5-14-25 (WEEK 13)

Shun/翔海 (@shun4midx)

HILBERT THEOREM 90

- Trace and norm: Let $L=K(\alpha)$, $f(x)=m_{\alpha,K}=x^n+a_{n-1}x^{n-1}+\dots+a_0$

↳ f is separable and $\exists$ exactly n monomorphisms $\sigma_i: L \xrightarrow{} \bar{K}$ fixing K and $\{\sigma_1(\alpha),\dots,\sigma_n(\alpha)\}$ consists of all roots of $f(x)$

$\Rightarrow x^n+a_{n-1}x^{n-1}+\dots+a_0=(x-\sigma_1(\alpha))\cdots(x-\sigma_n(\alpha))$

Norm: $(-1)^n a_0=\sigma_1(\alpha)\cdots\sigma_n(\alpha)$

Trace: $-a_{n-1}=\sigma_1(\alpha)+\dots+\sigma_n(\alpha)$

Moreover, we can take the K-linear transformation $T_\alpha: K(\alpha)\longrightarrow K(\alpha)$, $v\longmapsto \alpha v$

Then,

$$[T_\alpha]_{\{1,\dots,\alpha^{n-1}\}}=\begin{pmatrix} & & & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ & & 1 & -a_{n-1}\end{pmatrix} \Rightarrow \begin{cases}\text{Trace}=-a_{n-1}\\ \text{Norm}=(-1)^n a_0\end{cases}$$

Here, we call $\sigma_1(\alpha)+\dots+\sigma_n(\alpha)=Tr_{L/K}(\alpha)$ (trace of α) and $\sigma_1(\alpha)\cdots\sigma_n(\alpha)=N_{L/K}(\alpha)$ (norm of α)

↳ f is inseparable, char $K=p>0$, $f(x)=\underset{\text{irr}}{f_1}(x^p)$, $f_1(x)=\underset{\text{irr}}{f_2}(x^p)\Rightarrow f(x)=f_2(x^{p^2}),\dots, f(x)=f_{sep}(x^{p^k})$, $\deg f_{sep}=m$

If $f_{sep}(x)=(x-\beta_1)\cdots(x-\beta_m)$, then $f(x)=(x^{p^k}-\beta_1)\cdots(x^{p^k}-\beta_m)$ and $\beta_i=\alpha_i^{p^k}$

$\therefore f(x)=[(x-\alpha_1)\cdots(x-\alpha_m)]^{p^k}$

Note that $\beta=\alpha^{p^k}$ is separable over K with $[K(\alpha^{p^k}):K]=m$ and α is purely inseparable over $K(\alpha^{p^k})$

$\Rightarrow K(\alpha^{p^k})\subseteq L_{sep}$ and $L=K(\alpha)/K(\alpha^{p^k})$ is purely inseparable

DEFINITION

- α is purely inseparable over K if $\exists n\geq 0$, s.t. $\alpha^{p^n}\in K$ (separable is a type of purely inseparable)
- L/K is purely inseparable if $\forall \alpha\in L$, α is purely inseparable

FACT

- α purely insep $\Rightarrow K(\alpha)/K$ purely insep

$(k_1\alpha_1^{r_1}+k_2\alpha_2^{r_2})^{p^n}=k_1^{p^n}(\underset{K}{\alpha_1^{p^n}})^{r_1}+k_2^{p^n}(\underset{K}{\alpha_2^{p^n}})\in K$

- β: sep + purely insep $\Rightarrow \beta\in K$

$\underset{a}{\beta^{p^n}}\in K\Rightarrow m_{\beta,K}=(x-\beta)^{\ell}\mid x^{p^n}-\underset{K}{a}=(x-\beta)^{p^n}$

But β is sep $\Rightarrow \ell=1$, i.e. $\beta\in K$.

