Main Theorem 12.5.18 Let \( f(x) \in F[x] \)
where \( F \) has characteristic 0. Let \( E \) be the splitting field for \( f(x) \) and \( G = \text{Gal}(E/F) \). Then \( f(x) = 0 \) is solvable by radicals \( \iff G \) is solvable.

Sketch of proof: \( \Rightarrow \) (easy part)
If \( f(x) \) is solvable by radicals then there is a radical tower
\( F = K_0 \subset K_1 \subset \cdots \subset K_n = E \)

where \( K_{i+1} \) is a simple radical extension of \( K_i \) of degree \( d_i \).

Assume \( F \) contains \( d_i \) th roots of unity \( \zeta_i \). We know that each \( K_{i+1} \) is a cyclic extension of \( K_i \), i.e., \( K_{i+1} \) is Galois over \( K_i \) with \( \text{Gal} (K_{i+1}/K_i) = \mathbb{Z}/d_i\mathbb{Z} \). This means \( G \) is solvable.
About our assumption. If $F$ does not contain the required roots of unity, let $F'$ be the field obtained from $F$ by adjoining them.

Let $E'$ be the field similarly obtained from $E$. Can show $E'$ is the splitting field of $f(x)$ over $F'$.
Will show $F'$ and $E'$ are Galois extensions of $F$ and $E$ with abelian Galois groups $H$ and $H'$, $G'$ is solvable for the reasons given above. Let $\tilde{G} = \text{Gal}(E'/F)$. We can show $H$ is normal in $\tilde{G}$ and $\tilde{G}/H = G'$. This means $\tilde{G}$ is solvable. $G'$ is normal in $\tilde{G}$ with $\tilde{G}/G' = H'$. Hence $G'$ is solvable. \[\text{(Harder)}\]. Assume $G'$ is solvable.
This means there are subgps
\[ G_i = G_{i-1} > G_{i-1} > G_{i-2} > \cdots > G_0 = \{e\} \]
where \( G_{i+1} \) is normal in \( G_i \) and
\[ G_i / G_{i+1} \cong C_p \text{ for a prime } p. \]
Can show \( G' \) is a subgroup of \( G \)
and therefore solvable. It has
subgps
\[ G'_1 = G'_0 > G'_1 > \cdots > G'_m = \{e\} \]
where \( G'_{i+1} \) is normal in \( G'_i \) with
\[ G'_i / G'_{i+1} \cong C_p \text{ for some prime } p. \]
Hence there are fields
\[ F' = K_0' C K_1' C \ldots C K_n' = E' \]
where \( \text{Gal} (K_{i+1}' / K_i') = C_2 \).

This means \( K_{i+1}' \) is a simple radical extension of \( K_i' \), i.e. \( K_{i+1}' = K_i' (\sqrt{i}x) \) for some \( x \in K_i' \). This means \( F' \to E' \) is a radical tower \( f(x) \) can be solved by radicals over \( F' \). This proves the Thm assuming
That $F'$ and $E'$ are abelian radical extensions of $F$ and $E$.

What happens when we adjoin roots of unity in char 0?

Example

\[ \mathbb{Q}(\zeta^{1/3}) = \mathbb{Q}(\sqrt[3]{3}) \]
\[ \mathbb{Q}(\zeta^{1/4}) = \mathbb{Q}(\sqrt[4]{5} + \sqrt[4]{5}) \]

for $a, b \in \mathbb{Q}$.

\[ \mathbb{Q}(\zeta^{1/4}) = \mathbb{Q}(\sqrt[4]{5}) \]
Def. The \( n \text{th cyclotomic polynomial} \) is defined as:

\[
\Phi_n(x) = \prod (x - \alpha_i^k) \quad \text{where} \quad \alpha_i = \frac{e^{2\pi i / n}}{x}
\]

\( \alpha_i^k \) are the primitive \( n \text{th roots} \) of unity.

\[
\Phi_2(x) = x + 1
\]

\[
\Phi_3(x) = x^2 + x + 1 = (x - e^{\frac{2\pi i}{3}})(x - e^{\frac{4\pi i}{3}})
\]

\[
\Phi_4(x) = (x + i)(x - i) = x^2 + 1
\]

\[
\Phi_5(x) = x^4 + x^3 + x^2 + x + 1
\]

Let \( K_n = \mathbb{Q}[x] / \langle \Phi_n(x) \rangle \)

\( K_n \) is the field obtained from \( \mathbb{Q} \).
adjoining $m$ roots of unity

Thm 12.4.10 \( K_m = \mathbb{Q}(\alpha) \)
and \( G_m = \text{Gal}(K_m/\mathbb{Q}) = (\mathbb{Z}/m)^* = U(m) \)

= gp of integers \( k \) with \( 0 < k < m \)
with \( \gcd(k, m) = 1 \) under multiplication.

\( m = 10 \quad G_{10} = \{ 1, 3, 7, 9 \} \) under mult
\( 3^2 = 9 \quad 3^3 = 7 \) mod 10
\( \cong C_4 \)

\( m = 8 \quad G_8 = \{ 1, 3, 5, 7 \} \cong C_2 \times C_2 \)
If we choose a primitive n-th root, say $\zeta = e^{2\pi i/n}$, for each $K \subseteq \mathbb{Q}$, we have a field automorphism $s \mapsto s^\zeta$. This leads to an isomorphism between $\text{Gal}(K_n/\mathbb{Q})$ and $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Q.E.D.

Why is the extension radical? e.g. $n = \text{prime}$: $\text{Gal}(K_n/\mathbb{Q}) = C_{p-1}$

Let $\mathbb{Q}(\sqrt[4]{1})$
\[ E' = K_{p_1} \left( \sqrt[p_{h-1}]{u} \right) \]

\[ \text{Gal} (E'/F') = C_{p_{h-1}} \],

E' is a simple radical extension of F'.

\[ e.g. \quad n = 100 = 4 \cdot 25 = 2^2 \cdot 5^2 \]

\[ |G| = \phi(100) = \phi(4) \phi(25) = 2 \cdot 20 = 40 \]

\[ G \cong C_2 \times C_{20} \]

To get a simple radical extension we need a ground field with
the roots of unity

\( G_2 = G_0 \supset G_1 \supset G_{12} \supset G_{112} \supset G_{1112} \)

\( C_{2 \times 20} \supset C_{20} \supset C_{10} \supset C_5 \supset \mathbb{Q} \)

\( F = K_0 \supset K_1 \supset K_2 \supset K_3 \supset K_4 \)

\( \mathbb{Q}(\sqrt{-1}) \supset k_0(\sqrt{2}) \supset k_1(\sqrt{2}) \supset k_2(\sqrt{2}) \supset k_3(\sqrt{2}) \)

radical by induction

\( \mathbb{Q} \)