Thm] $f \in F[x]$, E = splitting field
$G = Gal(E/F)$. TFAE
a) f solvable by rads
b) G is solvable.

Last time $b \Rightarrow a$

Pf] $a \Rightarrow b$.

K_n
$\vdots$
we know $\exists$ tower K_1 so $K_1 = F$ (roots of unity)
$|$
F

$K_n = K_{n-1}$ (a root from K_{n-1})

s.t. $E \subset K_n$

Idea, enlarge $K_n \to L_n$ to get smthn galois $/F$.
$\Rightarrow$ get surj $Gal(L_n/F) \twoheadrightarrow G$ (as quotient)
this will be solvable $\Rightarrow G$ solvable as

Let $L_1 = F$(roots of 1) $\to$ use all appearing roots in K_1
& d^{th} roots of 1 for all d of form $[K_i : K_{i-1}]$

$K_1 \subset L_1$

$K_2 = K_1[a^{1/d}]$ $a \in K_1$

Like eg
$\mathbb{Q}(\sqrt{a+b\sqrt{2}})$
$|$
$\mathbb{Q}(\sqrt{2})$
$|$
$\mathbb{Q}$

let L_2 = galois closure of $L_1[a^{1/d}]$ / F
$\Rightarrow K_2 \subset L_2$ & L_2/F galois.
K_1/F is Galois, L_2 will be $L_1((\sigma a)^{1/d})$ as σ varies in $Gal(L_1/F)$

So, $Gal(L_2, L_1) \subset \prod_{\sigma \in Gal(K_1/F)} \mathbb{Z}/d\mathbb{Z}$ its abelian **Key** *

$\therefore$ have SES,
$1 \to Gal(L_2/L_1) \to Gal(L_2/F) \to Gal(L_1/F) \to 1$
$Gal(L_2/L_1)$: abelian
$Gal(L_1/F)$: abelian as all are roots

$\Rightarrow Gal(L_2/F)$ solvable by persistence.

Rmk * if F is a field with all d^{th} roots of unity
$\Rightarrow E = F(\alpha_1^{1/d}, \dots, \alpha_n^{1/d})$
$\Rightarrow E/F$ galois & $\mathrm{Gal}(E/F) \subset (\mathbb{Z}/d\mathbb{Z})^n$

<u>Now</u>, keep going

$k_3 = k_2(b^{1/e})$, $b \in k_2 \subseteq L_2$

$L_3 =$ gal closure of $k_2(b^{1/e}) / F$
$= L_2((\sigma b)^{1/e})$ as σ varies in $\mathrm{Gal}(L_2/F)$

$\Rightarrow \mathrm{Gal}(L_3/L_2) \subseteq \prod \mathbb{Z}/e\mathbb{Z}$ & so abelian

$$1 \to \underbrace{\mathrm{Gal}(L_3/L_2)}_{\text{abelian}} \to \underbrace{\mathrm{Gal}(L_3/F)}_{\text{so solvable}} \to \underbrace{\mathrm{Gal}(L_2/F)}_{\text{solvable}} \to 1$$

& rinse & repeat $\Rightarrow \mathrm{Gal}(L_n/F)$ solv & so

as $E \subset k_n \subset \underbrace{L_n}_{gal}$ $\therefore$ $\mathrm{gal}(L_n/F) \twoheadrightarrow \mathrm{Gal}(E/F) = G$

<u>So G solv</u>

Thm (Abel-Ruffini)

$\nexists$ quintic <u>formula</u>. $\to$ <u>think of roots</u>

Pf $E = \mathbb{C}(\alpha_1, \dots, \alpha_5)$ rational <u>fun field</u>.

$S^5 \circlearrowright E$ by permuting α's

$F = E^{S_5} = \mathbb{C}(a_0, \dots, a_4)$

$f(t) = \prod_{i=1}^{5}(t - \alpha_i) = t^5 + \dots + ta_1 + a_0$ ~ universal quintic

$\mathrm{Gal}(E/F) = S_5$, not solvable

$\Rightarrow F$ not solvable by radicals

i.e. can't express α_i in a_i using just <u>radicals</u>.

Warning | This thm doesn't say anything abt specific quintics. Some will be solvable by radicals.

$\exists$ fields F st that every irreducible quintic / F solvable by radicals.

Ex | • $F = \mathbb{C}, \mathbb{R}$ (no irred quintics)

• $F = \mathbb{F}_q$ every finite extn is Galois w/ ab Gal gp

• $\mathbb{Q}_p$ every galois extn has solvable gal grp.

Over $\mathbb{Q}$ $\exists$ irred quintics not solvable by radicals.

Lemma | Let $f \in \mathbb{Q}[x]$ irred quintic with gal grp G.
Spse f has 3 real roots.
$\Rightarrow G = S_5$

Pf | as f irred, $G \leq S_5$ & is transitive.
Orbit-stab $\Rightarrow 5 \mid \# G$.
$\Rightarrow G$ contain 5-cycle (must have order 5 elt).
Let E be spl in $\mathbb{C}$, compl. conj restricts to $\sigma \in Gal(E/\mathbb{Q})$
σ fixes to 3 real roots & permutes complex conj
$\hookrightarrow$ transp.
$\Rightarrow$ transp + 5 cycle $\Rightarrow$ gen S_5

E.g | $f(x) = x^5 - 16x + 2$.
is an irred w/ 3 real roots! $\hookrightarrow$ not solvable by radicals

$\Longrightarrow$

Cor of Gen Thm: $\exists$ cubic & quartic formula.

Cubic: look $\mathbb{C}(\alpha_1, \alpha_2, \alpha_3) = E$

$$F = E^{S_3} = \mathbb{C}(a_0, a_1, a_2)$$

$$f(t) = \prod_{i=1}^{3}(t - \alpha_i) = t^3 + a_2 t^2 + \cdots + a_0$$

Gal(E/F) is gal w/ grp S_3 (solv)

$\Rightarrow \exists$ expr for α_1 in terms of a_0, a_1, a_2 using radicals

note: $1 \to A_3 \to S_3 \to \mathbb{Z}/2 \to 1$

let $K = E^{A_3}$

Gal w grp S_3

$$\begin{array}{cl} E & \\ | & \Big\} \text{ gal w } \mathbb{Z}/3 \\ K & \\ | & \Big\} \text{ gal w/ } \mathbb{Z}/2 \\ F & \end{array}$$

$K = F(\delta)$

$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$

$\delta^2 \in F$

let $\zeta = e^{2\pi i/3}$ $\quad x = \alpha_1 + \zeta \alpha_2 + \zeta^2 \alpha_3$ ~ eigen for gal aut

x^3 fixed by $A^3 \Rightarrow$ belongs to K.

$\Rightarrow E = K(x)$.