\[ s = e^{\frac{2\pi i}{17}} = 17 \text{ the root of unity} \]

It is a root of
\[ x^{17} - 1 = (x-1)(x^{16} + x^{15} + \cdots + x + 1) \]

Let \( f(x) = \frac{x^{17} - 1}{x - 1} \) and \( \theta \in \{ \text{roots of } x^{17} - 1 \} \)

\[ E = \text{splitting field of } f(x) \]

Claim \( [E:Q] = 16 \) and \( \text{Gal } (E/Q) = C_{16} \)
There is an automorphism in $\phi \in G$ defined by $\phi(3) = 3^3$.

Note $3^8 = -1 \mod 17$

$3^{16} = 1 \mod 17$

So $\phi$ has order 16.

We have $G = C_{16} \supset C_8 \supset C_4 \supset C_2 \supset \mathbb{Z}_3$

and a corresponding tower of fields

$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \mathbb{C}$
This is a square root tower.

Armlan argument works whenever

\( G \) is a 2-group.

Thus \( 12^{3/2} \) is irreducible if and only if

with 3 real zeros is not solvable

by radicals

Example: Let \( f(x) = x^5 - 10x - 5 \).

It is irreducible by Eisenstein's

claim. \( f(x) \) has 3 real zeros.
$d_1, d_2, \text{ and } d_3$, and $2$ nonnegative
complex numbers $d_4$ and $d_5$.

2. The Galois group $G$ has an
    element of order 5.

3. A subgroup of $S_5$ having a
    2-cycle and a 5-cycle is
    all of $S_5$.

Note: 1. implies that complex conjugation
        is a 2-cycle.

Proof: \( f'(x) = 5(x^4 - 2) \)
Critical pts at $x = \pm 2^{1/4}$

3. Since $f'(x)$ is irreducible,

$$\left[ \mathbb{Q}[x] : \mathbb{Q} \right] = 5$$

so 5 divides $|G|$. By Cauchy's Thm, $G \leq S_5$ has an element of order 5.
3. $S_5$ is generated by $(12)$ and $(12345)$. This implies our group is all of $S_5$.

\[\text{Q.E.D.}\]

Theorem 12.5.18 (Main theorem) Let $f(x) \in \mathbb{F}$

where $\mathbb{F}$ has characteristic $0$.

$E$ is splitting of $f$ and $G = \text{Gal}(E/F)$.

Then $f(x)$ is solvable by radicals

$\implies G$ is solvable.
Some homework problem says $G$ is solvable if it satisfies $G_1 \supset G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{n-1} = \{ e \}$ such that $G_i \triangleleft G_{i+1}$ is normal in $G_{i+1}$, and $G_i / G_{i+1}$ is $C_p$ for $p$ a prime dividing $|G_i|$. We will want to look at field extensions with Galois group $C_p$. 
Prof 12, 25, 14. Let $F$ be a field containing all $n$th roots of unity, and let $E$ be a Galois extension with $G = \text{Gal}(E/F) \cong \mathbb{C}_n$. Then $E$ is a simple radical extension of $F$, i.e. $E = F[p^{1/p}]$ with $p^n \in F$.

**Proof.** Let $S = \text{primes that are not in } \mathbb{C}_n$. For $\alpha \in E$ not in $F$ and let $\sigma$ be a generator of $G \cong \mathbb{C}_n$, $g(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha)$.
\[ \sigma(g(x)) = \sigma(x) + s\sigma^2(x) + \cdots + s^{n-1}\sigma^n(x) \]

\[ = s^{-1}x + \sigma(x) + s\sigma^2(x) \cdots + s^{n-1}\sigma^n(x) \]

\[ = s^{-1}g(x) \; \text{[}g(x) \text{is an eigenvector for } s] \]

We can deduce that \( g(x) \) is not in any subfield of \( E \),

\[ \sigma(g(x)^n) = \sigma(g(x))^n = (s^{-1}g(x))^n \]

\[ = s^{-n}g(x)^n = g(x)^n. \]

This means \( g(x)^n \in F \). We can deduce \( E = \overline{F[\sqrt[n]{g(x)}]} \).
E is a simple radical extension. Q.E.D.

Conclusion: If $F$ has $n$th roots of unity, then any $C_n$ extension is a simple radical extension.

Let $G$ be the main term, and let $F$ contain $n$ $p$th roots of unity for each prime $p$ dividing $|G|$. If $G$ is solvable, the $E$ is the
top of a radical tower over $F$.

Proof: We have subgps

$$G_0 \supset G_1 \supset \ldots \supset G_m = \bar{F}$$

with $G_{i+1}$ normal in $G_i$ and

$$G_i / G_{i+1} \cong \bar{F}$$

for $p$ dividing $|G_i|$. By FTGT, we get a tower of fields

$$F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_m = E$$

$F_i / F_{i+1} \cong \bar{F}$

$F_{i+1}$ is a $\bar{F}$-extension of $F_i$.
Since $F$ contains $\sqrt{q}$, so does $F_1$. Hence $F_{i+1}$ is a simple radical extension of $F_i$. QED

We need a way to get around this demanding hypothesis about $F$.

Auxiliary irrationality lemma

$\exists E', G' = \text{Gal}(E'/F')$

$G = \text{Gal}(E'/F)$
$E$ is the splitting field of $f(x) \in F[x]$

Then for $\sigma \in G'$, $\sigma(E) = E$ and the map $G' \rightarrow G$ is 1-1.

Proof: Let $x_1, \ldots, x_n$ be the zeros of $f(x)$

$E = F(x_1, \ldots, x_n)$

$E = F'(x_1, \ldots, x_n)$

$G \in G'$ permutes the $x_i$'s. This means it sends any $F$-linear
Combination of them to another one, i.e., it sends $E$ to $E$.

We do get a hom $G_1 \rightarrow G$.

If $\sigma \neq e$ then there is an $i$ with $\sigma(x_i) = x_j$ for $j \neq i$.

The same is true in $G_2$, so

$P(0) = \text{id} \iff 0$ is identity $P$ is $1-1$.