5-7-25 (WEEK 12)

Shun / 舜海 (@shun4midx)

SOLUTION BY RADICALS

DEFINITION

- Given L/K and $\beta \in L$, β is called a **radical** over K if $\beta^n \in K$ for some $n \in \mathbb{N}$
- L/K is called an **extension by radicals** if $\exists\, L = L_n \supseteq L_{n-1} \supseteq \dots \supseteq L_0 = K$, s.t. $\forall i = 1, \dots, n$, $L_i = L_{i-1}(\beta_i)$ with β_i a radical over L_{i-1}
- $f(x) \in K[x]$ is **solvable by radicals** if $\exists\, L/K$ is an extension by radicals and f splits over L

RECALL

Let G be a finite group, G is **solvable** if $\exists\, \{e\} = G_n \lhd G_{n-1} \lhd \dots \lhd G_0 = G$, s.t. G_{i-1}/G_i is cyclic $\forall i$

MAIN THEOREM

Under some proper assumption on $\operatorname{char} K$, a separable poly $f(x) \in K[x]$ is solvable by radicals $\Leftrightarrow$ the Galois group of $f(x)$ over K is solvable

LEMMA 1

Given $M = L(\beta)$, $\beta^n \in L$, assume that $\operatorname{char} K \nmid n$. Then $\exists\, N$

$$\begin{array}{c} M \\ | \text{ by a radical} \\ L \\ | \text{ Galois} \\ K \end{array} \qquad \begin{array}{c} N \\ | \text{ by radicals} \\ M \\ | \\ L \\ | \\ K \end{array}$$

s.t. N/K is Galois and N contains a primitive root of unity ζ_n

Proof

We know that $M(\zeta_n) = L(\zeta_n, \beta)$ is a splitting field for $x^n - a = x^n - \beta^n$ (separable) over L

If we set $f(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x^n - \sigma(a))$ (separable), then all coef of $f(x)$ are elementary symmetric poly w.r.t. $\{\sigma(a) \mid \sigma \in \mathrm{Gal}(L/K)\}$, which are fixed by $\mathrm{Gal}(L/K)$, so $f(x) \in K(x)$

Assume that L is a splitting field for $g(x)$ over K. Then N is chosen as a splitting field for $f(x)g(x)$ (separable) over K

$\therefore$ By def, N/K is Galois

Note that $N = K(\underbrace{\alpha_1, \dots, \alpha_s}_{\text{roots of } g(x)}, \beta, \{\beta\sigma, \sigma \in \mathrm{Gal}(L/K) \setminus \{\mathrm{id}\}\}, \zeta_n)$

L — M — $\beta\sigma = \sigma(a)$

$\therefore$ N/M is an extension by radicals $\square$

LEMMA 2

Let $L = L_m \supseteq L_{m-1} \supseteq \dots \supseteq L_0 = K$ s.t. $L_i = L_{i-1}(\beta_i)$ with $\beta_i^{n_i} = a_i \in L_{i-1}$

If $\operatorname{char} K \nmid n_1 n_2 \cdots n_m$, then $\exists\, N/L$, s.t. N/K is a Galois extension by radicals and $\zeta_{n_i} \in N$ $\forall i = 1, \dots, m$

Proof

By induction on m,

- $m = 1$: $L = K(\beta_1)$ with $\beta_1^{n_1} = a_1 \in K$. Set $N = L(\zeta_n) = K(\zeta_n, \beta_1)$ which is a splitting field for $x^{n_1} - a_1$ over K
- $m > 1$: By induction hypothesis, $\exists\, N'/L_{m-1}$, s.t. N'/K is a Galois extension by radicals and N' contains ζ_{n_i} $\forall i = 1, \dots, m-1$

Sketch:

$L = L_{m-1}(\beta_m) \supseteq L_{m-1} \supseteq \dots \supseteq K$

$N'(\beta_m) \supseteq N'$ ← ind hyp

↑ By lemma 1

By lemma 1, $\exists\, N/N'(\beta_m)$, which is an extension by radicals s.t. N/K is Galois and N contains ζ_{n_m}. $\square$

Shun/翔海 (@shun4midx)

THEOREM A

Let $L=L_m \supseteq L_{m-1} \supseteq \dots \supseteq L_0 = K$ s.t. $L_i = L_{i-1}(\beta_i)$, $\beta_i^{n_i} = a_i \in L_{i-1}$ and $\mathrm{char} K \nmid n_1 \cdots n_m$.
If a separable poly $f \in K[x]$ splits over L, then the Galois group of f over K is solvable

REMARK

$H \lhd G$, G is solvable $\Leftrightarrow$ $H, G/H$ are solvable

Proof

"$\Leftarrow$": OK

"$\Rightarrow$": Assume $G = G_0 \rhd \cdots \rhd G_n = \{e\}$.