Now, $L=K(\alpha)\longleftrightarrow L_{sep}$. By fact, $L_{sep}=K(\alpha^{p^k})$, $m=\deg f_{sep}=[L:K]_{sep}$, $p^k=[L:K]_i$

$$\begin{tikzcd} L=K(\alpha) \arrow[rr, leftrightarrow] & & L_{sep} \\ & K(\alpha^{p^k}) \arrow[ul, "\text{purely insep}"] \arrow[ur] & \\ & K \arrow[u] \arrow[uur] & \end{tikzcd}$$

$$\begin{tikzcd} L=K(\alpha) & \\ & L_{sep} \arrow[ul, "\text{purely insep} \sim p^k"'] \\ K \arrow[uu] \arrow[ur, "m"'] & \end{tikzcd}$$

Also, $\exists$ exactly n monomorphisms $\sigma_i: L\longrightarrow \bar{K}$ fixing K and $f(x)=[(x-\sigma_1(\alpha))\cdots(x-\sigma_m(\alpha))]^{p^k}$

Thus, $N_{L/K}(\alpha)=(\prod_{i=1}^{m}\sigma_i(\alpha))^{p^k=[L:K]_i}$

$Tr_{L/K}(\alpha)=[L:K]_i(\sum_{i=1}^{m}\sigma_i(\alpha))$

Moral of the story: We don't always need "separable"

HILBERT THEOREM 90

Shun/翔海 (@shun4midx)

If L/K is a cyclic extension of deg n with $G = \langle \sigma \rangle$, then $\alpha \in L \setminus \{0\}$. $N_{L/K}(\alpha) = 1 \Leftrightarrow \exists \beta \in L \setminus \{0\}$, s.t. $\alpha = \frac{\sigma(\beta)}{\beta}$

$\Downarrow$

$H^1(Gal(L/K) = G, L^\times) = \{1\}$

Proof

"$\Leftarrow$": $N_{L/K}(\alpha) = \prod_{i=0}^{n-1} \frac{\sigma^{i+1}(\beta)}{\sigma^i(\beta)} = 1$

"$\Rightarrow$": We know $\exists c \in L$, s.t. $\beta^{-1} = id(c) + \alpha\sigma(c) + \{\alpha\sigma(\alpha)\}\sigma^2(c) + \dots + \{\alpha\sigma(\alpha) \cdots \sigma^{n-2}(\alpha)\}\sigma^{n-1}(c) \neq 0$

$\therefore \alpha\sigma\beta^{-1} = \beta^{-1} \Rightarrow \alpha = \frac{\beta^{-1}}{\sigma(\beta^{-1})} = \frac{\sigma(\beta)}{\beta}$. □

"$H^1(Gal(L/K) = G, L^\times) = \{1\}$"

Derivation / Image

$H^1(Gal(L/K), L^\times) = \frac{Z^1(G, L^\times)}{B^1(G, L^\times)} = \frac{\{\phi : G \to L^\times \mid \forall \sigma, \tau \in G,\ \phi(\sigma\tau) = \phi(\sigma)\sigma(\phi(\tau))\}}{\{\phi : G \to L^\times \mid \exists b \in L^\times, \text{ s.t. } \phi(\sigma) = \frac{b}{\sigma(b)}\ \forall \sigma \in G\}}$

Now, $G = \langle \sigma \rangle$, $\phi \in Z^1$, $\phi(\sigma) = a$, $\phi(\sigma^2) = a\sigma(a)$, $\phi(\sigma^3) = a\sigma(a)\sigma^2(a) \dots$

$\therefore 1 = \phi(1) = \phi(a^n) = a\sigma(a) \cdots \sigma^{n-1}(a) = N(a)$

$\therefore \exists b \in L$, s.t. $a \in \frac{b}{\sigma(b)}$, i.e. ϕ ✓

STATEMENT 2 OF HILBERT THEOREM

(II) $\alpha \in L$, $Tr_{L/K}\alpha = 0 \Leftrightarrow \exists \beta \in L$, s.t. $\alpha = \sigma(\beta) - \beta$

Proof

"$\Leftarrow$": $Tr_{L/K}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\sigma(\beta) - \beta) = 0$

"$\Leftarrow$": $\exists c \in L$, s.t. $\beta_1 := c + \sigma(c) + \dots + \sigma^{n-1}(c) \neq 0 \Rightarrow \sigma(\beta_1) = \beta_1$

Let $\beta_2 := \alpha\sigma(c) + \{\alpha + \sigma(\alpha)\}\sigma^2(c) + \dots + \{\underbrace{\alpha + \sigma(\alpha) + \dots + \sigma^{n-2}(\alpha)}_{-\alpha}\}\underbrace{\sigma^n(c)}_{c}$

Then, $\beta_2 - \sigma(\beta_2) = \alpha\beta_1 \Rightarrow \alpha = \frac{\beta_2}{\beta_1} - \sigma\left(\frac{\beta_2}{\beta_1}\right)$ □

COROLLARY

If $[L:K] = n$ with char $K \nmid n$ and $\zeta_n \in K$, then "L/K is cyclic $\Rightarrow L = K(\alpha)$, α is a root of $x^n - \overset{K}{a^n}$"

Proof

Let $Gal(L/K) = \langle \sigma \rangle$. Since $N_{L/K}(\zeta_n) = \zeta_n\sigma(\zeta_n) \cdots \sigma^{n-1}(\zeta_n) = \zeta_n \cdots \zeta_n = \zeta_n^n = 1$, thus $\zeta_n = \frac{\sigma(\alpha)}{\alpha}$ for some α.

