5-16-25 (WEEK 13)

Shun/舜海 (@shun4midx)

GALOIS RESULTANT

Given $f(x)$ separable in $K(x)$ and $\alpha_1, \dots, \alpha_n$ all roots of $f(x)$, let $L = K(\alpha_1, \dots, \alpha_n)$, how can we find $\mathrm{Gal}(L/K)$?

DEFINITION

Define $\theta = y_1\alpha_1 + \dots + y_n\alpha_n$

$\forall \sigma \in S_n$, $\sigma_y(\theta) = y_{\sigma(1)}\alpha_1 + \dots + y_{\sigma(n)}\alpha_n$, $\sigma_\alpha(\theta) = y_1\alpha_{\sigma(1)} + \dots + y_n\alpha_{\sigma(n)}$

Notice, $\sigma_y\sigma_\alpha(\theta) = \sigma_\alpha\sigma_y(\theta) = \theta \Rightarrow \sigma_\alpha(\theta) = \sigma_y^{-1}(\theta)$, $\sigma_y(\theta) = \sigma_\alpha^{-1}(\theta) = (\sigma^{-1})_\alpha(\theta)$

In $L(x, y_1, \dots, y_n)$, consider $F(x,y) = \prod_{\sigma\in S_n}(x - \sigma_y(\theta)) = \prod_{\sigma\in S_n}(x - (\sigma^{-1})_\alpha(\theta)) = \prod_{\sigma\in S_n}(x - \sigma_\alpha(\theta))$

EXAMPLE

$f(x) = x^3 - 3x + 1 \Rightarrow D = 81 \Rightarrow \sqrt{D} \in \mathbb{Q} \Rightarrow G(f) \cong A_3$ ($[\mathbb{Q}(\alpha):\mathbb{Q}] = 3 \mid |G(f)|$, $\sqrt{D} \in \mathbb{Q} \Rightarrow$ no intermediate field $\Rightarrow A_3$!)

($f(x) = x^3 + 3x + 1 \Rightarrow D = -135 \Rightarrow \sqrt{D} \notin \mathbb{Q} \Rightarrow G(f) \cong S_3$)

Consider $F(x,y) = (x - (y_1\alpha_1 + y_2\alpha_2 + y_3\alpha_3))(x - (y_1\alpha_2 + y_2\alpha_3 + y_3\alpha_1))(x - (y_1\alpha_3 + y_2\alpha_1 + y_3\alpha_2))(x - (y_1\alpha_2 + y_2\alpha_1 + y_3\alpha_3))(x - (y_1\alpha_1 + y_2\alpha_3 + y_3\alpha_2))$
$(x - (y_1\alpha_3 + y_2\alpha_2 + y_3\alpha_1)) \in \mathbb{Z}[x, y_1, y_2, y_3]$ (UFD)

FORMALIZATION

Each coefficient of F is a symmetric function of $\alpha_1, \dots, \alpha_n$, so it can be expressed in terms of the coef of $f(x)$, thus $F(x,y) \in K[x, y_1, \dots, y_n]$ (UFD)

We can decompose $F(x,y)$ into irr factors in $K(x, y_1, \dots, y_n)$: $F(x,y) = F_1(x,y)\cdots F_r(x,y)$

Note that $\forall \sigma \in S_n$, $F = \sigma_y F = (\sigma_y F_1)(\sigma_y F_2)\cdots(\sigma_y F_r)$ and F_i is irr $\Rightarrow \sigma_y F_i$ is irr (otherwise, $\sigma_y F_i = PQ \Rightarrow F_i = \sigma_y^{-1}P\,\sigma_y^{-1}Q$), so σ induces a permutation of $F_1, \dots, F_r$.

We may assume that $(x-\theta) \mid F_1$.

