Main Thm 12.5.18. A polynomial $f(x) \in F[x]$ is solvable by radicals if
$\Rightarrow G_i = \text{Gal}(E/F)$ is solvable, where $E$ is the splitting field of $f$.
Recall $G$ is solvable if it has subgroups of the form
$G_i = G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$
where $G_i$ is normal in $G_{i+1}$ and $G_i / G_{i+1}$ is abelian.

Homework exercise: If $G$ is solvable,
The \( G_i \) can be chosen so that each
\( G_i / G_{i+1} \cong \mathbb{Z}_p \) for some prime \( p \).

We want to study Galois extensions
with \( \mathbb{Q} \mid \mathbb{Q} \).

Prop 12.5.14 Suppose \( F \) contains a
primitive n-th root of unity \( S \) and
\( E \) is a Galois extension with
\( G = \text{Gal} (E / F) = C_n \). (Kummer extension)
Then \( E = F[\sigma] \) with \( \sigma^n \in F \).

If let \( x \in E \) not in \( F \) and let
Let \( \sigma \) be a generator of \( G \). Let
\[
g(\alpha) = \sum_{i=0}^{n-1} \sigma^i \delta^i(\alpha) = \alpha + \sigma \delta(\alpha) + \sigma^2 \delta^2(\alpha) + \cdots
\]
We will show that \( \sigma \) is the \( \sigma \) we are looking for.

\[
s(g(\alpha)) = \sigma(\alpha) + \sigma^2 \delta(\alpha) + \sigma^3 \delta^2(\alpha) + \cdots + \sigma^{n-1} \delta^n(\alpha)
\]

\[
= \sigma^{-1} \alpha + \sigma^{-1} (\sigma \delta(\alpha)) + \sigma^{-1} (\sigma^2 \delta^2(\alpha)) + \cdots
\]

\[
= \sigma^{-1} (g(\alpha))
\]

i.e. \( g(\alpha) \) is an eigenvector (over \( \mathbb{F} \)) for \( \sigma \) with eigenvalue \( \sigma^{-1} \).
\[ \sigma (g(\alpha)^n) = (\sigma g(\alpha))^n = g(\alpha)^n \]

Hence \( g(\alpha)^n \in F \)

\( g(\alpha) \) is not fixed by any nontrivial endomorphism of \( G \), so it does not lie in any proper subfield. It is the field we are looking for. \( \text{QED} \)

Let \( m \in G \) be the product of all primes dividing \( |G| \). Suppose \( F \) contains a primitive \( m \)-th root of unity. Then if \( G \) is solvable, \( F \) is the
top of a radical tower

Let \( G_1 = G_0 \supset G_1 \supset \cdots \supset G_m = \mathbb{Q} \) as before

and let \( F = F_0 \subset F_1 \subset \cdots \subset F_m = E \)

be the corresponding tower of fields. Then \((F_i : F_{i+1}) = G_i : G_{i+1} \cong C_p\) and \(E/F\) (and hence \(E_i\)) contains \( p \)th roots of \( 1 \).

By 12.5.14, \( F_{i+1} \) is a simple radical extension of \( F_i \), QED

We need to get around this demand on \( F \).
Auxiliary corollaries to Lemma 12.5.8

\[ G' = \text{Gal}(E'/F') \]
\[ G = \text{Gal}(E/F) \]
\[ f(x) \in F[x], \quad E \text{ is its splitting field} \]
\[ E \subseteq F'[x], \quad E' \]

Then there is a 1-1 homomorphism \( G' \rightarrow G \).

**Proof:** Let \( \alpha_1, \alpha_2, \ldots, \alpha_k \) be the roots of \( f(x) \).

Then \( E = F(\alpha_1, \ldots, \alpha_k) \)
\[ E' = F'(\alpha_1, \ldots, \alpha_k) \]

\( G \) and \( G' \) permute the \( \alpha_i \) and
in $G'$ in either $G$ which fixes each $x_i$ is the identity.

Let $g \in G'$. Consider $x = \sum a_i x_i$ with $a_i \in F$

$g(x) = \sum a_i g(x_i) \in E$

Any $x \in E$ can be written in this way, so $g : E \rightarrow E$ and we have a restriction hom $G' \rightarrow G$.

Since $g$ is determined by its action on the $x_i$s, the hom is 1-1. QED
Theorem 12.4.112. If $F'$ is obtained from $F$ by adjoining some roots of unity, then $\text{Gal}(F'/F)$ is abelian and the extension is radical.

Example. $F = \mathbb{Q}$, $F'$ obtained by adjoining all $\sqrt[n]{1}$ with roots of unity.

$G_1 = \text{Gal}(F'/F) = \mathbb{Z}/n \times \mathbb{Z}/n$

$= \mathbb{Z}/n$ of order $\phi(n)$

$|G_1| = \# \text{ of integers } 0 < k < n$

with $(k, n) = 1$. 
Let $G = e^{2\pi i/n} = \text{primitive } n\text{-th root of } 1$ and $\mathbb{k} \subseteq (\mathbb{Q}/n)^*$.

E.g., $n = 3$, $F' = \mathbb{Q}(-\sqrt{3})$

$n = 5$, $F' = \mathbb{Q} \left( \sqrt{5}, \sqrt{-1 + \sqrt{5}} \right)$

Let $m = \text{product of all primes dividing } 161$

\[ G' = \text{Gal} \left( E' / F' \right) \]
\[ F' = F \text{ (with roots of unity)} \]
\[ E' = E \]
\[ G' \text{ is solvable because it is a subgp of } G. \]

By the Corollary, \( E' \) is a radical extension of \( F' \).

Let \( \tilde{G} = \text{Gal}(E'/F) \) and \( H = \text{Gal}(E'/F) \).

We know (why?) that \( H \) is a normal subgroup of \( \tilde{G} \) and that \( \tilde{G}/H = G' \).

Hence \( G' \) is solvable.

Since \( E' \) is a radical extension of \( F' \),
and $F'$

$E'$ is a radical extension of $F$.

This means $f(x) = 0$ can be solved by radicals.

This proves one implication ($\leq$)

of the main theorem.

Next time we will prove $\Rightarrow$. 