4-30-25 (WEEK 11)

Shun/翔海 (@shun4midx)

FUNDAMENTAL THEOREM

MAIN THEOREM

Let L/K be a Galois extension (finite, separable, normal) and $G=Gal(L/K)$. Then, $\{M \mid M \text{ is a field with } K\subseteq M\subseteq L\} \longleftrightarrow \{H : H\leq G\}$

$$M \longmapsto Gal(L/M)$$
$$K\subseteq Inv\,H \longleftarrow H$$

s.t. (1) $H \longmapsto Inv\,H \longmapsto Gal(L/Inv\,H)=H$ by Artin theorem

$M \longmapsto Gal(L/M) \longmapsto Inv\,Gal(L/M)=M$ by corollary of Artin theorem

(2) If $M_1 = Inv\,H_1$, $M_2=Inv\,H_2$, then $M_1\subseteq M_2 \Leftrightarrow H_1 \supseteq H_2$

(3) If $M=Inv\,H$, then $H\trianglelefteq G \Leftrightarrow M/K$ is normal

Proof

Recall: M/K is normal $\Leftrightarrow \forall \sigma\in G,\ \sigma(M)=M \Leftrightarrow \forall\sigma\in G,\ Gal(L/\sigma(M)) = Gal(L/M)$ ("$\Leftarrow$": Just take Inv on both sides)

and $\tau\in Gal(L/\sigma(M)) \Leftrightarrow \tau(\sigma(x))=\sigma(x)\ \forall x\in M \Leftrightarrow \sigma^{-1}\tau\sigma(x)=x\ \forall x\in M \Leftrightarrow \sigma^{-1}\tau\sigma\in Gal(L/M) \Leftrightarrow \sigma Gal(L/M)\sigma^{-1}$ $\therefore Gal(L/\sigma(M)) = \sigma Gal(L/M)\sigma^{-1}$

So, M/K is normal $\Leftrightarrow Gal(L/M)\trianglelefteq G$ □

(4) If $H\trianglelefteq G$, then $G/H \cong Gal(M/K)$

Proof

Define $\phi: G \longrightarrow Gal(M/K)$

$\sigma \longmapsto \sigma|_M$

- ϕ is surjective: $\forall \tau\in Gal(M/K)$,

$$\begin{tikzcd}
L \arrow[r, "\therefore\exists", "\sim"'] & L \\
M \arrow[u, "\text{splitting field of } f \text{ over } M"] \arrow[r, "\sim", "\tau"'] & M \arrow[u, "\text{splitting field of } f=\tilde{\tau}(f) \text{ over } M"'] \\
& K \arrow[ul] \arrow[u]
\end{tikzcd}$$

- $\sigma\in\ker\phi \Leftrightarrow \sigma|_M = id_M \Leftrightarrow \sigma\in Gal(L/M)=H$

$\therefore$ By 1st isom thm, $G/H \cong Gal(M/K)$ □

(5) If $M_1=Inv\,H_1$, $M_2=Inv\,H_2$, then $M_1\cap M_2 = Inv\langle H_1,H_2\rangle$, $M_1M_2 = Inv\,H_1\cap H_2 \Leftrightarrow H_1\cap H_2 = Gal(L/M_1M_2)$

Proof

- $\alpha\in Inv\langle H_1,H_2\rangle \Leftrightarrow \alpha\in Inv\,H_1\cap Inv\,H_2$
- $\tau\in H_1\cap H_2 \Leftrightarrow \tau$ fixes $M_1=K(\alpha_1,\dots,\alpha_s)$ and τ fixes $M_2=K(\beta_1,\dots,\beta_t) \Leftrightarrow \tau$ fixes $K(\alpha_1,\dots,\alpha_s,\beta_1,\dots,\beta_t)=M_1M_2$ □

PROPOSITION

Let L/K be Galois and N/K be arbitrary

Then, LN/N is Galois and $\phi: Gal(LN/N)\cong Gal(L/L\cap N)$

$\sigma \longmapsto \sigma|_L$?