↳ Here, $\zeta_n = \frac{\sigma(\alpha)}{\alpha} \Rightarrow \sigma(\alpha) = \zeta_n\alpha \Rightarrow \sigma(\alpha^n) = \alpha^n \Rightarrow \alpha^n \in K$

Note that $\alpha, \zeta_n\alpha, \dots, \zeta_n^{n-1}\alpha$ are n roots of $x^n - a = x^n - \alpha^n$

$\because m_{\alpha,K}(\zeta_n^i\alpha) = m_{\alpha,K}(\sigma^i(\alpha)) = \sigma^i(m_{\alpha,K}(\alpha)) = \sigma^i(0) = 0$

$\therefore$ We can conclude that $(x^n - a) \mid m_{\alpha,K} \Rightarrow m_{\alpha,K} = x^n - a \Rightarrow [K(\alpha):K] = n \Rightarrow L = K(\alpha)$ □

PROPOSITION

Let char $K = p$ and $[L:K] = p$. Then, L/K is cyclic $\Leftrightarrow L = K(\alpha)$ where α is a root of $x^n - x - a = 0$

Proof

"$\Leftarrow$": All roots of $x^n - x - a$ are $\alpha, \alpha+1, \dots, \alpha+p-1$

Let $\sigma : \alpha \mapsto \alpha + 1 \Rightarrow \sigma^i : \alpha \mapsto \alpha + i$. Hence, $Gal(L/K) = \langle \sigma \rangle$

"$\Rightarrow$": $\because Tr_{L/K}(1) = p = 0$

$\therefore \exists \alpha \in L$, s.t. $1 = \sigma(\alpha) - \alpha \Rightarrow \sigma(\alpha) = \alpha + 1$

On one hand, $\sigma^i(\alpha) = \alpha + i \Rightarrow \alpha, \alpha+1, \dots, \alpha+p-1$ are roots of $m_{\alpha,K}$.

On the other hand, $\alpha, \alpha+1, \dots, \alpha+p-1$ are all roots of $x^p - x - a$, $a = \alpha^p - \alpha$

Similarly, $x^p - x - a \mid m_{\alpha,K} \Rightarrow m_{\alpha,K} = x^p - x - a \Rightarrow [K(\alpha):K] = p \Rightarrow L = K(\alpha)$. □

GALOIS GROUP EXAMPLE

If $|G| = pq$, p, q are distinct primes: WLOG assume $p > q$. By Sylow thm, $n_p = 1 + p \mid q \Rightarrow n_p = 1 \Rightarrow \exists H \in Syl_p(G)$ s.t. $H \trianglelefteq G \Rightarrow |H| = p \Rightarrow H$ is solvable

As $|G/H| = q$, thus G/H is also solvable. $\therefore G$ is solvable.

Shun/翔海(@shun4midx)

Case: $|G|=pqr$, primes $p>q>r$.
Assume none of $n_p, n_q, n_r=1$.
Then, $n_p=1+kp \mid qr \Rightarrow n_p=qr$
$n_q=1+kq \mid pr \Rightarrow n_q \geq p$
$n_r=1+kr \mid pq \Rightarrow n_r \geq q$
$\therefore \exists\, n_p=1$ or $n_q=1$ or $n_r=1$
Then by similar logic as "$|G|=pq$", thus G is solvable

Case: $|G|=p^2q$
If $p>q$, we know similarly $n_p=1$, so $|H|=p^2 \Rightarrow H$ is abelian $\Rightarrow H$ is solvable (solvable if normal or abelian)
If $p<q$, then assume $n_p \neq 1$ and $n_q \neq 1$.
Thus, $n_p=q$, $n_q=p^2 \Rightarrow p^2=1+kq \Rightarrow q \mid p^2-1=(p-1)(p+1) \Rightarrow q=p+1 \Rightarrow p=2, q=3 \Rightarrow |G|=12$. However $|G|=12$ has a normal subgroup $\divideontimes$