$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Q}$.

roots of p are $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$.

Want: $\alpha_i = b_1 + \sqrt[3]{b_2 - \sqrt[5]{b_3 + \sqrt[6]{b_6 - \sqrt{b_7}}}}$, $b_i \in \mathbb{Q}$.

(express α_i by radicals in terms of rationals.

$\{\omega : \omega^n = 1,\ n \in \mathbb{N}\}$ - roots of unity

Let F be the field generated by $\mathbb{Q}$ and roots of unity.

$b_7 \in F$, $F_1 = F(\sqrt{b_7})$ - field generated by F and $\sqrt{b_7}$,
extension of F by $\sqrt{b_7}$.

$F_2 = F(\sqrt[6]{b_6 - \sqrt{b_7}})$

We get a tower of "radical extensions"

$$\begin{array}{c} F_k \supset K \\ | \\ \vdots \\ | \\ F_2 \\ | \\ F_1 \\ | \\ F \end{array}$$

s.t. $\forall i$, $F_{i+1} = F_i(\sqrt[m_i]{c_i})$

where $c_i \in F_i$.

The goal is to find such a tower that contains all α_i,

and so containing $F(\alpha_1, \dots, \alpha_n)$ – field generated by α_i.
$$\underset{K}{\overset{\|}{}}$$

Note: $F(\sqrt[n]{c})$ contains all n^{th} roots of c:

$$\beta^n = c \Rightarrow \{\text{all roots of } c\} = \{\omega\beta, \omega^2\beta, \dots, \omega^{n-1}\beta, \beta\}$$

where $\omega = \sqrt[n]{1} = e^{2\pi i/n}$

$z \mapsto \bar{z}$ permutes roots of -1.

If K is an extension of F, the group

$$\mathrm{Aut}(K/F) = \{\varphi \in \mathrm{Aut}(K) : \varphi|_F = \mathrm{Id}_F\}$$

is the <u>Galois group</u> of the extension.
$\mathrm{Gal}(K/F)$

If K is generated by roots of a pol-l f, then $\mathrm{Gal}(K/F)$ is a subgroup of the group of permutations of the roots of f.

Since any such aut-sm is uniquely defined by its actions on generators.

For $K = F(\sqrt[n]{c})$, $Gal(K/F)$ is cyclic.

Fundamental Galois Thm: if K/F is "good", then

Subfields of K containing F are in 1-1 correspondence w/ subgroups of $Gal(K/F)$.

if $F \subseteq E \subseteq K$, then $Gal(K/E) \leq Gal(K/F)$

$$\begin{array}{l} K \\ E \\ F \end{array} \quad G$$

If $Gal(K/E) \trianglelefteq Gal(K/F)$, then

$$Gal(E/F) = Gal(K/F) / Gal(K/E)$$

K is contained in a tower of radical extensions iff $Gal(K/F)$ is a quotient group of a solvable tower of cyclic groups iff $Gal(K/F)$ is solvable.

solvable, so P is solvable in radicals

$\deg P = 4 \Rightarrow Gal \leq S_4$

S_3: $1 \triangleleft \mathbb{Z}_3 \triangleleft S_3$ $\quad S_3/\mathbb{Z}_3 = \mathbb{Z}_2$

$S_4: \quad 1 \trianglelefteq \underset{\mathbb{Z}_2}{} \mathbb{Z}_2 \trianglelefteq \underset{\mathbb{Z}_2}{} V_4 \trianglelefteq \underset{\mathbb{Z}_3}{} A_4 \trianglelefteq \underset{\mathbb{Z}_2}{} S_4$

S_5: not solvable.

<u>Field</u>: Integral domain w/ $R^\times = R \setminus \{0\}$.

eg $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \quad F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F(x),\ q(x) \neq 0 \right\}$

no nontrivial ideals, so no factor fields

$\forall$ field hom-sm is injective (Kernel is an ideal, & $1 \mapsto 1$ so $\ker = 0$).

<u>Prime subfield</u>: subfield generated by 1

$\hookrightarrow$ it's either $\underbrace{\mathbb{Z}_p}_{\text{Characteristic} = p}$ or $\underbrace{\mathbb{Q}}_{\text{characteristic} = 0}$.

If F is a subfield of K, K is an extension of F,

also we write K/F or $\begin{array}{c} K \\ | \\ F \end{array}$.

Tower of extensions $K_1/K_2/K_3/\dots/K_n$ or $\begin{array}{c} K_1 \\ | \\ K_2 \\ | \\ \vdots \\ | \\ K_n \end{array}$

Composite of two ...

extensions: K/F

Subextensions K_1/F, K_2/F s.t. $K_1, K_2 \subseteq K$.

Then composite K_1K_2/F is minimal $\underbrace{\text{subfield}}_{\text{subextension}}$ of K/F containing both K_1 & K_2.

$$
\begin{tikzcd}[column sep=small]
 & K \arrow[d, dash] & \\
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \text{minimal} \arrow[l] \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & K_1 \cap K \arrow[d, dash] & \\
 & F &
\end{tikzcd}
$$