# 4. Galois Theory of Polynomials

Recall: If $f(x) \in F[x]$ and $K$ is the splitting field over $F$, then the Galois group of $f(x)$ over $F$ is $G := Gal(K/F)$.

$G$ acts faithfully on the set $S$ of roots of $f(x)$, i.e,
$G \hookrightarrow S_n$ (where $|S| = n$).

Exercise. If $f(x)$ is irreducible, then this action is transitive.
(This follows immediately from Prop 1.9: $\exists \phi : F(a) \to F(b) \ldots$).

Def: A simple radical extension of $F$ is a field $K = F(a)$, where $a^n \in F$ for some $n \in \mathbb{N}$, i.e, $a$ is a root of $x^n - b \in F[x]$.

Example: If char $F \neq 2$ and $[K:F] = 2$, then $K/F$ is a simple radical extension (complete the square).

Consider $f(x) = x^n - 1 \in F[x]$, let $K$ be the splitting field.

If char $F = p > 0$, suppose $p \nmid n$ (so $f'(x) \neq 0$, & $(f(x), f'(x)) = 1$).

Prop 3.2 $\Rightarrow$ $f(x)$ has $n$ distinct roots, called the roots of unity.

The $n^{th}$ roots of unity form a multiplicative subgroup of $K \setminus \{0\}$.

By Prop 3.7, it is cyclic.

The generators are the primitive $n^{th}$ roots of unity.

Note: There are $\phi(n)$ primitive roots of unity, where $\phi$ is Euler's totient function: $\phi(n) = |\{0 < k < n : (n,k) = 1\}|$.

<u>Remark</u>: If $\omega$ is a primitive $n^{th}$ root of unity, then

* $1, \omega, \omega^2, \dots, \omega^{n-1}$ are all the $n^{th}$ roots of unity
* $K = F(\omega)$, a simple radical extension
* $1 + \omega + \omega^2 + \dots + \omega^{n-1} = 0$ (actually $\omega$ need not be primitive).

<u>Prop 4.1</u>: (a) If char $F = p \nmid n$, then the Galois group of $x^n - 1 \in F[x]$ is abelian

(b) Moreover, if $F = \mathbb{Q}$, the Galois group $x^n - 1 \in F[x]$ is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.

<u>Pf</u>: (a) Take $G = Gal(F(\omega)/F)$, $\omega$ is a primitive $n^{th}$ root of unity.

If $\phi, \theta \in G$, then $\phi(\omega)$ and $\theta(\omega)$ are roots of $f(x)$.

Therefore, $\phi(\omega) = \omega^i$, $\theta(\omega) = \omega^j$ for some $i, j$.

Thus, $\phi\theta(\omega) = \omega^{ij} = \theta\phi(\omega)$

Since $F(\omega)$ is simple, every $\phi \in G$ is determined by $\phi(\omega)$,

so $\phi\theta = \theta\phi \implies G$ is abelian. ✓

(b) Check that $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow Gal(\mathbb{Q}(\omega)/\mathbb{Q})$

$$a \pmod n \longmapsto \sigma_a \quad \text{where } \sigma_a(\omega) = \omega^a$$

is an isomorphism (Easy exercise!). ✓

□

<u>Def</u>: The polynomial $\Phi_n(x) = \prod_{i=1}^{\phi(n)} (x - \omega_i)$, where $\omega_1, \dots, \omega_{\phi(n)}$ are the primitive roots of unity, is the $n^{th}$ <u>cyclotomic polynomial</u>.

Remark: If $\eta$ is a root of $f(x) = x^n - 1$, then $\eta$ is a primitive $d^{th}$ root of unity, where $|\eta| = d$ in $K \setminus \{0\}$, so $d \mid n$ (Lagrange). Therefore, $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$, and so

$$\Phi_n(x) = \frac{x^n - 1}{\prod \{\Phi_d(x) : d \text{ proper divisor of } n\}}.$$

Examples: $\Phi_1(x) = x - 1$

$$\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = \frac{x^2-1}{x-1} = x+1$$

$$\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = \frac{x^3-1}{x-1} = x^2+x+1$$

$$\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = x^2+1$$

$$\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2 - x + 1.$$

Fact: If $F = \mathbb{Q}$, then $\Phi_n(x) \in \mathbb{Z}[x]$.

Thm 4.2: The cyclotomic polynomial $\Phi_n(x)$ in $\mathbb{Q}[x]$ is monic, irreducible, in $\mathbb{Z}[x]$, and has degree $\phi(n)$.

