(106)

4/26/2019 $\rightarrow$ proof (that all roots of $f(x)$ solvable $\Rightarrow G(\mathbb{K}/\mathbb{F})$ a solvable group):

let α be any root of $f(x)$, lying in $\mathbb{F}'$ atop a root tower over $\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_r = \mathbb{F}'$

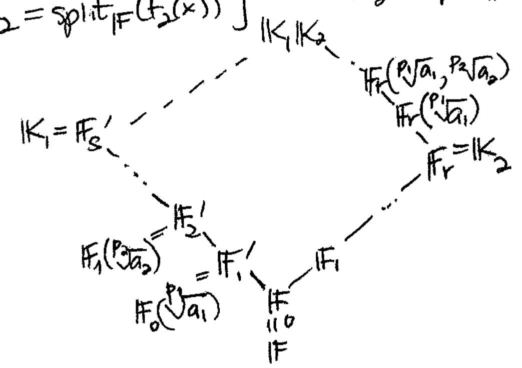
We repeatedly use this:

LEMMA: In this setting
$$\begin{array}{ccc} & \mathbb{C} & \\ & \mathbb{K}_1\mathbb{K}_2 & \\ \mathbb{K}_1 & & \mathbb{K}_2 \\ & \mathbb{F} & \end{array}$$
, (a) $\mathbb{K}_1/\mathbb{F}$, $\mathbb{K}_2/\mathbb{F}$ Galois $\Rightarrow \mathbb{K}_1\mathbb{K}_2/\mathbb{F}$ Galois

(b) $\mathbb{K}_1, \mathbb{K}_2$ atop root towers over $\mathbb{F}$ $\Rightarrow$ same for $\mathbb{K}_1\mathbb{K}_2$

proof: (a): $\left.\begin{array}{l}\mathbb{K}_1 = \mathrm{split}_{\mathbb{F}}(f_1(x)) \\ \mathbb{K}_2 = \mathrm{split}_{\mathbb{F}}(f_2(x))\end{array}\right\} \Rightarrow \mathbb{K}_1\mathbb{K}_2 = \mathrm{split}_{\mathbb{F}}(f_1(x)f_2(x))$

(b):



Let $\mathbb{L}$ be the smallest Galois extension of $\mathbb{F}$ containing $\mathbb{F}'$, namely if $\mathbb{F}' = \mathbb{F}(\beta)$ via Prim Elt Thm

then $\mathbb{L} = \mathrm{split}_{\mathbb{F}}(m_{\mathbb{F},\beta}(x))$ (called Galois closure of $\mathbb{F}'$ over $\mathbb{F}$)

$= \mathbb{F}(\sigma_1(\beta), \sigma_2(\beta), \ldots, \sigma_n(\beta))$ if $G(\mathbb{L}/\mathbb{F}) = \{\sigma_1, \ldots, \sigma_n\}$

$= \underbrace{\sigma_1(\mathbb{F}')\sigma_2(\mathbb{F}')\cdots\sigma_n(\mathbb{F}')}_{\text{compositum!}}$

Since $\sigma_i(\sqrt[p]{a}) = \sqrt[p]{\sigma_i(a)}$, the root tower for $\mathbb{F}'$ atop $\mathbb{F}$ gives root towers for each $\sigma_i(\mathbb{F}')$ atop $\mathbb{F}$ by applying σ_i.

Hence $\mathbb{L}$ is atop a root tower over $\mathbb{F}$ (by LEMMA (b)), and $\mathbb{L}/\mathbb{F}$ is Galois.

If $f(x)$ has roots $\alpha_1, \ldots, \alpha_d$, create such an $\mathbb{L}_i \ni \alpha_i$ for each $i = 1, 2, \ldots, d$, and then $\mathbb{L}_1\mathbb{L}_2\cdots\mathbb{L}_d := \hat{\mathbb{L}}$ is atop a root tower over $\mathbb{F}$, and is Galois over $\mathbb{F}$, containing $\alpha_1, \ldots, \alpha_d$, so $\hat{\mathbb{L}}$ contains $\mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x)) = \mathbb{F}(\alpha_1, \ldots, \alpha_d)$.

If $p_1, p_2, \ldots, p_m$ are all the primes in the root towers' $\sqrt[p_i]{a_i}$, let $\mathbb{L}' := \mathbb{F}(\zeta_{p_1}, \ldots, \zeta_{p_m})$
$= \mathbb{F}(\zeta_{p_1})\cdots\mathbb{F}(\zeta_{p_m})$

which also has $\mathbb{L}'/\mathbb{F}$ Galois and lies atop a root tower over $\mathbb{F}$.

