5-2-25 (WEEK 11) Shun/翔海 (@shun4midx)

ABELIAN EXTENSIONS

LEMMA

If L/K is finite, then L/K is simple $\Leftrightarrow \exists$ finitely many fields M s.t. $L \supseteq M \supseteq K$

Proof

"$\Rightarrow$": Suppose $L = K(\alpha)$ and $L \supseteq M \supseteq K$

Let $m_{\alpha,M} = x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_i \in M$

We find that $M = K(a_0, \dots, a_{n-1})$

Since $[K(\alpha) : K(a_0, \dots, a_{n-1})] = \deg m_{\alpha,M} = [M(\alpha):M] = [K(\alpha):M]$, thus $M = K(a_0, \dots, a_{n-1})$.

And $m_{\alpha,M} \mid m_{\alpha,K} \Rightarrow$ There are finitely many monic divisors of $m_{\alpha,K} \Rightarrow \exists$ finitely many fields M s.t. $L \supseteq M \supseteq K$

"$\Leftarrow$": Case 1: $|K| < \infty$

In this case, $|L| < \infty$. We know that $(L \setminus \{0\}, \dots, \cdot)$ is a cyclic group, say $L \setminus \{0\} = \langle x \rangle$

Then, $L \setminus \{0\} = \langle x \rangle \subseteq K(\alpha) \setminus \{0\}$, so $L \setminus \{0\} = K(\alpha) \setminus \{0\} \Rightarrow L = K(\alpha)$ ✓

Case 2: $|K| = \infty$

Let $L = K(\alpha_1, \dots, \alpha_n)$ and $M = K(\alpha_1, \alpha_2)$

For $\beta \in K$, set $F_\beta : K(\alpha_1 + \beta\alpha_2)$ and thus $K \subseteq F_\beta \subseteq L$

Since $|K| = \infty$, by contradiction, $\exists \beta \neq r$ in K, s.t. $F_\beta = K(\alpha_1 + \beta\alpha_2) = K(\alpha_1 + r\alpha_2) F_\alpha$, i.e. $\alpha_1 + \beta\alpha_2 - (\alpha_1 + r\alpha_2) \in F_\beta$

By induction, $L = f(\alpha)$ and hence $M = F_\beta$ □

THEOREM (PRIMITIVE ROOT THEOREM)

If L/K is finite and separable, then L/K is simple

Proof

Let $L = K(\alpha_1, \dots, \alpha_n)$ and $f(x) := m_{\alpha_1,K} m_{\alpha_2,K} \cdots m_{\alpha_n,K}$ be separable over K

Take N to be a splitting field for f over K. Since $|Gal(N/K)| = [N:K] < \infty$, $\exists$ finitely many subgroups of $|Gal(N/K)|$

$\therefore \exists$ finitely many intermediate fields between N and K

$\therefore \exists$ finitely many intermediate fields between L and K. □

COROLLARY

If L/K is Galois, then $\exists$ irr f in $K[x]$, s.t. L is the splitting field for f over K

Proof

Finite, separable $\Rightarrow L = K(\alpha)$, $f = m_{\alpha,K}$ ($\because L/K$ is normal) □

DEFINITION

L/K is called a cyclic (abelian) extension if L/K is Galois and $Gal(L/K)$ is cyclic (abelian)

PROPOSITION 1

Let $\sigma_1, \dots, \sigma_n$ be distinct in $Aut(K)$ and $k_1, \dots, k_n \in K^*$. Then, $\exists c \in K$, s.t. $(k_1\sigma_1 + \dots + k_n\sigma_n)(c) \neq 0$

Proof

We want to show "$\sigma_1, \dots, \sigma_n$ are lin indep over K"

Assume it is not true.

