5-21-25 (WEEK 14)

Shun/翔海 (@shun4midx)

COMPUTATIONS

Let $G \leq S_n$

- If G contains an n-cycle, then G is transitive
- If G is transitive, then H may NOT contain an n-cycle (e.g. $V_4 \leq S_4$)
- When $n=p$: a prime, if G is transitive, then G must contain a p-cycle
  - ↳ Let $G \curvearrowright \{1, \dots, p\}$, then $p = |orb(1)| = \frac{|G|}{|Stab_G(1)|} \Rightarrow p \mid |G|$
  - ∴ By Cauchy thm, $\exists \sigma \in G$, s.t. $ord(\sigma) = p \Rightarrow \sigma$ is a p-cycle

Notice, all subgroups of S_5 have order 5, 10, 20, 60, 120.

The transitive subgroups of S_5:

- $\langle (1\ 2\ 3\ 4\ 5) \rangle \cong C_5$ } solvable
- $\langle \overset{\text{rotation}}{(1\ 2\ 3\ 4\ 5)}, \overset{\text{reflection}}{(2\ 5)(3\ 4)} \rangle \cong D_{10}$ } solvable
- $\langle (1\ 2\ 3\ 4\ 5), (1\ 2\ 3) \rangle \cong A_5 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5) \rangle$
- $\langle (1\ 2\ 3\ 4\ 5), (1\ 2) \rangle \cong S_5$
- $\langle \underset{a}{(1\ 2\ 3\ 4\ 5)}, \underset{b}{(1\ 2\ 3\ 4)} \rangle \cong C_5 \rtimes C_4 =: F$ $= \langle a, b \mid a^5=1, b^4=1, bab^{-1}=a^2 \rangle$ ← order $20 = 2^2(5) \Rightarrow$ solvable ✓

EXAMPLE

Notice, $[\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] = 10$ ($\because x^{10}+x^9+\dots+x^2+x+1=0$)

Say $\alpha = \zeta_{11} + \zeta_{11}^{-1}$, notice the original equation becomes $x^5+x^{-5}+x^4+x^{-4}+x^3+x^{-3}+x^2+x^{-2}+x+x^{-1}+1=0$

↳ $(x+x^{-1})^2 = x^2+x^{-2}+2 \Rightarrow x^2+x^{-2} = (x+x^{-1})^2 - 2$

↳ $(x+x^{-1})^3 = x^3+3x+3x^{-1}+x^{-3} = x^3+x^{-3}+3(x+x^{-1}) \Rightarrow x^3+x^{-3} = (x+x^{-1})^3 - 3(x+x^{-1})$

↳ $(x+x^{-1})^4 = x^4+x^{-4}+4(x^2+x^{-2})+6 \Rightarrow x^4+x^{-4} = (x+x^{-1})^4 - 4(x+x^{-1})^2 - 2$

↳ $(x+x^{-1})^5 = x^5+x^{-5}+5(x^3+x^{-3})+10(x+x^{-1}) \Rightarrow x^5+x^{-5} = (x+x^{-1})^5 - 5(x+x^{-1})^3 - 5(x+x^{-1})$

∴ Original equation: $(x+x^{-1})^5+(x+x^{-1})^4-4(x+x^{-1})^3-3(x+x^{-1})^2+3(x+x^{-1})+1=0$

As $x^5+x^4-4x^3-3x^2+3x+1$ is irr, thus $x^{10}+x^9+\dots+x+1=0$ corr to C_5 (We can use this method to construct any cyclic Galois group)

S_5: x^5-4x+2 (3 real roots, 2 complex roots)

F: $x^5-2 \rightsquigarrow L = \mathbb{Q}(\sqrt[5]{2}, \zeta_5) \Rightarrow$ roots: $\sqrt[5]{2}, \sqrt[5]{2}\zeta_5, \dots, \sqrt[5]{2}\zeta_5^4$