(107) Finally, $\mathbb{L}'\cdot\hat{\mathbb{L}}$ lies atop a root tower extending

$$\mathbb{F} \;\text{———}\; \underset{\mathbb{F}(\zeta_{p_1},\dots,\zeta_{p_m})}{\underset{\parallel}{\mathbb{L}'}} \;\text{————}\; \mathbb{L}'\cdot\hat{\mathbb{L}}$$

in which every step $\mathbb{F}_i/\mathbb{F}_{i-1}$ has $\mathbb{F}_i/\mathbb{F}_{i-1}$ Galois with Galois group $G(\mathbb{F}_i/\mathbb{F}_{i-1})$ cyclic

(use our (prime) cyclotomic results in the $\mathbb{F}$ — $\mathbb{L}'$ steps,
and the (prime) Kummer results in the $\mathbb{L}'$ — $\mathbb{L}'\hat{\mathbb{L}}$ steps, since the p_i^{th} roots of unity are present)

Since $\mathbb{L}'\hat{\mathbb{L}}$ is also Galois over $\mathbb{F}$, the main theorem shows $G(\mathbb{L}'\hat{\mathbb{L}}/\mathbb{F})$ is solvable:

$$\begin{array}{ccccc}
 & \mathbb{L}'\hat{\mathbb{L}} & & \{1\} & \\
 & \vdots & & \vdots & \\
\text{Galois, cyclic}\left\{\begin{array}{c}\\ \\ \end{array}\right. & \begin{array}{c}\mathbb{F}_{i-1}\\ | \\ \mathbb{F}_i\end{array} & \longleftrightarrow & \begin{array}{c}G_{i-1}\\ | \\ G_i\end{array} & \leftarrow \left\{\begin{array}{l} G_{i-1}\lhd G \text{ and} \\ G_i/G_{i-1} = G(\mathbb{F}_{i-1}/\mathbb{F}_i)\end{array}\right. \\
 & \vdots & & \vdots & \\
 & \mathbb{F} & & G(\mathbb{L}'\hat{\mathbb{L}}/\mathbb{F}) &
\end{array}$$

Now consider

$$\begin{tikzcd}
 & \mathbb{L}'\hat{\mathbb{L}} \arrow[dl, dash] \arrow[dd, dash, "\leftarrow \text{Galois with solvable Galois group } G = G(\mathbb{L}'\hat{\mathbb{L}}/\mathbb{F})"] \\
(\mathbb{L}'\hat{\mathbb{L}})^N = \mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x)) & \\
 & \mathbb{F} \arrow[ul, dash]
\end{tikzcd}$$

Galois, so $N \trianglelefteq G$ and Galois group G/N

It only remains to prove this LEMMA: G a finite solvable group, $N \trianglelefteq G$
$\Rightarrow$ G/N solvable.

proof: The subgroup tower

$$\{1\} = G_0 \lhd G_1 \lhd \dots \lhd G_{i-1} \lhd G_i \lhd \dots \lhd G_r = G \text{ with } G_i/G_{i-1} \text{ cyclic}$$

leads to a tower

$$N = \bar{G}_0 \lhd \bar{G}_1 \lhd \dots \lhd \bar{G}_{i-1} \lhd \bar{G}_i \lhd \dots \lhd \bar{G}_r = G/N \text{ where } \bar{H} := HN/N$$
having $\bar{G}_i/\bar{G}_{i-1}$ cyclic

once we check ~~two~~ three things:

(i) $N \lhd HN < G$ (so that $\bar{H} := HN/N$ makes sense as a quotient group)
This is an easy exercise using $N \lhd G$, so $hN = Nh$ $\forall h \in H$
and $HN = NH$

(ii) $K \triangleleft H < G \Rightarrow \underset{KN/N}{\overline{K}} \triangleleft \underset{HN/N}{\overline{H}}$. This is because $K \triangleleft H \overset{\text{easy}}{\Rightarrow} KN \triangleleft HN$
$\overset{\text{easy}}{\Rightarrow} \underset{\overline{K}}{KN/N} \triangleleft \underset{\overline{H}}{HN/N}$

(iii) H/K cyclic, say generated by hK

$\Rightarrow \overline{H}/\overline{K}$ is also cyclic, generated by $\left(hN/N\right)\cdot\left(KN/N\right)$ (!)

$\overline{H}/\overline{K} = HN/N \,/\, KN/N$ (This becomes easier to deal with notationally if one first checks Noether's 3rd/4th isomorphism thm. saying for $N \triangleleft K \triangleleft H < G$,

$$(H/N)/(K/N) \cong H/K$$
via $hN\cdot(K/N) \leftarrow hK$) ∎

To complete the story of why there is no "quintic formula":

PROPOSITION: A_5 is a simple group (no normal subgroups except $\{1\}, A_5$)
so not solvable,
and hence neither is S_5 solvable.

(REMARK: But A_4, S_4 are solvable: we saw $\{1\} \underset{2}{\triangleleft} C_2 \underset{2}{\triangleleft} V_4 \underset{3}{\triangleleft} A_4 \underset{2}{\triangleleft} S_4$)

(REMARK: ~~Prop~~ actually true for A_n, S_n with $n \geq 5$; see THM 7.5.4 in Artin)

proof: A_5 has $|A_5| = \frac{5!}{2} = 60$ and conjugacy class sizes

	size
$\{e\}$	1
$\{(12)(34)(5),\ldots\}$	15
$\{(123)(4)(5),\ldots\}$	20
$\{(12345),\ldots\}$	12
$\{(12354),\ldots\}$	12
	60

and a normal subgroup N with $\{1\} \subsetneq N \subsetneq A_5$ would require 1 plus some of the others to add to $|N| < 60$ dividing 60, which one can see is impossible.

S_5 can't be solvable else one would have some $N \underset{\neq}{\triangleleft} S_5$, $N \not\supseteq A_5$ and S_5/N cyclic but this would give $N \cap A_5 \underset{\neq}{\triangleleft} A_5$ and hence $N \cap A_5 = \{1\}$ with $A_5 \cong A_5/N\cap A_5$ a subgroup of S_5/N. This is impossible since A_5 is not abelian, but S_5/N is cyclic ∎