4-25-25 (WEEK 10) Shun/翔海 (@shun4midx)

GALOIS EXTENSIONS

DEFINITION

L/K is called a normal extension if $\forall \alpha \in L$, α is alg over K, and $m_{\alpha,K}$ splits over L

PROPOSITION 1

L/K is finite and normal $\Leftrightarrow$ L is a splitting field for f over K

Proof

"$\Rightarrow$": Write $L = K(\alpha_1, \dots, \alpha_n)$ and let $f(x) = m_{\alpha_1,K} \dots m_{\alpha_n,K}$

Claim: L is a splitting field Σ of $f(x)$, i.e. "$L = \Sigma$"

Proof

"$\subseteq$": $\forall \alpha_i$, $f(\alpha_i) = 0 \Rightarrow \alpha_i \in \Sigma \Rightarrow L \subseteq \Sigma$ ✓

"$\supseteq$": $\forall \beta$: root of $m_{\alpha_i,K}$, by def of normal, $\beta \in L$ ✓

"$\Leftarrow$": Let $L = K(\alpha_1, \dots, \alpha_n)$, $\{\alpha_1, \dots, \alpha_n\}$ is the set of all roots of $f(x)$

Note: $f(x)$ and $m_{\alpha_1,K} \cdots m_{\alpha_n,K}$ have the same set of roots

$\therefore$ We know $\forall \beta \in K(\alpha_1, \dots, \alpha_n)$, $m_{\beta,K}$ splits over L, i.e. L/K is normal

Moreover, $\forall \alpha_i$, α_i is alg over $K \Rightarrow L/K$ is finite. □

REMARK

If L/K is normal, then $\forall M$ with $L \supseteq M \supseteq K$, L/M is normal but M/K need not be normal

Proof

$\forall \alpha \in L$, $m_{\alpha,M} \mid m_{\alpha,K}$, so "$m_{\alpha,K}$ splits over $L \Rightarrow m_{\alpha,M}$ splits over L"

However, "M/K need not be normal":

↳ Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, which is a splitting field for $x^3 - 2$ over $\mathbb{Q}$

But $M = \mathbb{Q}(\sqrt[3]{2})$ is not normal, since $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$ does not split over $\mathbb{Q}(\sqrt[3]{2})$

DEFINITION

Given L/K, $(\mathrm{Aut}(L), \circ)$ is a group. Then, $\mathrm{Aut}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\} \leq \mathrm{Aut}(L)$

PROPOSITION 2

Let L be finite, normal, and $L \supseteq M \supseteq K$. Then, TFAE

(a) M/K is normal

(b) $\forall \sigma \in \mathrm{Aut}(L/K)$, $\sigma(M) \subseteq M$

(c) $\forall \sigma \in \mathrm{Aut}(L/K)$, $\sigma(M) = M$

$$L \xrightarrow{\sigma} L$$
$$M \longmapsto M?\ \neq M?$$

Proof

(a)$\Rightarrow$(b): $\forall \beta \in M$, $m_{\beta,K}(\sigma(\beta)) = \sigma(m_{\beta,K}(\beta)) = 0$

$\therefore \sigma(\beta)$ is a root of $m_{\beta,K}$

$\therefore \sigma(\beta) \in M$ since $m_{\beta,K}$ splits over M.

(b)$\Rightarrow$(c): $\because M/K$ is alg $\therefore \sigma|_M$ is nontrivial $\Rightarrow$ surjective

(c)$\Rightarrow$(a): Assume L is a splitting field for f over K. For $\beta \in M$, if $\gamma \in L$ is another root of $m_{\beta,K}$, then we have

$$\begin{tikzcd}
L \arrow[r, "\exists\sigma", "\sim"'] & L \\
K(\beta) \arrow[u, "\text{splitting field for } f \text{ over } K(\beta)"] \arrow[r, "\tau_1", "\sim"'] & K(\gamma) \arrow[u, "\text{splitting field}"'] \\
& K \arrow[ul] \arrow[u]
\end{tikzcd}$$

Here, σ extends τ_1, so it fixes K, i.e. $\sigma \in \mathrm{Aut}(L/K)$. By assumption, $\gamma = \tau_1(\beta) = \sigma(\beta) \in M$ □

