In 12.5.16 we have not discussed \( \implies \). Will discuss \( \Leftarrow \).

Let \( n = |G| \) on the product of all primes dividing \( G \).

Apply 12.5.8 to

\[
\begin{align*}
\mathbb{Q}& \to \mathbb{Q}^{	ext{radical}} \to E' \\
\text{abelian} & \to \text{radical} \to \text{splitting fields} \\
G & \to E
\end{align*}
\]

\( G' \) is solvable because \( G \) is.

Every prime dividing \( |G'| \) also
divides n. $G'$ has a nested sequence of subgroups, in which each $G_i'/G_{i-1}' = G_i$. For some prime $p|n$. Hence we have $E' = K'_m \supset K'_{m-1} \supset \cdots \supset K_0' = F'$. $k'_i = (E')^{G_{k_i}}$. Each extension (by (2.4.15)) is a simple radical extension. Hence $E'$ is a radical extension of $F'$. Since $F'$ is a radical extension of $F$, $f(x)$ can be solved by radicals.
Thm 12.4.10 The extension $Q \to Q(\sqrt[n]{1})$ is an abelian radical extension.

Proof later.

Assuming this is true, apply 12.5.8 to

$$
\begin{array}{c}
F \\
\downarrow \\
A'
\end{array} \quad F' = F(\sqrt[n]{1}) \quad \text{splitting fields for} \quad \mathbb{Q}(\sqrt[n]{1}) \\
\downarrow \\
\mathbb{Q} \\
\downarrow \\
A = \text{abelian} \quad Q(\sqrt[n]{1}) \\
\downarrow \\
\mathbb{Q}(\sqrt[n]{1}) \quad \Phi_n(x)
\end{array}
$$

$A = \text{Rad}(Q(\sqrt[n]{1})/\mathbb{Q})$ is abelian by 12.4.11.

$A'$ is a subgroup of $A$ so $A'$ is abelian.
Hence

\[ E'(\sqrt[n]{D}) \rightarrow F \]
\[ \text{radical} \quad \rightarrow \quad E' \]
\[ A' \quad \text{radical} \quad \rightarrow \quad E \]
\[ F \quad \rightarrow \quad E \]

\[ \{ \text{splitting fields of } \beta(x) \in F[x] \} \]

\[ E' \text{ is a radical extension of } F \]

Each root of \( \beta(x) \) is expressible in terms of radicals of elements of \( F \), so \( \beta(x) \) is solvable by radicals. This is \( \leq \) in the main theorem.
To prove 12.4.10 we need to recall $\phi_n(x)$ and so on.

E.g., $n = 12$

$$x^{12} - 1 = (x^6 + 1)(x^6 - 1)$$

$$= (x^4 - x^2 + 1)(x^2 + 1)(x^2 - 1)$$

$$= \phi_{12}(x) \cdot \zeta_{12}(x)$$

Let $\zeta = e^{2\pi i/12} = \text{primitive 12th root of unity}$,

$$\zeta^{2k} = 6\text{th root of unity}$$

$$\zeta^{3k} = 4\text{th}$$

The remain roots are $\zeta, \zeta^5, \zeta^7$ and $\zeta^{11}$. 
$n = 20 \quad s = e^{2\pi i/20}$

$s^{2k}$ is a 10th root

$s^{5k}$ is 4th

$s^1, s^3, s^7, s^9, s^{11}, s^{13}, s^{17}, s^{19}$

In the general the # of primitive n-th roots of unity is $\phi(n)$, the Euler totient, the # of integers prime to n between 0 and n.

The exponents form a gp under multiplication mod n.
What is \( \text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \)?

Each primitive root has the same minimal polynomial, \( \Phi_{20}(x) \)

\[
\Phi_{20}(x) = (x^{10} + 1)(x^{10} - 1) = (x^8 - x^6 + x^4 - x^2 + 1)(x^2 + 1)(x^{10} - 1)
\]

\[
\Phi_{20}(x) \quad \text{and} \quad l_{20}(x)
\]

Claim \( \Phi_{20}(x) = (x-5)(x-5^2)(x-5^3)(x-5^7)(x-5^{13})(x-5^{17})(x-5^{19}) \)

\( \text{Gal gp is } C_m \) the multiplicative
of unity in the ring \( \mathbb{Z}/n \).

For \( \mathbf{a} \in \text{U}(n) \) there is a Galois
automorphism \( \sigma \) defined by
\[
\sigma(\mathbf{a}) = \mathbf{a}^k.
\]

Precise definition of \( \tilde{\mathbf{F}}_n(x) \) is
tricky to write, but clear
in any specific case.

Example \( n = 30 \)

\[
x^{30} - 1 = (x^{15} + 1)(x^{15} - 1) = (x^4 + x^3 + x + 1)(x^6 - 1)
\]

\[
= (x^2 + x^1 + 1)(x^{10} - 1)
\]
\[ f(x) = (x^{10} - x^5 + 1)(x^{15} - 1) \]

\( \Phi_{30}(x) \) is a degree 6 factor of \( x^{10} - x^5 + 1 \).

Def \( \Phi_n(x) \) is the minimal poly of \( e^{2\pi i/n} \) in \( \mathbb{C} \).

Properties

\[ \Phi_n(x) \in \mathbb{Z}[x] \quad 12, 4, 8 \]
$\phi_n(n)$ is defined as the degree in $\mathbb{U}(n)$.

$G_n = \mathbb{N}/(\mathbb{Z}/n) = \mathbb{U}(n) = C_n^x = \gamma \beta$ of units in the ring $\mathbb{Z}/n$.

$G_n$ acts by sending $\mathbb{G} \rightarrow \mathbb{G}$ to various powers of itself. $G_{130} = \{1, 7, 11, 13, 17, 19, 23, 29, 37 \}$

$n = 100 \quad \mathbb{U}(100) = 40$
Facts about $\varphi$:

\[ \varphi(p^n) = p^n - p^{n-1} \quad (p - 1) p^{n-1} \quad p = \text{prime} \]

\[ \varphi(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}) \quad \text{for distinct primes} \]

\[ = \prod_{i=1}^{k} \varphi(p_i^{n_i}) = \prod_{i=1}^{k} (p_i^{n_i} - 1) \]

\[ \varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \varphi(5^2) \]

\[ = 2 \cdot 20 = 40 \]

\[ c_m = \left\{ 1, 3, 7, 9, 11, 13, 17, 19, \ldots \right\} \]
\[ C_p^x = U(p^n) = C_{p-1} \times C_{p^{n-1}} = C_{p-1}^{n-1} \quad (p \text{ is prime}) \]

Let \( m = \prod_{i=1}^{k} p_i^{n_i} \), \( p_i \) are distinct prime.

\[ C_m^x = U(m) = \prod_{i=1}^{k} U(p_i^{n_i}) \]

\[ = \prod_{i=1}^{k} \left( C_{p_i-1} \times C_{p_i^{n_i}-1} \right) \]

e.g. \( U(100) = U(4) \times U(25) \)
This is $\text{Gal} \left( \mathbb{Q}(\sqrt[100]{1+i}) / \mathbb{Q} \right)$.