Proof

- Let L be the splitting field for the separable poly f over N, say $L=K(\alpha_1,\dots,\alpha_n)$

Then, $LN=N(\alpha_1,\dots,\alpha_n)$, hence LN/N is Galois ✓

- ϕ is well-def: $\because f(\sigma(\alpha_i)) = \sigma(f(\alpha_i))=0$ (as σ fixes K and $f\in K[x]$)

$\therefore \{\sigma(\alpha_1),\dots,\sigma(\alpha_n)\} = \{\alpha_1,\dots,\alpha_n\}$

- ϕ is 1-1: $\sigma\in\ker\phi \Leftrightarrow \sigma|_L = id_L \Leftrightarrow \sigma(\alpha_i)=\alpha_i\ \forall i \Leftrightarrow \sigma|_N$

- ϕ is onto: Let $H = Inv\,\phi \leq Gal(L/L\cap N)$ ($\Leftrightarrow Inv\,H = L\cap N$ (★))

(★): "$\supseteq$": obvious

"$\subseteq$": $\forall\sigma\in Gal(LN/N)$, $\sigma(x)=x\ \forall x\in (Inv\,H)N$

$\Rightarrow N\subseteq (Inv\,H)N\subseteq Inv\,Gal(LN/N)=N \Rightarrow N=(Inv\,H)N \Rightarrow Inv\,H\subseteq N$ ✓

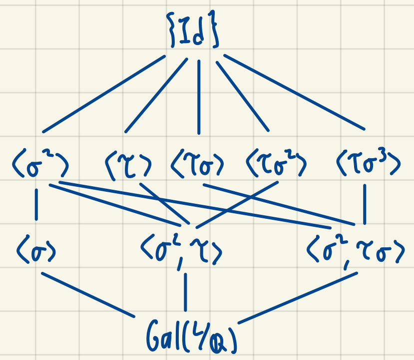
Check ϕ isom

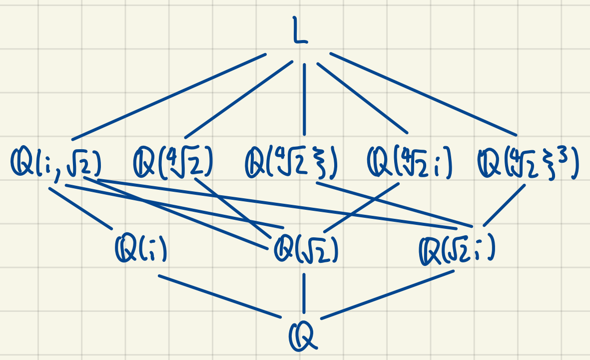
Shun/羊羽海 (@shun4midx)

EXAMPLE

Let $f(x)=x^4+2 \Rightarrow$ splitting field $L=\mathbb{Q}(i,\sqrt[4]{2})$

$\therefore [L:\mathbb{Q}]=8$, $Gal(L/\mathbb{Q}) \cong D_8$
$$\overset{\shortparallel}{\langle \sigma, \tau \rangle}$$





CYCLOTOMIC EXTENSION OVER $\mathbb{Q}$

DEFINITION

- $\zeta \in \mathbb{C}$ is called an n-th root of unity if $\zeta^n=1$
- ζ is primitive if $\zeta^n=1$ but $\zeta^\ell \neq 1$ for $\ell<n$
- $\zeta_n = e^{\frac{2\pi i}{n}}$
- $\{\text{primitive n-th root of unity}\} = \{\zeta_n^k \mid 1 \leq k<n, \gcd(k,n)=1\}$

DEFINITION

The nth cyclotomic poly is $\Phi_n := \prod_{1\leq k<n, \gcd(k,n)=1} (x-\zeta_n^k)$ which has degree $\phi(n)$

FACTS

- $\Phi_n \in \mathbb{Z}[x]$: By induction on n, $n=1$: $\Phi_1 = x-1$.

  $n>1$: $\underbrace{x^n-1}_{\in \mathbb{Z}[x]} = \prod_{d|n} \Phi_d = \underbrace{\left(\prod_{d|n, d<n} \Phi_d\right)}_{\text{By ind hyp, } \in \mathbb{Z}[x]} \Phi_n$

  By direct comparison of coeffs on both sides, $\Phi_n \in \mathbb{Z}[x]$. □

- Φ_n is irr in $\mathbb{Z}[x]$: [Φ_n is monic, Φ_n irr in $\mathbb{Z}[x] \Leftrightarrow \Phi_n$ irr in $\mathbb{Q}[x]$, so $\Phi_n = m_{\zeta_n, \mathbb{Q}}$]