Then, $\exists$ a minimal nonempty subset $\{\sigma_{i_1}, \dots, \sigma_{i_m}\}$ which is lin indep over K, say $b_1\sigma_{i_1}(k) + \dots + b_m\sigma_{i_m}(k) = 0 \; \forall k \in K$

If $m = 1$, then $b_1 \neq 0$, $b_1\sigma_{i_1}(k) = 0 \; \forall k \in K \Rightarrow \sigma_{i_1}(k) = 0 \; \forall k \in K \Rightarrow \sigma_{i_1} = 0$ $\times$

So $m > 1$, choose $0 \neq h \in K$, s.t. $\sigma_{i_1}(h) \neq \sigma_{i_m}(h) \neq 0$

$\therefore$ We have $b_1\sigma_{i_1}(hk) + \dots + b_m\sigma_{i_m}(hk) = 0$ and $b_1\sigma_{i_1}(h)\sigma_{i_1}(k) + \dots + b_m\sigma_{i_m}(h)\sigma_{i_m}(k) = 0 \; \forall k \in K$.

Subtract the two, we get $b_1(\underbrace{\sigma_{i_m}(h) - \sigma_{i_1}(h)}_{\neq 0})\sigma_{i_1}(k) + \dots + b_{m-1}(\sigma_{i_m}(h) - \sigma_{i_1}(h))\sigma_{i_{m-1}}(k) = 0$ $\times$

Shun/翔海(@shun4midx)

PROPOSITION 2

Assume that char $K \nmid n$. Let L be the splitting field for separable x^n-a over K and ζ be a primitive n^{th} root of unity. Then, $Gal(L/K(\zeta))$ is cyclic of order dividing n. Moreover, $\underbrace{x^n-a \text{ is irr over } K(\zeta)}_{m_{\alpha,K(\zeta)}=x^n-a} \Leftrightarrow [L:K(\zeta)]=n$, i.e. $|Gal(L/K(\zeta))|=n$

Proof

Let α be a root of x^n-a. Then $\alpha, \alpha\zeta, \dots, \alpha\zeta^{n-1}$ are all roots of x^n-a. Thus, $L=K(\alpha,\zeta)=K(\zeta)(\alpha)$

Consider $\phi: Gal(L/K(\zeta)) \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$(\sigma: \alpha \mapsto \alpha\zeta^{j_\sigma}) \longmapsto \overline{j_\sigma}$$

- ϕ is a homo: $(\tau\circ\sigma)(\alpha)=\tau(\alpha\zeta^{j_\sigma})=\tau(\alpha)\tau(\zeta^{j_\sigma})=\alpha\zeta^{j_\tau}\zeta^{j_\sigma}=\alpha\zeta^{j_\tau+j_\sigma} \rightsquigarrow \overline{j_\tau}+\overline{j_\sigma}$
- ϕ is 1-1: $\sigma\in\ker\phi \Leftrightarrow \overline{j_\sigma}=\overline{0} \Leftrightarrow \sigma(\alpha)=\alpha \Leftrightarrow \sigma=Id$

THEOREM 1

Assume that char $K\nmid n$

If L/K is a cyclic extension of degree n with $\zeta\in K$, then L is a splitting field for some irr poly x^n-a over K

Proof

Let $Gal(L/K)=\langle\sigma\rangle$ with $ord(\sigma)=n$

By prop 1, $\exists\, c\in L$, s.t. $\alpha=c+\zeta\sigma(c)+\zeta^2\sigma^2(c)+\dots+\zeta^{n-1}\sigma^{n-1}(c)\neq 0$

$\therefore \sigma(\alpha)=\sigma(c)+\zeta\sigma^2(c)+\zeta^2\sigma^3(c)+\dots+\zeta^{n-1}c=\zeta^{-1}\alpha \Rightarrow \alpha\notin K$

But $\sigma(\alpha^n)=\zeta^{-n}\alpha^n=1(\alpha^n)=\alpha^n\in K$

$\therefore K(\alpha)=K(\zeta,\alpha)\subseteq L$ is a splitting field for x^n-a over K.

