4-18-25 (WEEK 9) Shun / 翔海 (@shun4midx)

SPLITTING FIELDS

DEFINITION

Let $f(x)$ be a nonconstant polynomial in $K[x]$.
L is called a splitting field for f over K if L is the smallest field over which f splits

THEOREM 1 (Existence of a splitting field)

If $f(x)$ is of $\deg n>0$, then $\exists$ a splitting field L for f over K with $[L:K]\le n!$

Proof

By induction on n,

- $n=1$: $f(x)=ax+b$, $a,b\in K \Rightarrow L=K(-\frac{b}{a})=K \Rightarrow [L:K]=1$
- $n>1$: By Kronecker's Thm, $\exists\, K_1/K$ and $\alpha\in K_1$, s.t. $f(\alpha_1)=0$
  By division algorithm, $\exists f_1(x)\in K(\alpha_1)[x]$ with $\deg f_1=n-1$, s.t. $f(x)=(x-\alpha_1)f_1(x)$
  By induction hypothesis, $\exists$ a splitting field L for f_1 over $K(\alpha_1)$ with $[L:K(\alpha_1)]\le n!$
  By def, $f_1(x)=\lambda(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$, $\alpha_i\in L$
  Hence, $f(x)=\lambda(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ and $L=K(\alpha_1)(\alpha_2,\ldots,\alpha_n)=K(\alpha_1,\ldots,\alpha_n)$
  $\therefore [L:K]=[L:K(\alpha_1)][K(\alpha_1):K]\le(n-1)!\,n=n!$ $\square$

FACT

$K\xrightarrow{\sim}\tau(K)$

Let K, L be two fields and $\tau: K\hookrightarrow L$ be a nontrivial homo. Then, $\exists\ \bar{\tau}: K[x]\xrightarrow{\sim}\tau(K)[x]$ and if $f(x)$ is irred, then
$a_nx^n+\ldots+a_0\longmapsto\tau(a_n)x^n+\ldots+\tau(a_0)$
$\bar{\tau}(f)$ is also irred

Proof

- $\tau: K\xrightarrow{\sim}\tau(K)$ since $\operatorname{Ker}\tau=\{0\}\Rightarrow\bar{\tau}: K[x]\xrightarrow{\sim}\tau(K)[x]$
- If $\bar{\tau}(f)=gh$ with $\deg g>0$, $\deg h>0$, then $f=\bar{\tau}^{-1}(g)\,\bar{\tau}^{-1}(h)$ $\square$

LEMMA

Given $K(\alpha)/K$ with α being algebraic over K, if $\tau: K\to L$ is nontrivial, then $\exists$ an extension σ of τ from $K(\alpha)$ to $L \Leftrightarrow \exists\,\beta\in L$, s.t. $\bar{\tau}(m_{\alpha,K})(\beta)=0$

Proof

"$\Rightarrow$": let $\beta=\sigma(\alpha)$ and $m_{\alpha,K}: x^n+a_{n-1}x^{n-1}+\ldots+a_0$
Then, $\bar{\tau}(m_{\alpha,K})(\beta)=\bar{\tau}(m_{\alpha,K})(\sigma(\alpha))=\sigma(\alpha)^n+\underbrace{\tau(a_{n-1})}_{=\sigma(a_{n-1})}\sigma(\alpha)^{n-1}+\ldots+\underbrace{\tau(a_0)}_{=\sigma(a_0)}=\sigma(\alpha^n+a_{n-1}\alpha^{n-1}+\ldots+a_0)=\sigma(0)=0$ $\square$

"$\Leftarrow$": First observe that $\bar{\tau}(m_{\alpha,K})=m_{\beta,\tau(K)}$ since $\bar{\tau}(m_{\alpha,K})(\beta)=0$ and it is irreducible and monic
Then, σ comes from the following diagram:

$$\begin{tikzcd}
K[x] \arrow[r, "\bar{\tau}", "\sim"'] \arrow[d] & \tau(K)[x] \arrow[d] \\
K[x]/\langle m_{\alpha,K}\rangle \arrow[r, "\sim"] \arrow[d, "\wr\ ev_\alpha"] & \tau(K)[x]/\langle\bar{\tau}(m_{\alpha,K})\rangle = \tau(K)[x]/\langle m_{\beta,\tau(K)}\rangle \arrow[d, "\wr\ ev_\beta"] \\
K(\alpha) \arrow[r, bend left, "\exists\ ✓"] & K(\beta)
\end{tikzcd}$$