LEMMA

$Q = \{\sigma \in S_n \mid \sigma_y F_1 = F_1\} = \{\sigma \in S_n \mid x - \sigma_y(\theta) = \sigma_y(x-\theta) \mid F_1\}$

Proof

"$\subseteq$": $x - \theta \mid F_1 \Rightarrow \sigma_y(x-\theta) = x - \sigma_y$

"$\supseteq$": $\sigma_y(F_1) = F_i$ for some i and $x - \sigma_y(\theta) \mid F_i \Rightarrow F_1 = F_i$

PROPOSITION

$\mathrm{Gal}(L/K) = Q = \{\sigma \in S_n \mid \sigma_y F_1 = F_1\}$

Proof

"$\subseteq$": For $\sigma \in \mathrm{Gal}(L/K) \subseteq S_n$, we extend σ to an action,

$$\begin{aligned} \sigma^e : L(y_1, \dots, y_n) &\longrightarrow L(y_1, \dots, y_n) \\ y_i &\longmapsto y_i \\ \alpha \in L &\longmapsto \sigma(\alpha) \\ \theta &\longmapsto \sigma_\alpha(\theta) \end{aligned}$$

which fixes $K(y_1, \dots, y_n)$

Observe that $\sigma^e(\theta) = \sigma_\alpha(\theta)$ and θ share the same min poly over $K(y_1, \dots, y_n)$, and F_1 is irr in $K[y_1, \dots, y_n][x] \Rightarrow$ irr in $K(y_1, \dots, y_n)[x]$,

so $F_1 = m_{\theta, K(y_1,\dots,y_n)} = m_{\sigma(\theta), K(y_1,\dots,y_n)} \Rightarrow (x - \sigma_\alpha(\theta)) \mid F_1 \Rightarrow \sigma^{-1} \in Q$, i.e. $(\sigma^{-1})_y F_1 = F_1 \Rightarrow F_1 = \sigma_y F_1 \Rightarrow \sigma \in Q$ ✓

($\sigma_\alpha = (\sigma^{-1})_y$)

"$\supseteq$": $\forall \sigma \in Q$, i.e. $x - \sigma_y(\theta) \mid F_1$ ($\sigma_\alpha^{-1} = \sigma_y$), we have $F_1 = m_{\theta, K(y_1,\dots,y_n)}$

Hence, $\exists \tau \in \mathrm{Aut}(L(y_1,\dots,y_n)/K(y_1,\dots,y_n))$ s.t. $\tau(\theta) = \sigma_\alpha^{-1}(\theta)$

Here, we find that $\tau|_L \in \mathrm{Gal}(L/K)$ and $\tau|_L(\alpha_i) = \alpha_{\sigma^{-1}(i)} \Rightarrow \sigma^{-1} \in \mathrm{Gal}(L/K) \Rightarrow \sigma \in \mathrm{Gal}(L/K)$ (group) □

THEOREM

Shun/翔海 (@shun4midx)

Given $f(x)$ monic and separable in $\mathbb{Z}[x]$, assume that $p \nmid D := \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}$. Then, the Galois group of $F(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ is a subgroup of the Galois group of $f(x)$

Proof

By assumption, the discriminant of $\bar{f}(x)$ is $\bar{D} \pmod p \neq 0$, so $\bar{f}(x)$ is still separable

$\because D = (-1)^{\frac{n(n-1)}{2}} R(f, f')$

$\therefore \bar{D} = (-1)^{\frac{n(n-1)}{2}} R(\bar{f}, \bar{f}')$

As above, $F(x,y) = F_1(x,y) \cdots F_r(x,y)$ in $\mathbb{Z}[x, y_1, \cdots, y_n]$

Observe that if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ has roots $\alpha_1, \cdots, \alpha_n$, then $\bar{f}(x) = x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0$ has roots $\beta_1, \cdots, \beta_n$ with $S_i(\beta_1, \cdots, \beta_n) = \overline{S_i(\alpha_1, \cdots, \alpha_n)}$ in $\mathbb{Z}/p\mathbb{Z}$

Also, $\theta_\rho = y_1\beta_1 + \cdots + y_n\beta_n$, $F_\rho(x,y) = \prod_{\sigma \in S_n} (x - \sigma_y(\theta_\rho)) = \bar{F}(x,y) = \bar{F}_1 \cdots \bar{F}_r$ in $\mathbb{Z}/p\mathbb{Z}[x, y_1, \cdots, y_n]$

$= (G_{1,1} \cdots G_{1,s_1})(G_{2,1} \cdots G_{2,s_2}) \cdots (G_{r,1} \cdots G_{r,s_r})$, G_{ij} : irr

Since the Galois group of $\bar{f} = \{\sigma \in S_n \mid \sigma_y G_{1,j} = G_{1,j}\}$ $\forall j$ and $G_{1,j} \mid \bar{F}_1$, Gal group of $f \subseteq \{\sigma \in S_n \mid \sigma_y \bar{F}_1 = \bar{F}_1\} = \{\sigma \in S_n \mid \sigma_y F_1 = F_1\}$ = Galois group of f □