  Suppose $\Phi_n = f\cdot g$, f is irr and monic, g is monic in $\mathbb{Z}[x]$

  Let ζ be a primitive nth root of unity s.t. $f(\zeta)=0$ and p be a prime s.t. $p \nmid n$

  If $g(\zeta^p)=0$, then ζ is a root of $g(x^p) \Rightarrow f(x) \mid g(x^p)$, say $g(x^p)=f(x)h(x)$

  In $\mathbb{Z}/p\mathbb{Z}[x]$, $\bar{g}(x^p)=\bar{f}(x)\bar{h}(x) \Rightarrow (\bar{g}(x))^p = \bar{f}(x)\bar{h}(x) \Rightarrow \bar{g}(x)$ and $\bar{f}(x)$ have a common root

  $\therefore \bar{\Phi}_n = \bar{f}\cdot\bar{g}$ has a repeated root $\Rightarrow x^n-\bar{1}$ has a repeated root $\Rightarrow (x^n-\bar{1})' = \bar{n}x^{n-1}=0 \Rightarrow p \mid n$ $\rightarrow\!\times\!\leftarrow$

  $\therefore$ We conclude that $f(\zeta^p)=0$ $\forall p \nmid n$. By induction, $f(\zeta^{p^r}) = f((\zeta^{p^{r-1}})^p)=0$ $\forall r \in \mathbb{N}$ and $f(\zeta^{p_1^{r_1}\cdots p_s^{r_s}}) = f((\zeta^{p_1^{r_1}\cdots p_s^{r_s-1}})^{p_s})=0$ $\forall p_i \nmid n, r_i \in \mathbb{N}$

  $\therefore f(\zeta^k)=0$ $\forall 1 \leq k<n, \gcd(k,n)=1$, i.e. $\Phi_n = f$ is irr □

QUESTION: IS EVERY FINITE GROUP G ISOMORPHIC TO SOME GALOIS GROUP $Gal(L/K)$?

Strategy: $S_n \overset{?}{\cong} Gal(L/K)$

CONSTRUCTION

Write $f(x)=(x-t_1)(x-t_2)\cdots(x-t_n) = x^n - s_1x^{n-1} + s_2x^{n-2} \cdots + (-1)^n s_n \in K[x]$, $K=F(s_1,\ldots,s_n)$

Let $L=K(t_1,\ldots,t_n)$ be a splitting field for f over K. Then, $Gal(L/K) \hookrightarrow S_n$. Notice, $L=F(t_1,\ldots,t_n)$

Now, for S_n, we can regard σ as an element in $Gal(L/K)$:
$$\begin{aligned} \sigma: F(t_1,\ldots,t_n) &\longrightarrow F(t_1,\ldots,t_n) \\ a\in F &\longmapsto a\in F \\ t_i &\longmapsto t_{\sigma(i)} \\ f(t_1,\ldots,t_n) &\longmapsto f(t_{\sigma(1)},\ldots,t_{\sigma(n)}) \end{aligned}$$

Key: $\sigma(s_i)=s_i\ \forall i$ since $\{\sigma(t_1),\dots,\sigma(t_n)\}=\{t_1,\dots,t_n\} \Rightarrow \sigma|_K = id_K$, i.e. $\sigma\in Gal(L/K)=S_n$

Shun/翔海(@shun4midx)

COROLLARY

$$\mathrm{Inv}\, S_n = K = F(s_1,\dots,s_n)$$
$$\|$$
$$\{f(t_1,\dots,t_n)\in K \mid f(t_{\sigma(1)},\dots,t_{\sigma(n)}) = f(t_1,\dots,t_n)\ \forall \sigma\in S_n\}$$

- $P_k=\sum_{i=1}^{n} t_i^k$

  Newton's identities: $kS_k=\sum_{i=1}^{k}(-1)^{i-1}S_{k-i}P_i$, $P_k=\sum_{i=1}^{k-1}(-1)^{i+k-1}S_{k-i}P_i+(-1)^{k-1}kS_k$

REMARK

Cubic equations, char $F\neq 2,3$:

For $f(x)=x^3+px+q$, $L=F(\alpha_1,\alpha_2,\alpha_3)$, $\delta=(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$, $\delta^2=D:=$ discriminant

Then, we have: $Gal(L/F)\cong S_3 \Leftrightarrow \sqrt{D}\notin F$

$Gal(L/F)\cong A_3 \Leftrightarrow \sqrt{D}\in F$