∴ $\sqrt[5]{2} \longmapsto$ 5 choices

$\zeta_5 \longmapsto \zeta_5^i$, $i = 1, 2, \dots, 4$

∴ $Gal(L/\mathbb{Q}) = F$

A_5: $x^5+20x+16 \Rightarrow D = 2^{16}5^6 \Rightarrow \sqrt{D} \in \mathbb{Q} \Rightarrow Gal(f) \leq A_5 \Rightarrow Gal(f) = A_5$

D_{10}: $x^5-5x+12$

HILBERT'S THEOREM

$\forall n \in \mathbb{N}$, $\exists$ infinitely many $f(x)$ of deg n in $\mathbb{Z}[x]$, s.t. $Gal_{\mathbb{Q}}(f) \cong S_n$

RECALL

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

Shun/羊羽海 (@shun4midx)

PROOF OF THEOREM

We choose some monic poly as follows:

- $f_1(x)$ in $\mathbb{Z}[x]$ s.t. $\deg f_1 = n$ and $\bar{f}_1(x)$ is irr in $\mathbb{Z}/2\mathbb{Z}[x]$ (in $x^{2^n}-x$)
- Let $g(x)$ be irr in $\mathbb{Z}/3\mathbb{Z}[x]$ of deg $n-1$ (in $x^{3^{n-1}}-x$) and $f_2(x)$ of deg n s.t. $\bar{f}_2(x) = xg(x)$ in $\mathbb{Z}/3\mathbb{Z}[x]$
- Let $h(x)$ be irr in $\mathbb{Z}/5\mathbb{Z}[x]$ of deg 2 (in $x^{5^2}-x$)

Will have a 2-cycle since $((a\,b)(c_1 \cdots c_{n-2}))^{n-2} = (a\,b)$

If n is odd, let $p(x)$ be irr in $\mathbb{Z}/5\mathbb{Z}[x]$ of deg $n-2$ (in $x^{5^{n-2}}-x$) and choose $f_3(x)$ of deg n s.t. $\bar{f}_3(x) = h(x)p(x)$ in $\mathbb{Z}/5\mathbb{Z}[x]$

If n is even, let $p_1(x)$ and $p_2(x)$ be irr in $\mathbb{Z}/5\mathbb{Z}[x]$ of deg 1 and $n-3$ respectively and choose $f_3(x)$ of deg n, s.t. $\bar{f}_3(x) = h(x)p_1(x)p_2(x)$

$((a\,b)(c_1 \cdots c_{n-3}))^{n-3} = (a\,b)$

Now, let $f(x) = -15f_1(x) + 10f_2(x) + 6f_3(x)$ which is monic and $G = \mathrm{Gal}(f)$

$\Rightarrow \bar{f}(x) = \bar{f}_1(x)$ in $\mathbb{Z}/2\mathbb{Z}$, $\bar{f}(x) = \bar{f}_2(x)$ in $\mathbb{Z}/3\mathbb{Z}$, $\bar{f} = \bar{f}_3(x)$ in $\mathbb{Z}/5\mathbb{Z}$

$\therefore G = S_n$

Notice, there are infinitely many $f(x)$ s.t. $\bar{f}(x) = f_1(x)$ in $\mathbb{Z}/2\mathbb{Z}[x]$ (e.g. $f_1(x) = x^2+x+1 \Rightarrow x^2+(2k+1)x+1\ \forall k \in \mathbb{Z}$)

WHAT IS F?

- Say $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$

  Let $G = G_0 \cong \langle 0 \rangle \times G_1 \cong \langle 0 \rangle \times \langle 0 \rangle \times G_2 \dots$

  $\therefore$ All abelian G are solvable
- G is solvable $\Leftrightarrow \exists\ 1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_s = G$, H_{i+1}/H_i is abelian

DERIVED SERIES: $G^{(0)} = G$, $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$, ...

