Theorem (Galois Thm)

Let char $F=0$.

Then $f(x)\in F[x]$ is soluble by radicals $\Leftrightarrow$ $Gal(f)$ is a soluble group.

Let $f(x)=x^5-8x+2\in\mathbb{Q}[x]$ —— has exactly two roots.

$Gal(f)\cong S_5$ —— insoluble.

A_5 —— simple.

Lemma Let G be a transitive permutation group on $\Omega=\{1,2,\cdots,p\}$.

Assume that G contains a transposition and $|\Omega|=p$ is a prime.

Then $G=Sym(\Omega)\cong S_p$.

Proof: Since G is trans. on Ω, $|\Omega|\,\big|\,|G|$, so $p\,|\,|G|$. and G contains an elt of order p.

i.e. $g=(1\,2\cdots p)$. without loss of generality. Then $\langle(1\,2\cdots p),(i\,j)\rangle=S_p$. $\square$

Rmk: $\langle(1\,2\cdots p),(1\,2\,3)\rangle=A_p$. $(p\geq 5)$

Prop. Let $f(x)\in F[x]$ with char $F=0$. $F=\mathbb{Q}$.

Assume that $f(x)$ is irreducible of deg p with p prime.

Assume further that $f(x)$ has exactly two complex roots. Then $Gal(f)=S_p$.

Proof: The complex conjugation is a transposition of $Gal(f)$ acting on $\Omega=\{$ roots of $f(x)\}$.

By Lemma, $Gal(f)\cong S_p$.

$f(x)=x^p-a\in\mathbb{Q}[x]$, where p prime, $a^{\frac{1}{p}}\notin\mathbb{Q}$. $f(x)$ irreducible.

$Gal(f)\cong \mathbb{Z}_p:\mathbb{Z}_{p-1}=Hol(\mathbb{Z}_p)\overset{?}{=}Aut(D_{2p})$

Let $w=e^{2\pi i/p}$, root of $x^{p-1}+x^{p-2}+\cdots+x+1$. (x^p-1)

$\alpha=a^{\frac{1}{p}}\notin\mathbb{Q}$.

Then $\alpha,\alpha w,\alpha w^2,\cdots\alpha w^{p-1}$ are the roots of x^p-a. $\#=p$.

Let $E=\mathbb{Q}(\alpha,\alpha w,\cdots,\alpha w^{p-1})$. Then E is a splitting field of x^p-a.

splitting extension.

Let $L=\mathbb{Q}(w)<E$. then $\mathbb{Q}<L<E$. and L is a splitting extension (normal extension) of $\mathbb{Q}$, a splitting field of x^p-1 over $\mathbb{Q}$.

$Gal(f)$ is transitive on the roots of f.

$\Rightarrow Gal(f)$ primitive of prime deg p.

blocks: $\Omega=\Delta_1\cup\Delta_2\cup\cdots\cup\Delta_m$.

s.t. $\{\Delta_1,\cdots,\Delta_m\}$. $\Delta_i^g=\Delta_j$.

Thus, $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/\mathbb{Q})$. and $\boxed{\mathrm{Gal}(E/\mathbb{Q}) / \mathrm{Gal}(E/L) \cong \mathrm{Gal}(L/\mathbb{Q})}$.

$$\begin{tikzcd} E \arrow[d, dash] \arrow[d, bend left] \arrow[dd, bend left=60] \\ L \arrow[d, dash] \arrow[d, bend right] \\ \mathbb{Q} \end{tikzcd}$$

Consider $\mathrm{Gal}(E/L)$ and $\mathrm{Gal}(L/\mathbb{Q})$.

Now $\mathrm{Gal}(L/\mathbb{Q})$ is a splitting field of irr. poly $x^{p-1}+x^{p-2}+\cdots+x+1$. So $\mathrm{Gal}(L/\mathbb{Q})$ is transitive on the $p-1$ roots: $w, w^2, \cdots, w^{p-1}$.

The group $\mathrm{Gal}(E/L)$, where $E = L(\alpha)$, contains an elt. $\rho: \alpha \mapsto \alpha w \mapsto \alpha w^2 \mapsto \cdots \mapsto \alpha w^{p-1}$. $\langle \rho \rangle \cong \mathbb{Z}_p$.

<u>Claim:</u> $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q})$.
$= \mathbb{Z}_p \cdot \mathbb{Z}_{p-1}$.

① $\mathrm{Gal}(E/L) = \langle \rho \rangle$.

