Insolvability of Quintic - Prelim

Def) let G a finite grp.

A composition series for G is a chain of subgps

$$1 = H_0 \subsetneq H_1 \subsetneq \cdots \subsetneq H_n = G$$

s.t. H_i normal in H_{i+1} & max'll among normal subgrps.

Obs) these exist by finiteness & rinse & repeat! (not

Warning) not unique! There are 2 for $\mathbb{Z}/6$

$$1 \subseteq \mathbb{Z}/2 \subseteq \mathbb{Z}/6 \quad \text{or} \quad 1 \subseteq \mathbb{Z}/3 \subseteq \mathbb{Z}/6$$

Obs) The comp series H_i / H_{i-1} is a simple group (no normal subgrp except trivial & all)

Jordan Holder Thm) let $1 = H_0 \subset \cdots \subset H_n = G$

$1 = H_0' \subset \cdots \subset H_m' = G$

two comp series

$\Rightarrow$ 1) $n = m$

2) $\exists \sigma \in S_n$ so $H_i / H_{i-1} \cong H'_{\sigma(i)} / H'_{\sigma(i)-1}$

some uniqueness result

Def) These H_i / H_{i-1} are the jordan holder constituents.

n is the " " length

E.g.) 1) If G is simple, it is only J-H const (length 1)

2) $G = S_5$ has length 2 consts are A_5, $\mathbb{Z}/2$

3) $G = S_3$ has lenght 2 const are $\mathbb{Z}/3 = A_3$, $\mathbb{Z}/2$

4) $G = S_4$ $V = \{1, (12)(34), (13)(24), (14)(23)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$

V is normal subgrp of A_4

$\Rightarrow 1 \subseteq \mathbb{Z}/2 \subseteq V \subseteq A_4 \subseteq S_4$

has len 4 consts $\mathbb{Z}/2, \mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/2$

Defn| G is solvable if its J-H comps are $\mathbb{Z}/p\mathbb{Z}$'s (for varying primes p)

E.g.| S_2, S_3, S_4 solvable, S_5 not solvable.

Prop| (permanence prop of soln) (finite)

a) A sub or quot of solvable is solvable.

b) An extension of solvable grp is solvable.
If G has normal subgrp N so N, G/N solvable
$\Rightarrow$ G is solvable.

c) product of solvable is solvable.

Pf sk| Say G is solvable & so $G \twoheadrightarrow G'$

let $1 = H_0 < \cdots < H_n = G$ chain for G

$1 = H_0' < \cdots < H_n' = G'$ let $H_i' =$ img of H_i in G'

$\underbrace{H_0' < \cdots < H_n'}_{\text{not nec strict}}$

$H_i / H_{i-1} \to H_i' / H_{i-1}'$

$\mathbb{Z}/p$ ... being triv or $\mathbb{Z}/p$

$\Rightarrow$ deleting duplicates gives comp series!

Sub similar

2) If N, G/N solvable have

$1 = H_0 < \cdots < H_r = N$

$1 = \overline{H}_r < \cdots < \overline{H}_s < G/H$

let inv img of $\overline{H}_i$ in G $\Rightarrow$ get com series in G

3) $b \Rightarrow c$.

$\Rightarrow$ abelian $\Rightarrow$ simple!

Defn) Let F be a field. Let Ω = alg closure $\alpha \in \Omega$

We can say α can be expressed w/ radicals, if $\exists$ tower of fields

so $F_1 = F(\text{roots of } 1)$

$F_n = F_{n-1}(n^{th} \text{ roots of something in } F_{i-1})$ $i \geq 2$

↳ n allowed to vary.

$\alpha \in F_r$.

$$\begin{array}{c} \Omega \\ | \\ F_r \\ \vdots \\ | \\ F_2 \\ | \\ F_1 \\ | \\ F \end{array}$$

Defn) A polynomial $f \in F[x]$ is solvable in radicals if its roots can be expressed w/ radicals.

Thm) Let f be a polynomial w/ gal grp G ↳ Gal grp of split. field

TFAE:

1) G is solvable
2) G is a solvable grp.

Pf) b $\Rightarrow$ a (work in fixed Ω)

E/F galois extn

Spse splitting field of f has solvable galois grp G.

Let $F' = F(\text{all } n^{th} \text{ roots of unity w/ } n \mid \text{ord } G)$

$$\begin{tikzcd} & E \cdot F' \arrow[dl, dash] \arrow[dr, dash] & \\ F' \arrow[dr, dash] & & E \arrow[dl, dash] \\ & F & \end{tikzcd}$$

↳ comps :- subfield of Ω gen'd by F', E.

↳ intersectn of normal is normal

$F' \cdot E / F$ is gal extn of F (also over F')

have a grp homo $\text{Gal}(F' \cdot E / F) \to \text{Gal}(F'/F) \times \text{Gal}(E/F)$

$\sigma \mapsto (\sigma|_{F'}, \sigma|_E)$

inj as F' & E gen $F'E$ so if id on those $\Rightarrow$ id on $F' \cdot E$

$\mathrm{Gal}(F'\cdot E/F') = \ker\big(\mathrm{Gal}(F'\cdot E/F) \to \mathrm{Gal}(F'/F)\big)$

$\Longrightarrow$ $\mathrm{Gal}(F'\cdot E/F')$ is isom to subgrp of $\mathrm{Gal}(E/F) = G$

$\Longrightarrow$ $\mathrm{Gal}(F'\cdot E/F')$ is solvable as $\underline{G \text{ is}}$!

note: $F'\cdot E$ = splitting field of $f(x)$ over F'

We may as well relabel now & assume, F contains nth roots of unity
↳ $\underline{n \mid \#G}$.

Since G solvable, $\Longrightarrow$ $\exists$ normal subgrp N
so $G/N \cong \mathbb{Z}/p\mathbb{Z}$

$$\text{gal grp } G\left\{\begin{array}{c} \left.\begin{array}{c} E \\ | \\ E^N \end{array}\right\} \text{Gal w/ } N \\ | \\ F \end{array}\right. \quad \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} \text{gal w/ grp } \mathbb{Z}/p$$

by last time, $E^N = F(a^{1/p})$ w/ $a \in F$

By continuing w/ normal subgrp in N

$\Longrightarrow$ everything in E expressible w/ radicals / E^N

As $E^N = F(a^{1/p})$, same true for $\underline{E/F}$.