G is solvable $\Leftrightarrow \exists n$, s.t. $G^{(n)} = 1$ for some $n \geq 1$

Proof

"$\Leftarrow$": $G^{(0)} = G \triangleright G^{(1)} \triangleright \dots \triangleright G^{(n)} = 1$

"$\Rightarrow$": $\exists\ 1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_s = G$, where H_{i+1}/H_i: abelian

Claim: $G^{(i)} \leq H_{s-i}$

Proof

By induction on i,

- $i = 0$: $G^{(0)} = G = H_s$
- $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [H_{s-i}, H_{s-i}] \leq H_{s-i-1}$ ($\because H_{s-i}/H_{s-i-1}$: abelian)
- $H_0 = 1 \Rightarrow G^{(s)} = 1$ ✓

GOAL

Let G be a transitive (contains a p-cycle) solvable subgroup of S_p.

The derived series: $1 = G^{(n)} \triangleleft G^{(n-1)} \triangleleft \dots \triangleleft G^{(1)} \triangleleft G_0 = G$ (abelian; $\triangleright \langle (1 \cdots n) \rangle \triangleleft$)

We have $G^{(n-1)} \triangleleft G$

Claim: $p \mid |G^{(n-1)}|$ (abelian)

Proof

Let $H = \mathrm{Stab}_G(1)$

- $p = |\mathrm{orb}(1)| = \frac{|G|}{|H|} \Rightarrow H$ is max in G
- $H \cap G^{(n-1)} \triangleleft G$:

  $\hookrightarrow G^{(n-1)} \leq H \Rightarrow G^{(n-1)} \cap H = G^{(n-1)} \triangleleft G$

  $\hookrightarrow G^{(n-1)} \not\leq H \Rightarrow \because H$ is max $\therefore HG^{(n-1)} = G$

$\forall x \in H \cap G^{(n-1)}$, $g = ha \in G$ ($\in H$, $\in G^{(n-1)}$) $\Rightarrow gxg^{-1} = h(axa^{-1})h^{-1} = hxh^{-1} \in H \cap G^{(n-1)}$

- H has no nontrivial subgroup in G
- $\therefore H \cap G^{(n-1)} = \{1\} \Rightarrow HG^{(n-1)} = G \Rightarrow \sigma = (1 \dots p) \in G^{(n-1)}$

Shun/羊羽海(@shun4midx)

Assume that $\langle e\rangle = G^{(n)} \triangleleft \langle (1\ 2 \cdots p)\rangle = G^{(n-\frac{1}{2})} \triangleleft G^{(n-1)} \triangleleft \cdots \triangleleft G^{(1)} \triangleleft G^{(0)} = G$, where $(1\ 2 \cdots p) = \langle\sigma\rangle$

Consider $\sigma: \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$, $i \longmapsto i+1$, an affine transformation of $\mathbb{Z}/p\mathbb{Z}$ $\tau_{(a,b)}(k) = ak+b \in S_p$ ($a \neq 0$), $\{0,\dots,p-1\} \mapsto \{0,\dots,p-1\}$ (order $p(p-1)$)

$\therefore \{\{\tau_{(a,b)} \mid a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z}\}, \circ\}$ forms a subgroup F of S_p of order $p(p-1)$

THEOREM

$G \leq F$

Proof

- $G^{(n-\frac{1}{2})} \leq F$
- Suppose $G_j \leq F$ and $\tau \in G_{j-1}$. Then, $\tau\sigma\tau^{-1} = \tau_{(a,b)} \in G_j$ $\Rightarrow G_{j-1} \leq F$

  Since σ is a p-cycle, thus $\tau\sigma\tau^{-1}$ is a p-cycle, so it doesn't fix x, i.e. no sol

  Thus, $\tau\sigma\tau^{-1}(x) = ax+b = x$ has no solution in $\mathbb{Z}/p\mathbb{Z}$ $\Rightarrow a=1, b\neq 0 \Rightarrow \tau\sigma\tau^{-1} \in G^{(n-\frac{1}{2})} \setminus \{id\}$

  So, $\tau(k+1) = \tau\sigma(k) = \tau\sigma\tau^{-1}\tau(k) = \tau(k)+b \Rightarrow \tau \in F$

  $\hookrightarrow \tau(k+1) = \tau(k)+b,\ \tau(k) = \tau(k-1)+b, \dots \Rightarrow \tau(k+1) = \tau(0)+b(k+1)$