Also, $\sigma: K(\alpha)\longrightarrow K(\alpha)$ $\Rightarrow \langle\sigma|_{K(\alpha)}\rangle \leq Gal(K(\alpha)/K)$

$\qquad\alpha \longmapsto \zeta^{-1}\alpha$

Hence, $n=[L:K]\geq[K(\alpha)-K]=|Gal(K(\alpha)/K)|\geq n \Rightarrow [L:K]=[K(\alpha):K] \Rightarrow L=K(\alpha)$, $[L:K]=n \Rightarrow x^n-a$ is irr. □

DEFINITION

Say char $K\nmid n$ and ζ is a primitive n^{th} root of unity

- L/K is a Kummer extension of exponent n if $\zeta\in K$ and L is a splitting field for $(x^n-a_1)(x^n-a_2)\cdots(x^n-a_k)$ over K, $a_i\in K$
- Recall: $e(G)$ is the least positive integer m, s.t. $g^m=e$ $\forall g\in G$

THEOREM 2

If L/K is Galois s.t. $Gal(L/K)$ is abelian of exponent n and $\zeta\in K$, then L/K is a Kummer extension of exponent n

Proof

By induction on $[L:K]$, $[L:K]=1$, $n=1\Rightarrow$ ok. Assume that $[L:K]>1$, by FTOFAG, $Gal(L/K)\cong \underbrace{\mathbb{Z}/d_1\mathbb{Z}\times\dots}_{H}\times\underbrace{\mathbb{Z}/d_s\mathbb{Z}}_{N= \text{ cyclic group of order } N}$ with $d_i|d_{i+1}, i=1,\dots,s-1$

$\Rightarrow n=d_s$, $e(H)=e=d_{s-1}|n$

If $s=1$, then, by thm 1, it is done. Assume $s>1$.

Set $M=Inv\, N$, $[M:K]<[L:K]$ and $Gal(M/K)\cong Gal(L/K)/\underbrace{Gal(L/M)}_{=N}\cong H$

Also, $(\zeta^{\frac{n}{e}})^e=\zeta^n=1 \Rightarrow \zeta^{\frac{n}{e}}\in K$ is a primitive eth root of unity

$\therefore$ By induction hypothesis, M is a splitting field for $(x^e-b_1)\cdots(x^e-b_{k-1})$ over K, $b_j\in K$

Note: if we set $a_i:=b_i^{\frac{n}{e}}\in K$, then M is also a splitting field for $(x^n-a_1)\cdots(x^n-a_{k-1})$ over K

Let $N=\langle\sigma\rangle$, then $Gal(L/K)=\{\sigma^i\tau \mid 0\leq i\leq n-1, \tau\in H\}$

By prop 1, $\exists c$, s.t. $\alpha=\sum_{\tau\in H}\tau(c)+\zeta\sum_{\tau\in H}\sigma\tau(c)+\dots+\zeta^{n-1}\sum_{\tau\in H}\sigma^{n-1}\tau(c)\neq 0$

$\therefore \sigma(\alpha)=\zeta^{-1}\alpha$, $\tau(\alpha)=\alpha$ $\forall\tau\in H$, $\sigma(\alpha^n)=\alpha^n \Rightarrow \alpha\notin M$, $a_k:=\alpha^n\in M$, so $M(\alpha)$ is a splitting field for x^k-a over M

Also, $n=[L:M]\geq[M(\alpha):M]=|Gal(M(\alpha)/M)|\geq n \Rightarrow L=M(\alpha)$ □

REMARK

$L \rightsquigarrow (x^n-\overset{\rightsquigarrow \alpha_1}{a_1})\cdots(x^n-\overset{\rightsquigarrow \alpha_k}{a_k}) \Rightarrow \forall\sigma\in Gal(L/K)$, $\sigma(\alpha_i)=\alpha_i\zeta^{j_{\sigma,i}}$, $0\leq j_{\sigma,i}\leq n-1 \Rightarrow \sigma^n(\alpha_i)=\alpha_i\zeta^{nj_{\sigma,i}}=\alpha_i$ $\forall i \Rightarrow \sigma^n=id$

$\forall\tau\in Gal(L/K)$, $\tau\sigma(\alpha_i)=\tau(\alpha_i\zeta^{j_{\sigma,i}})=\alpha_i\zeta^{j_{\tau,i}}\zeta^{j_{\sigma,i}}=\sigma\tau(\alpha_i)$ $\forall i \Rightarrow \sigma\tau=\tau\sigma$