(evaluation map は "$x\leftarrow\beta$" のみたい; $ev_\beta(f(x))=f(\beta)$)

REMARK

The number of extensions $\underset{\text{"<" because we can have repeated roots}}{\le}\deg m_{\alpha,K}$. In particular, "=" holds if all roots of $m_{\alpha,K}$ are distinct ($\because$ extension $\Rightarrow$ need to "grab" a root)

Shun/羊羽海 (@shun4midx)

THEOREM 2 (Uniqueness of a Splitting Field)

Let $\tau: K \xrightarrow{\sim} K'$ be an isomorphism of fields. Let $f(x) \in K[x]$ with a splitting field L over K. Then, τ can be extended to an isomorphism $\sigma: L \xrightarrow{\sim} L'$ and $\tilde{\tau}(f(x)) \in K'[x]$ with a splitting field L' over K'.

<u>Proof</u>

By induction on $n = \deg f$,

- $n=1$: $L=K$ and $L'=K'$, so set $\sigma = \tau$
- $n>1$: Assume $f(\alpha)=0$. Since $m_{\alpha,K} \mid f \Rightarrow \tilde{\tau}(m_{\alpha,K}) \mid \tilde{\tau}(f)$, $\exists \beta \in L'$, s.t. $\tilde{\tau}(m_{\alpha,K})(\beta)=0$ and $\tilde{\tau}(m_{\alpha,K}) = m_{\beta,K'}$

  By lemma, $\exists \tau_1 : K(\alpha) \xrightarrow{\sim} K'(\beta)$ which extends τ

  On one hand, we can write $f(x) = (x-\alpha) f_1(x)$, $f_1(x) \in K(\alpha)[x]$. Note, L is a splitting field for f_1 over $K(\alpha)$.

  On the other hand, $\tilde{\tau}(f(x)) = \tilde{\tau}_1(f(x)) = (x - \tau_1(\alpha))(\tilde{\tau}_1(f_1(x))) = (x-\beta)\tilde{\tau}_1(f_1(x)) \Rightarrow L$ is a splitting field for $\tilde{\tau}_1(f_1)$ over $K'(\beta)$

  $\therefore$ By induction hypothesis, τ_1 is extended to an isom $\sigma: L \xrightarrow{\sim} L'$ which is also an extension of τ $\square$

REMARK

The number of such extensions of τ is $\le [L:K]$

$$\left.\begin{array}{l} \#\text{ of } \tau_1 \le \deg m_{\alpha,K} = [K(\alpha):K] \\ \text{By induction hypothesis, } \#\text{ of } \sigma \text{ over } \tau_1 \le [L:K(\alpha)] \end{array}\right\} \therefore \text{Total} \le [L:K(\alpha)][K(\alpha):K] = [L:K]$$

THEOREM 3

If L/K_1 is algebraic and $0 \ne \tau: K_1 \to K_2$ with K_2 algebraically closed, then τ can be extended to $\sigma: L \to K_2$

<u>Proof</u>

Set $S = \{(M,\theta) \mid M \text{ is a field s.t. } K_1 \subseteq M \subseteq L,\ \theta: M \to K_2 \text{ is an extension of } \tau\}$

Since $(K_1, \tau) \in S$, thus $S \ne \emptyset$

Define partial order "$(M_1, \theta_1) \le (M_2, \theta_2)$ iff $M_1 \subseteq M_2$ and $\theta_2|_{M_1} = \theta_1$"

Given a chain $\{(M_i, \theta_i) \mid i \in \Lambda\}$ in S, consider $N = \bigcup_{i \in \Lambda} M_i$, which is a field, and

$$\begin{aligned} \phi: N &\longrightarrow K_2 \\ M_i \ni \alpha &\longmapsto \theta_i(\alpha) \end{aligned}$$

Then, (N, ϕ) is a least upper bound for this chain.