DEFINITION

- L/K is called a Galois extension if L/K is finite, normal, and separable, i.e. L is a splitting field for some separable poly over K
- If L/K is Galois, then define $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$

PROPOSITION

If L/K is Galois, then $|\mathrm{Gal}(L/K)| = [L:K]$. Otherwise, $|\mathrm{Aut}(L/K)| < [L:K]$

Proof

We know:

- normal $\Rightarrow \forall \beta \in L$, $m_{\beta,K}$ splits over L
- separable $\Rightarrow \exists$ exactly $[L:K]$ extensions $\sigma: L \to L$ of id_K. Also, L/K is alg $\Leftrightarrow \sigma$ is an auto
  That is, $|\mathrm{Aut}(L/K)| = [L:K]$

Otherwise, $|\mathrm{Aut}(L/K)| < [L:K]$ □

DEFINITION

Let G be a subgroup of $\mathrm{Aut}(L)$. Then, $\underbrace{\mathrm{Inv}\ G}_{\text{invariant}} = \{\alpha \in L \mid \sigma(\alpha) = \alpha\ \forall \sigma \in G\}$ is a subfield of L

THEOREM (Artin)

If $\underbrace{G}_{\text{finite}} \leq \mathrm{Aut}(L)$, then $|G| = [L : \mathrm{Inv}\ G]$, and $G = \mathrm{Aut}(L/\mathrm{Inv}\ G)$, i.e. $L/\mathrm{Inv}\ G$ is a Galois group

Proof

Claim: $[L : \mathrm{Inv}\ G] \leq |G|$

Proof

Assume that $[L : \mathrm{Inv}\ G] > |G| =: n$. Let $G = \{\sigma_1 := \mathrm{id}, \dots, \sigma_n\}$ and lin indep $b_1, \dots, b_{n+1} \in L$ over $\mathrm{Inv}\ G$

Consider

$$(*) \begin{cases} \sigma_1(b_1)x_1 + \dots + \sigma_1(b_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(b_1)x_1 + \dots + \sigma_n(b_{n+1})x_{n+1} = 0 \end{cases}$$

, which has a nontrivial solution, since #variables > #equations

Choose one $(a_1, \dots, a_{n+1})$ with the smallest number, say m, nonzero members

By reordering, we may assume it is $(a_1, \dots, a_m, 0, \dots, 0)$

If $m=1$, then $\underbrace{\sigma_1(b_1)}_{b_1 \neq 0} a_1 = 0 \Rightarrow a_1 = 0$ ⨳

Hence, $m > 1$, and $\sigma_i(b_1)a_1 + \dots + \sigma_i(b_m)a_m = 0$ $(**)$ $\forall i = 1, \dots, n$

By multiplying a_m^{-1}, we may assume $a_m = 1$.

Observe, for $i=1$, $b_1 a_1 + \dots + b_m a_m = 0$, so not all $a_i \in \mathrm{Inv}\ G$, say $a_1 \notin \mathrm{Inv}\ G$ and $\sigma_t(a_1) \neq a_1$ for some t.

By applying σ_t to $(**)$, we get $\sigma_t\sigma_i(b_1)\sigma_t(a_1) + \dots + \sigma_t\sigma_i(b_m)\sigma_t(a_m) = 0$ $\forall i = 1, \dots, n$

As $\{\sigma_t\sigma_1, \dots, \sigma_t\sigma_n\} = \{\sigma_1, \dots, \sigma_n\}$, hence we have $(***)$ $\sigma_i(b_1)\sigma_t(a_1) + \dots + \sigma_i(b_m)\underbrace{\sigma_t(a_m)}_{= 1\ \because a_m = 1} = 0$ $\forall i = 1, \dots, n$

$(**) - (***)$: $\sigma_i(b_1)(\underbrace{a_1 - \sigma_t(a_1)}_{\neq 0\ \because a_1 \neq \sigma_t(a_1)}) + \dots + \sigma_i(b_{m-1})(a_{m-1} - \sigma_t(a_{m-1})) = 0$ $\forall i = 1, \dots, n$

