Main Theorem (12.5.18) Let $F$ be a field of char $0$, $f(x) \in F[x]$, $E$ the splitting field for $f(x)$, $G = \text{Gal}(E/F)$. Then the equation $f(x) = 0$ is solvable by radicals $\iff G$ is solvable.

Proof $\Rightarrow$ Being solvable by radicals means that $E$ is contained in $K$ which is a radical extension.
of $F$.

Note: a radical extension need not be Galois, e.g. $\mathbb{Q}(\sqrt[3]{2}) = E$ is not a Galois extension of $\mathbb{Q}$, since the Galois group is trivial. If we adjoin cube roots of unity to $F$ and $E$ to get fields $F'$ and $E'$, then $E'$ is a Galois extension of $F'$ with Galois group $C_3$. 
We have
\[ F \xrightarrow{\text{radical}} E \xrightarrow{\text{radical}} K \]
Then \( \text{Gal}(E/F) = \text{Gal}(L/E)/\text{Gal}(L/F) \)
in solvable. QED for \( \Rightarrow \)

\[ \Rightarrow \] Assume \( G = \text{Gal}(E/F) \) is solvable
Let \( n = |G| \). Let \( F' \) and \( E' \) be the fields obtained from \( F \) and \( E \)
by adjoining all nth roots of unity.

By 12.5.8, $G'$ is isomorphic to a subgroup of $G$, and therefore solvable.

$\text{Rad}(F'/F) = \text{Rad}(E'/F)/\text{Rad}(E'/F')$

5/3/11 says that if $N \triangleleft G$ and
both $H$ and $G/H$ are solvable, then $G$ is solvable. Hence $Gal(E'/F)$ is solvable.

We have a chain of subgroups

$$\mathfrak{End}^s = G_m \leq G_{m-1} \leq G_{m-2} \leq \cdots \leq G_1 = G'$$

with $G_{i+1}$ is normal in $G_i$ with $G_i/G_{i+1} = \mathfrak{F}_p$ for $p$ prime with $p \mid m$. Using FTGT we get a chain of fields

$$F_1 = F_0 \leq F_1 \leq E \leq \cdots \leq F_m = E'$$
where each extension is cyclic of prime degree. Since $E'$ contains $p$th roots of unity, each of these extensions is a simple radical one. Hence $E'$ is a radical extension of $F$. Hence $E'$ is a radical extension of $F$ containing $E$. This means $f(x) = 0$ is solvable by radicals (QED).
For (D) we need

**Theorem 12.5.16:** Given F, E and K as above, we can find L with the indicated properties.

This can be derived from

**Lemma 12.5.14**

If the hypothesis with K a simple radical extension of E, same conclusion.
3. Cyclotomic extensions

Let \( \mathbb{Q} \subset K_n \) be a field obtained by adjoining all \( n \)th roots of unity.

1) \([K_n : \mathbb{Q}] = \phi(n)\)
   
   \[ k \leq n \quad \text{with} \quad d \mid n \quad \text{and} \quad \gcd(k, n) = 1 \]

2) \(K_n\) is splitting field for
   
   \[ \Phi_n(x) = \prod_{0 \leq k < n} (x - \zeta_m^k) \quad \text{where} \quad \zeta_m = e^{2\pi i / n} \]
If \( n = p^i \) then, \( \Omega(n) = (p-1) p^{i-1} \)

and \( \Phi_n(x) = \frac{x^{p^i} - 1}{x^{p^i-1} - 1} = 1 + x^{p^i-1} + x^{2(p^i-1)} + \ldots + x^{(p-1)p^{i-1}} \)

3) \( \Omega(n) = \left( \frac{\mathbb{Z}}{n} \right)^x \) multi group of units in the ring \( \mathbb{Z}/n \)

with \( S_n \rightarrow S_n \)

4) \( K_n \) is a radical extension of \( Q \).
Side notes

a) A regular \( n \)-sided polygon is constructible if with \( R + C \leq \n \) is a power of \( 2 \).

\[ \Phi(17) = 16 = 2^4 \]
\[ \Phi(7) = 6 \neq 2^i \]

A heptagon is not constructible.

b) (?) A regular \( n \)-gon is constructible if

\[ \Phi(n) = 2^i \cdot 3^j \]
c) "Sneakers theorem" due to Kronecker.

Let $E$ be an abelian extension of $\mathbb{Q}$. Then $E$ is a subfield of some $\mathbb{Q}( \sqrt[n]{1})$. 