Otherwise, $\exists\, \tau \in \mathrm{Gal}(E/L)$ s.t. $\begin{array}{l} \alpha^\tau = \alpha \\ (\alpha w^i)^\tau = \alpha w^j \text{ with } i \neq j. \end{array}$

$\tau: \alpha \mapsto \alpha$,
$\alpha w^i \mapsto \alpha w^j$. $\tau \in \mathrm{Gal}(E/L)$, i.e. τ fixes L pointwise, so $w^\tau = w$.

$\Rightarrow w^i \mapsto w^j$. $i \neq j$. a contradiction. So $\mathrm{Gal}(E/L) = \langle \rho \rangle$.

② $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$, where $\sigma: w \mapsto w^r$, with r being a primitive root in $\mathbb{Z}_{p-1}$, i.e.

$w, w^r, w^{r^2}, w^{r^3}, \cdots, w^{r^{p-1}}$ distinct, or $r^i \not\equiv r$ if $i<p$, or $O_p(r) = p-1$.
$\downarrow$
r's order in $\mathbb{Z}_p$.

If $p=5$, then $r=2$.
$p=7$, then $r=3$. i.e. $\sigma: w \mapsto w^3$.

Note that $\mathbb{Z}_{p-1} \cong \langle \sigma \rangle \leq \mathrm{Gal}(L/\mathbb{Q}) =: G$. So $G = \langle \sigma \rangle G_w$. transitive on $\{w, w^2, \cdots, w^{p-1}\}$.

Suppose $\tau \in G_w$, s.t. $w^j \mapsto w^k$ with $j \neq k$.
$w \mapsto w$.
$w^j \mapsto w^j$ not possible.

Therefore, $G = \mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q})$
$= \langle \rho \rangle \cdot \langle \sigma \rangle$.
$\cong \mathbb{Z}_p \cdot \mathbb{Z}_{p-1}$
$= \mathbb{Z}_p : \mathbb{Z}_{p-1} = \mathrm{Aut}(D_{2p})$.
$= AGL(1,p)$. $AGL_1(p)$.

$G = N : H$.
Let $C = C_G(N)$.
$= \{g \in G \mid [g, N] = 1\}$.
Then $N \leq C$, and C is trans. $\Rightarrow N = C$.

Ex. A transitive abelian permutation group is regular.

(G is trans. on Ω. and $|G| = |\Omega|$ or $G_w = 1$)

Thus $\langle \sigma \rangle$ acts on $\langle \rho \rangle$ faithfully. so $\sigma \in Aut(\rho)$.

Let $\sigma_0 = \sigma^{\frac{p-1}{2}}$, then $|\sigma_0| = 2$. Now $\rho^{\sigma_0} = \rho^j$ for some integer j with $1 \le j < p$.

Since $\sigma_0^2 = 1$, we have $\rho^{\sigma_0^2} = (\rho^j)^{\sigma_0} = \rho^{j^2} = \rho$. So $\rho^{j^2-1} = 1$. and $\underset{(j-1)(j+1)}{\underset{\parallel}{j^2-1}} \equiv 0 \pmod p \Rightarrow j = -1$. $\langle \rho, \sigma_0 \rangle = D_{2p}$.

Ex. Prove $f(x) = x^5 - 6x + 3$ or $x^5 - 4x + 2$ are not soluble by radicals, i.e. $Gal(f)$ is not soluble.

faithful: $G = N : H$. $\alpha : H \to Aut(N)$ $\ker \alpha = 1$.

faithful for group action: $G \curvearrowright \Omega$, $g \in G$, g fix Ω pointwise $\Leftrightarrow g = e$.

primitive: $G \curvearrowright \Omega$ has no non-trivial blocks.

regular: $G \curvearrowright \Omega$, $G_\alpha = 1$, $\forall \alpha \in \Omega$.

Thm if $G \curvearrowright \Omega$ tran. $N \le G$, $N \curvearrowright \Omega$ tran.

Then $G = N G_w$. for arbitrary $w \in \Omega$.

eg. $w_1 \in G$, $G \overset{?}{=} N G_{w_1}$

$g \in G$, $w_1^g = w_2$.

$\exists n \in N$, $w_1^n = w_2$.

$w_1 = w_2^{n^{-1}} = w_1^{gn^{-1}}$ $gn^{-1} \in G_{w_1}$

$\exists h \in G_{w_1}$, $gn^{-1} = h$, $g = hn$ $G = G_{w_1} N$.