MATH4302, Algebra II

Jiang-Hua Lu

The University of Hong Kong

Thursday April 28, 22

Topics for today:

1. §3.1.3: The main theorem of Galois theory: the Galois Correspondence
2. §3.1.5: Examples of the Galois Correspondence

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$

Recall the 4 characterizations of finite Galois extensions:

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. *$K = L^G$;* (Alway have $K \subset L^G$)
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 $K \subset M \subset L$.
- 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.

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

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

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

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = L$. $M = \mathbb{Q}$

$F(\Gamma(M)) = \Gamma(G = \{e\})$

$= L$

Lemma. For all intermediate field M and subgroup H of G, one has

$$M \subset F(\Gamma(M)), \qquad H \overset{=}{\subset} \Gamma(F(H)).$$

When H is a finite subgroup of G, Artin's Theorem gives $\underline{H = \Gamma(F(H))}$.

$F(\Gamma(M)) = \{a \in L : \sigma(a) = a \text{ for } \forall \sigma \in \Gamma(M)\}$

$= \{a \in L : \sigma(a) = a \text{ for } \forall \sigma \in G,\ \sigma(m) = m\ \forall m \in M\}$

$\supseteq M$

jhlu@maths.hku.hk $\mathrm{Aut}_{\mathbb{Q}}(\overline{\mathbb{Q}})$

Theorem (Fundamental Theorem of Galois Theory)

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

1. *the two maps Γ and F are inverses of each other;* i.e. $M = F(\Gamma(M))$
2. *for any intermediate $K \subset M \subset L$,*
    1. *the extension $M \subset L$ is Galois;*
    2. *$K \subset M$ 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,*

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

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7} + i\sqrt{130} / \sqrt{11})$

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.

2nd char. of Galois ext.

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,

$$\begin{aligned} |\mathrm{Aut}_K(L)/\mathrm{Aut}_M(L)| &= \frac{|\mathrm{Aut}_K(L)|}{|\mathrm{Aut}_M(L)|} = \frac{[L : K]}{[L : M]} = [M : K] \\ &= |\mathrm{Aut}_K(M)|. \end{aligned}$$

  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.

$\mathbb{Q}(\sqrt{2}+i) \supseteq \mathbb{Q}$

$(a+b)^p = a^p + b^p$

Example. $\mathbb{F}_p \subset \mathbb{F}_{p^n}$: p is a prime number, $n \geq 1$

- $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ 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 $\sigma : a \mapsto a^p$.

$\langle \sigma \rangle \subset G$ ① $\sigma^n = 1$. $\sigma^{n'} \neq 1$ $n' < n$. $(\sigma^d)^m = \sigma^n = 1$

- One subgroup of G of order m for each $m | n$, generated by σ^d, $\in G$ where $d = n/m$.

$n = md$

- 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 $\omega = e^{(2\pi i)/3}$.

splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$.

- 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.

$\mathbb{Z}_2 \times \mathbb{Z}_3$

$\simeq \mathbb{Z}_6$

- Every $g \in G$ must satisfy

$$g(\omega) \in \{\omega, \omega^2\}, \qquad g(\sqrt[3]{2}) \in \{r_1, r_2, r_3\}.$$

$x^3 - 1 = 0$

- 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

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

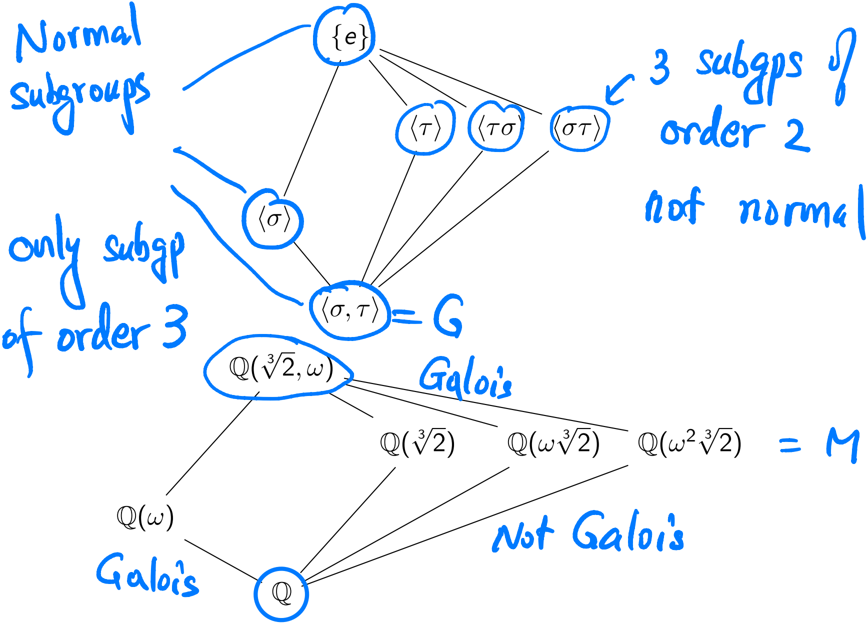
  are Galois, corresponding to the three normal subgroups

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

- 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.



Normal subgroups
$\{e\}$
$\langle\tau\rangle$
$\langle\tau\sigma\rangle$
$\langle\sigma\tau\rangle$
3 subgps of order 2 not normal
$\langle\sigma\rangle$
only subgp of order 3
$\langle\sigma,\tau\rangle = G$
$\mathbb{Q}(\sqrt[3]{2},\omega)$
Galois
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\omega\sqrt[3]{2})$
$\mathbb{Q}(\omega^2\sqrt[3]{2}) = M$
$\mathbb{Q}(\omega)$
Galois
Not Galois
$\mathbb{Q}$