$\therefore$ By Zorn's Lemma, $\exists$ a max element $(M, \sigma) \in S$.

Claim: $M = L$

<u>Proof</u>

Suppose $M \subsetneq L$. Pick $\alpha \in L \setminus M$. Since K_2 is algebraically closed, $\exists \beta \in K_2$, s.t. $\tilde{\sigma}(m_{\alpha,M})(\beta) = 0$

Hence, $\exists \sigma_1 : M(\alpha) \longrightarrow K_2$ with $\sigma_1|_M = \sigma$. Thus, $(M(\alpha), \sigma_1) \gneq (M, \sigma)$ $\rightarrow\!\!\times$

$$\alpha \longmapsto \beta$$

COROLLARY

Any two algebraic closures L_1, L_2 of K are isomorphic

<u>Proof</u>

Consider the inclusion homo $\tau: K \longrightarrow L_2$

$\because L_1/K$ is alg and L_2 is alg closed

$\therefore \exists\, 0 \ne \sigma: L_1 \hookrightarrow L_2$, s.t. $\sigma|_K = id_K$

Note that $\sigma(L_1)$ is alg closed since $L_1 \cong \sigma(L_1)$. Now, $\forall \beta \in L_2$, β is alg over $K \subseteq \sigma(L_1) \Rightarrow \beta \in \sigma(L_1)$, i.e. $L_2 = \sigma(L_1)$ $\square$

EXAMPLE

$f(x) = x^p - 2$, p: prime (it is irred due to Eisenstein)

- $m_{\sqrt[p]{2},\mathbb{Q}} = f(x)$ since $f(x)$ is irred and monic
- Roots: $\sqrt[p]{2}, \sqrt[p]{2}\zeta_p, \sqrt[p]{2}\zeta_p^2, \dots, \sqrt[p]{2}\zeta_p^{p-1} \Rightarrow L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}(\sqrt[p]{2})\mathbb{Q}(\zeta_p)$

(はい，associated poly は x^p-1 けど，$x^p - 1 = (x-1)\underline{(x^{p-1}+\dots+1)}$) それは irred じゃない　それは irred

We know that $[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}] = p$, $\underline{[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1}$

$\therefore [L:\mathbb{Q}] = p(p-1)$ ($\because p, p-1$ coprime)

Shun/翔海 (@shun4midx)

REMARK

Given L/L_1 and L/L_2, L_1L_2 = smallest subfield of L containing L_1 and L_2

Assume $[L_1:K]=m$ and $[L_2:K]=n$ with $\gcd(m,n)=1$. Then, $[L_1L_2:K]=mn$

<u>Proof</u>

$m=[L_1:K] \mid [L_1L_2:K]$, $n=[L_2:K] \mid [L_1L_2:K] \Rightarrow mn \mid [L_1L_2:K]$ ✓

Now, $L_2=K(\alpha_1,\dots,\alpha_n)$, $L_1L_2=L_1K(\alpha_1,\dots,\alpha_n)=L_1(\alpha_1,\dots,\alpha_n)$ since $m_{\alpha,L_1} \mid m_{\alpha,K}$

$\Rightarrow [L_1L_2:K]=[L_1(\alpha_1,\dots,\alpha_n):L_1][L_1:K]\le mn$

$\therefore$ $[L_1L_2:K]=mn$ $\square$

REMARK (IMPORTANT)

Let L/K be algebraic and $\tau: L \to L$ be a monomorphism fixing K. Then, τ is onto

$\underset{z}{\rotatebox{90}{$\in$}}$

$f(x)=m_{z,K}(x)$, $\deg f=n$, f has roots $z=z_1,\dots,z_n$

Then, $\tau: z_i \longmapsto z_j$, i.e. $\tau: \{z_1,\dots,z_n\}\cap L \xrightarrow{1-1} \{z_1,\dots,z_n\}\cap L$