$\therefore$ We find that $(a_1 - \sigma_t(a_1), \dots, a_{m-1} - \sigma_t(a_{m-1}), 0, \dots, 0)$ is a nontrivial solution of $(*)$, smaller than m nonzero terms ⨳

Now, by def, $G \leq \mathrm{Aut}(L/\mathrm{Inv}\ G)$, so $|G| \leq |\mathrm{Aut}(L/\mathrm{Inv}\ G)| \leq [L : \mathrm{Inv}\ G] \leq |G| \Rightarrow |G| = |\mathrm{Aut}(L/\mathrm{Inv}\ G)| = [L : \mathrm{Inv}\ G]$

$\therefore G = \mathrm{Aut}(L/\mathrm{Inv}\ G)$ and $L/\mathrm{Inv}\ G$ is Galois □

COROLLARY

L/K is Galois $\Leftrightarrow \mathrm{Inv}\ \mathrm{Aut}(L/K) = K$

Proof

"$\Rightarrow$": $\because L/K$ is Galois $\therefore |\mathrm{Aut}(L/K)| = [L:K]$. By thm, $[L:K] = |\mathrm{Aut}(L/K)| = [L : \mathrm{Inv}\ \mathrm{Aut}(L/K)]$ $\therefore K = \mathrm{Inv}\ \mathrm{Aut}(L/K)$ □

"$\Leftarrow$": By thm, ok.

Shun/翔海 (@shun4midx)

DEFINITION

Let $f \in K[x]$ be separable and L be a splitting field for f over K. $\mathrm{Gal}(L/K)$ is called the Galois group of f.

FACT

If $\deg f = n$, then the Galois group of f can be regarded as a subgroup of S_n

Proof

Let $\{\alpha_1, \dots, \alpha_n\}$ be the set of roots of f.

For $\sigma \in \mathrm{Gal}(L/K)$, $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0 \Rightarrow \sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_n\} = A$

So, $\sigma : \{\alpha_1, \dots, \alpha_n\} \longrightarrow \{\alpha_1, \dots, \alpha_n\}$ is 1-1 and thus onto

$\therefore \sigma|_A \in S_n$

EXAMPLE

To determine the Galois group of $x^4 - 2$

The roots of x^4-2 are $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$

$\therefore$ The splitting field for x^4-2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i) =: L$

- $[L:\mathbb{Q}] = \overbrace{[L:\mathbb{Q}(\sqrt[4]{2})]}^{\mathbb{Q}(\sqrt[4]{2})(i)}\overbrace{[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]}^{(x^4-2)} = 2(4) = 8$
- $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$: $\sigma: i \longmapsto i, \ \sqrt[4]{2} \longmapsto \sqrt[4]{2}i$, $\tau: i \longmapsto -i, \ \sqrt[4]{2} \longmapsto \sqrt[4]{2}$

  Then, $\sigma^4 = \tau^2 = id$, $\tau\sigma\tau = \sigma^3$

  $\therefore \langle \sigma, \tau \mid \sigma^4 = \tau^2 = id, \tau\sigma\tau = \sigma^3 \rangle \subseteq \mathrm{Gal}(L/\mathbb{Q})$, where $|\mathrm{Gal}(L/\mathbb{Q})| = 8$

  $\therefore \mathrm{Gal}(L/\mathbb{Q}) \cong D_8$
- $G = \langle\sigma\rangle \leq \mathrm{Gal}(L/\mathbb{Q})$: $\mathrm{Inv}\, G = ?$

  ↳ $\because |G| = 4$, $[L:\mathrm{Inv}\, G] = 4 \Rightarrow [\mathrm{Inv}\, G : \mathbb{Q}] = 2$. As $\mathbb{Q}(i) \subseteq \mathrm{Inv}\, G$, thus $\mathrm{Inv}\, G = \mathbb{Q}(i)$ ($\because [\mathbb{Q}(i):\mathbb{Q}] = 2$)
- Similarly, $G = \langle\tau\rangle \Rightarrow \mathrm{Inv}\, G = \mathbb{Q}(\sqrt[4]{2})$