KEY FACTS (STRATEGY TO EVALUATE GALOIS GROUPS)

- Every finite extension of $\mathbb{Z}/p\mathbb{Z}$ is cyclic
- If $f(x)$ is irr, then the Galois group of $f(x)$ is transitive on its roots
- If $\bar{f}(x)$ is in $\mathbb{Z}/p\mathbb{Z}[x]$ and its Galois group is $\langle \sigma \rangle \subseteq S_n$, then σ must be a cycle of length n

CONCLUSION

If $\bar{f}(x) = \bar{f}_1(x) \cdots \bar{f}_r(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ with $\bar{f}_i$ irr of deg m_i, then the Galois group of $f(x)$ contains a permutation of the type $(\alpha_{1,1} \cdots \alpha_{1,m_1}) \cdots (\alpha_{r,1} \cdots \alpha_{r,m_r})$

EXAMPLE

1. $f(x) = x^5 - x - 1$ (If $\delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \in K$, then $\delta \in \mathrm{Fix} G \Rightarrow G \subseteq A_n$. $\therefore \delta \notin k \Rightarrow G \not\subseteq A_n$)
   - $D = 2869 = 19 \times 151 \Rightarrow \sqrt{D} \notin \mathbb{Q} \Rightarrow G(f) \not\subseteq A_5$
   - In $\mathbb{Z}/2\mathbb{Z}[x]$, $\bar{f}(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$ ← Got from factoring $x^{2^2} - x$, $x^{2^3} - x$
     $\Rightarrow (ab)(cde) \in G$, $(a\ b) = [(ab)(cde)]^3 \in G$
   - In $\mathbb{Z}/3\mathbb{Z}[x]$, $\bar{f}(x) = x^5 - x - 1$
     - No linear factor
     - No quadratic factor. If $\bar{f} = h \cdot g$, $\deg h = 2$, then $h(x) \mid x^{3^2} - x \Rightarrow h(x) \mid x^8 - 1$ or $h(x) \mid x^4 + 1$ ✗ ($x^5 - x \Rightarrow (x^5 - x - 1) - (x^5 - x) = -1 \Rightarrow h(x) \mid -1$ ✗; $x^5 + x \Rightarrow 2x + 1$ ✗)
     - $\therefore (a'\ b'\ c'\ d'\ e') \in G$

   $\therefore G \cong S_5$.

LEMMA

A transitive subgroup G of S_n containing a 2-cycle and $(n-1)$-cycle is S_n.

Proof

Say $(i\ j)$, $(1\ 2 \cdots (n-1)) \in G$ (σ)

$\because G$ is transitive

$\therefore \exists \sigma \in G$ s.t. $\sigma(j) = n$

Then, $\tau = \sigma(i\ j)\sigma^{-1} = (k\ n)$, where $\sigma(i) = k$, $1 \le i \le k-1$

Notice, $(1\ 2 \cdots n-1)(k\ n)(1\ 2 \cdots n-1)^{-1} = (k+1\ n) \in G \Rightarrow$ By induction, $(i\ n) \in G$ $\forall i$

$\therefore G = \langle (1\ n), (2\ n), \cdots, (n-1\ n) \rangle = S_n$ □

EXAMPLE

Shun / 翔海 (@shun4midx)

$f(x)=x^6+22x^5+21x^4+12x^3-37x^2-29x-15$

In $\mathbb{Z}/2\mathbb{Z}[x]$, $\bar{f}(x)=x^6+x^4+x^2+x+1$ is irr $\Rightarrow$ $G(f)$ is transitive

In $\mathbb{Z}/3\mathbb{Z}[x]$, $\bar{f}(x)=x^6+x^5-x^2+x=x(x^5+x^4-x+1)$ is irr $\Rightarrow$ $(1\ 2\ 3\ 4\ 5) \in G(f)$ (deg 5)

In $\mathbb{Z}/5\mathbb{Z}[x]$, $\bar{f}(x)=x^6+2x^5+x^4+2x^3-2x^2+x=x(x-1)(x+1)(x+2)(x^2+2) \Rightarrow (a\ b) \in G(f)$

$\therefore$ By lemma, $G(f)\cong S_6$