Recall a finite group $G$ is solvable if there exists a sequence of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \{e\}$$

where $G_{i+1}$ is normal in $G_i$ and $G_i / G_{i+1}$ is abelian for each $i$.

**Theorem 5.3.8** Let $G^{(0)} = G$, and

$$G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

Then $G = G^{(0)} > G^{(1)} > G^{(2)} > \cdots$
$G$ is solvable $\iff G^{(n)} = \{e\}$ for some $n$.

Def: A group $G$ is perfect if $G = [G, G]$.

Example: $A_5$ is perfect.

Thm 5.3.9: The symmetric group $S_n$ is not solvable for $n \geq 5$.

Proof: Let $H \leq S_n$ be a subgroup containing all 3-cycles.
Claim the same is true of $H' = [H, H]$.

Let $\sigma = (i, j, k) \in H$

$\tau = (i', k', l) \in H$

$\rho = (k, i, m) \in H$

with $i, j, k, l, m$ distinct.

$\sigma = [\tau \rho] \text{ (exercise)}$

Hence $H'$ contains all 3-cycles.

Suppose $H = S_3$. Then $S_3'$ also contains all 3-cycles.
Let $G_i = S_m$

Then $G_i^{(i)}$ as defined above contains all 3-cycles for any $i$.

Hence no $G_i^{(i)}$ is trivial, so $S_m$ is not solvable by 5.3.8.

QED

Thm 5.3.10 Let $G_i$ be solvable. Then any subgroup or quotient $G_j$ of $G_i$ is also solvable.
pf: (1) Let \( H \subseteq G \). Can show by induction on \( i \) that \( H(i) \subseteq G(i) \).

If \( G(n) = \exists H \subseteq G \) for some \( n \), let \( H(n) \) be solvable by 5.3.8.

(2) Let \( \phi: G \to M \) be onto, so \( M \) is quotient of \( G \). Can show \( M(i) \subseteq \phi(G(i)) \). To do this, let \( x, y \in G(i) \) with \( \phi(x) = u \) and \( \phi(y) = v \).

\[ [u, v] = [\phi(x), \phi(y)] = [x, y] \in G(i) \]

\[ \phi([x, y]) \in \phi(G(i+1)) \]
Theorem 5.3.11
Let \( H \) be a normal subgroup of \( G \). Then \( G \) is solvable \( \iff \) \( H \) and \( G/H \) are solvable.

Proof \( \Rightarrow \) in 5.3.11
(\( \Leftarrow \)) Assume \( H \) and \( G/H \) are solvable.
\[ H = H_0 \supset H_1 \supset \cdots \supset H_m = \{ e \} \]
\[ G/H = G_0/H \supset G_1/H \supset \cdots \supset G_m/H = \{ e \} \]
Then \( G_i / G_{i+1} = (G_i / H) / (G_{i+1} / H) \)
\( = \text{abelian} \)

(Theorem 5.1.8 third use, then 3.4.7 in Fraleigh)

Hence we have

\[ G = G_0 > G_1 > G_2 > \ldots > G_m = H_0 > H_1 > \ldots > H_m = \{e\} \]

This makes \( G \) solvable. QED
How to solve polynomial equations of low degree

\[ f(x) = x^2 + bx + c \]

The zeroes are \[ x = -\frac{b \pm \sqrt{b^2 - 4c}}{2} \]

let \( \Delta = b^2 - 4c = \text{discriminant} \)

The splitting field is \( \mathbb{Q}(\sqrt{\Delta}) \) if \( \sqrt{\Delta} \in \mathbb{Q} \) then \( E = \mathbb{Q} \) and \( G = \text{Gal} \left( E / \mathbb{Q} \right) = \{ e \} \)

Otherwise, \( G_1 = G_2 = S_2 \)
Cubic case

\[ f(x) = x^3 + ax^2 + bx + c = g(y) \]

Let \( y = x - a/3 \)

\[ y^3 = x^3 - ax^2 + \frac{a^2}{3}x - \frac{a^3}{27} \]

Can replace \( f(x) \) by \( g(y) = y^3 + py + q \) \( \chi, \psi \in \mathbb{Q} \)

Let \( \chi_1 = \left( \frac{\psi}{2} \right)^2 + \left( \frac{\chi}{3\chi} \right)^2 \in \mathbb{Q} \)

\[ \chi_2 = \chi_1 - \frac{\chi}{2} \in \mathbb{Q}(\chi_1) \]

\( \omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}}{2} \)
There is a formula for the zeros of \( f(x) \) involving these quantities. They are \( u + v \), \( uv + vv + uu \), \( uv + v^2 + uw \), where \( u = \alpha_2 \) and \( v = -b/3m \).

In terms of fields we have

\[
K_0 \subset K_1 \subset K_2 \subset K_3
\]

\[
\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset \mathbb{Q}(\alpha_1, \alpha_2) \subset \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)
\]

\( K_3 \) is the splitting field.
If \( f(x) \) is irreducible,
$G$ is either $S_3$ or $A_3 \cong C_3$.

Quartic case

$f(x) = x^4 + ax^2 + bx + c$

blah blah blah

There is a formula in terms of radicals

If $f(x)$ is irreducible, then

$G \cong C_4, \ D_4, \ A_4, \ S_4, \ or \ C_2 \times C_2$

$A_4$ and $S_4$ only occur when $b \neq 0$. 
They are all solvable.

Def 12.5.5 F is a simple radical extension if

\[ K = F(p) \text{ with } p^n \in F \text{ for some } n. \]

A radical tower is

\[ F = K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_m, \quad K_m = \text{top of tower} \]

where \( K_{i+1} \) is a simple radical extension of \( K_i \).
$F \subset K$ is an extension by radicals if $K$ is the top of a radical tower. 
If $\Delta \in F[x]$ is solvable by radicals if its splitting field $K$ is a radical extension of $F$.

Example:

$S_5 = e^{2\pi i/5} = \sqrt[5]{1} - i \sqrt[5]{\frac{\sqrt{5}}{2}}$