For H, $\dfrac{G_{i-1}\cap H}{G_i \cap H} = \dfrac{G_{i-1}\cap H}{(G_{i-1}\cap H)\cap G_i} \cong \dfrac{(G_{i-1}\cap H)G_i}{G_i} \hookrightarrow G_{i-1}/G_i$

For G/H, $G/H \rhd G_1H/H \rhd \cdots \Rightarrow \dfrac{G_{i-1}H/H}{G_iH/H} \cong G_{i-1}H/G_iH \ni xnG_iH = (\underbrace{xnx^{-1}}_{\in H})(\underbrace{a_ib_i}_{\in H}) = a^s a^{-s}(xnx^{-1})a^s b_i H = a^s G_i H \Rightarrow \dfrac{G_{i-1}H}{G_iH} \le \langle aG_iH \rangle$

PROOF OF THEOREM A

By lemma 2, we can assume that L/K is Galois ($\lceil L/L_i$ is Galois)

If we set $n = \mathrm{lcm}(n_1, \dots, n_m)$, then
- "containing ζ_n" $\Leftrightarrow$ "containing ζ_{n_i} $\forall i = 1, \dots, m$"
- $\zeta_n \in L$

Consider $L = L(\zeta) \supseteq L_{m-1}(\zeta) \supseteq \cdots \supseteq L_0(\zeta)$ (Galois)
(L, L_m'; L_{m-1}'; L_0')

We have L/L_i' is Galois and let $G_i = \mathrm{Gal}(L/L_i')$. We may also find:
- $G_m = \{e\}$, $G_0 = \mathrm{Gal}(L/L_0')$
- $G_{i-1}/G_i = \dfrac{\mathrm{Gal}(L/L_{i-1}')}{\mathrm{Gal}(L/L_i')} \cong \mathrm{Gal}(L_i'/L_{i-1}')$ is cyclic.

$\therefore$ G_0 is solvable

Moreover, $L \supseteq L_0 \supseteq K$, $K(\zeta)$ is a splitting field for $x^n - 1$ over K and $\mathrm{Gal}(K(\zeta)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow \mathrm{Gal}(K(\zeta)/K)$ is solvable
As $\mathrm{Gal}(K(\zeta)/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_0)$, thus $\mathrm{Gal}(L/K)$ is solvable

Let N be a splitting field for $f(x)$ over K. Then, $L \supseteq N$ and $\mathrm{Gal}(N/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/N)$ is solvable $\square$

THEOREM B

Let f be separable in $K[x]$ and L be a splitting field for f over K. Assume $\mathrm{char} K \nmid |\mathrm{Gal}(L/K)|$
If $\mathrm{Gal}(L/K)$ is solvable, then f is solvable by radicals

Proof

Let $n = |\mathrm{Gal}(L/K)|$ and $\zeta := \zeta_n$.
Let N be a splitting field for f over $K(\zeta)$, i.e. $N = LK(\zeta)$

Since $\mathrm{Gal}(LK(\zeta)/K(\zeta)) \cong \mathrm{Gal}(L/K(\zeta)\cap L) \le \mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/K)$ is solvable $\Rightarrow \mathrm{Gal}(LK(\zeta)/K(\zeta))$ is solvable
Say $\{e\} = G_n \lhd \cdots \lhd G_0 = \mathrm{Gal}(N/K(\zeta))$, G_i/G_{i-1} is cyclic

If we set $N_j := \mathrm{Inv}\, G_j \le N$, then $N = N_m \supseteq \cdots \supseteq N_0 = K(\zeta)$ and $G_j = \mathrm{Gal}(N/N_j)$
Also, $G_{i-1}/G_i = \mathrm{Gal}(N/N_{i-1})/\mathrm{Gal}(N/N_i) \cong \mathrm{Gal}(N_i/N_{i-1})$ is cyclic

Note, $n_i = [N_i : N_{i-1}] = |G_{i-1}/G_i| \mid |G_0| \mid n \Rightarrow \zeta_{n_i} \in N_{i-1}/N_i$
Also, $\mathrm{char} K \nmid n_i$, so $N_i = N_{i-1}(\beta_i)$ with $\beta_i^{n_i} \in N_{i-1}$
$\therefore$ $N/K(\zeta)$ is an extension by radicals and thus N/K is too. $\square$

Shun / 翔海 (@shun4midx)

REMARK

In thm A, $Gal(K(\zeta)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

In fact, $\hookrightarrow$ may not be "$=$".

For example, $n=5 \Rightarrow x^5-1$, $[K(\zeta_5):K]=4=\varphi(5)$ assume $\mathrm{char}K \neq 5$

$\Updownarrow$

$x^4+x^3+x^2+x+1$ irr in $K(x)$

$K=\mathbb{Z}/11\mathbb{Z}$, $x^4+x^3+x^2+x+1$ is divisible by $x-3$, in fact, it is $(x-3)(x-5)(x-4)(x-9) \Rightarrow \not\Rightarrow$ ($\because$ deg $=1 \neq \varphi(5)$)

$K=\mathbb{Z}/19\mathbb{Z}$, $x^4+x^3+x^2+x+1=(x^2+5x+1)(x^2-4x+1) \Rightarrow \not\Rightarrow$ ($\because$ deg $=2 \neq \varphi(5)$)