dash] & & & \\
\mathbb{Q}(\omega) \arrow[dr, dash] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[dll, dash] & \mathbb{Q}(\omega^2\sqrt[3]{2}) = M \arrow[dlll, dash] \\
 & \mathbb{Q} & & &
\end{tikzcd}$$