Pf: It is clear that $\Phi_n(x)$ is monic of degree $\phi(n)$.

To show $\Phi_n(x) \in \mathbb{Z}[x]$, use induction. Base case trivial ✓

Assume it's true for all $1 \leq d < n$.

Then $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod_{d \mid n,\, d<n} \Phi_d(x) \in \mathbb{Z}[x]$ is monic.

$\boxed{4}$

Clearly, $f(x) \mid x^n - 1$ in $\mathbb{Q}(\omega_n)[x]$ ($\omega_n$ a primitive $n^{th}$ root of unity)
and $f(x), x^n-1 \in \mathbb{Q}[x] \implies f(x) \mid x^n - 1$ in $\mathbb{Q}[x]$
(by Euclidean Algorithm).

By Gauss' Lemma (Thm 3.13), $f(x) \mid x^n - 1 \in \mathbb{Z}[x] \implies \Phi_n(x) \in \mathbb{Z}[x]$. ✓

<u>Show $\Phi_n(x)$ irreducible:</u> Suppose that $\Phi_n(x) = f(x)\,g(x)$,
where $f(x), g(x) \in \mathbb{Z}[x]$ are both monic. (<u>Goal</u>: show one of these is 1).

Let $\omega$ be a primitive $n^{th}$ root of unity, which is a root of $f(x)$
If $p \nmid n$ is prime, then $\omega^p$ is primitive, so $\omega^p$ is a root
of $f(x)$ or $g(x)$.

Suppose $g(\omega^p) = 0$. Then $\omega$ is a root of $g(x^p) \implies f(x) \mid g(x^p)$.
(since $f(x)$ is the min'l poly for $\omega$ over $\mathbb{Q}$).

Say $g(x^p) = f(x)\,h(x)$, $h(x) \in \mathbb{Z}[x]$.

Reduce mod $p$: $\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\,\bar{h}(x) \in \mathbb{F}_p[x]$.

Since $\mathbb{F}_p[x]$ is a UFD, $\bar{f}(x)$ & $\bar{h}(x)$ have a common factor in $\mathbb{F}_p[x]$.

<u>Note</u>: $\Phi_n(x) = f(x)\,g(x) \implies \bar{\Phi}_n(x) = \bar{f}(x)\,\bar{g}(x)$

$\implies \bar{\Phi}_n(x) \in \mathbb{F}_p[x]$ has a multiple root.

$\implies x^n - 1$ has a multiple root, since $\bar{\Phi}_n(x) \mid x^n - 1$. $\lightning$

Therefore, $f(\omega^p) = 0$.

Similarly, if $(n,a)=1$, then $\omega^a$ is a root of $f(x)$.

$\Rightarrow$ every primitive $n^{th}$ root of unity is a root of $f(x)$

$\Rightarrow f(x) = \Phi_n(x)$ $\lightning$

Thus, $\Phi_n(x)$ is irreducible. $\square$

<u>Prop 4.3</u>: Suppose char $F = p \nmid n$, and $\omega \in F$ is a primitive $n^{th}$ root of unity, and $0 \neq b \in F$. Then a splitting field $K$ for $f(x) = x^n - b$ over $F$ is a simple radical extension of $F$ and the Galois group $G$ of $f(x)$ is abelian.

<u>Pf</u>: Let $a \in K$ be a root of $f(x)$. The distinct roots are then $a, a\omega, a\omega^2, \dots, a\omega^{n-1}$, so $K = F(a)$, and $a^n = b \in F$, so $K/F$ is a simple radical extension. ✓

The proof that $G$ is abelian is analogous to that in Prop 4.1 (but moreover, $G$ is cyclic). $\square$

<u>Def</u>: $K/F$ is an <u>extension by radicals</u> if there is a sequence $F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_k = K$ such that $L_i/L_{i-1}$ is a simple radical extension.

<u>Def</u>: A polynomial $f(x) \in F[x]$ is <u>solvable by radicals</u> over $F$ if there is an extension $K/F$ by radicals such that $f(x)$ splits in $K[x]$.

This just means that we have a "formula" for the elements of $K$, e.g., quadratic formula, cubic formula.

**Fact:** Over $\mathbb{Q}$, all degree-2, 3, and 4 polynomials are solvable by radicals, but not all degree-5 polynomials are. We will formalize & prove this using Galois theory.

**Def:** If $F \subseteq E \subseteq K$ and $F \subseteq L \subseteq K$, define the join of $E$ & $L$ to be $E \vee L = F(E \cup L)$:

i.e, "smallest subfield of $K$ containing $E$ and $L$."

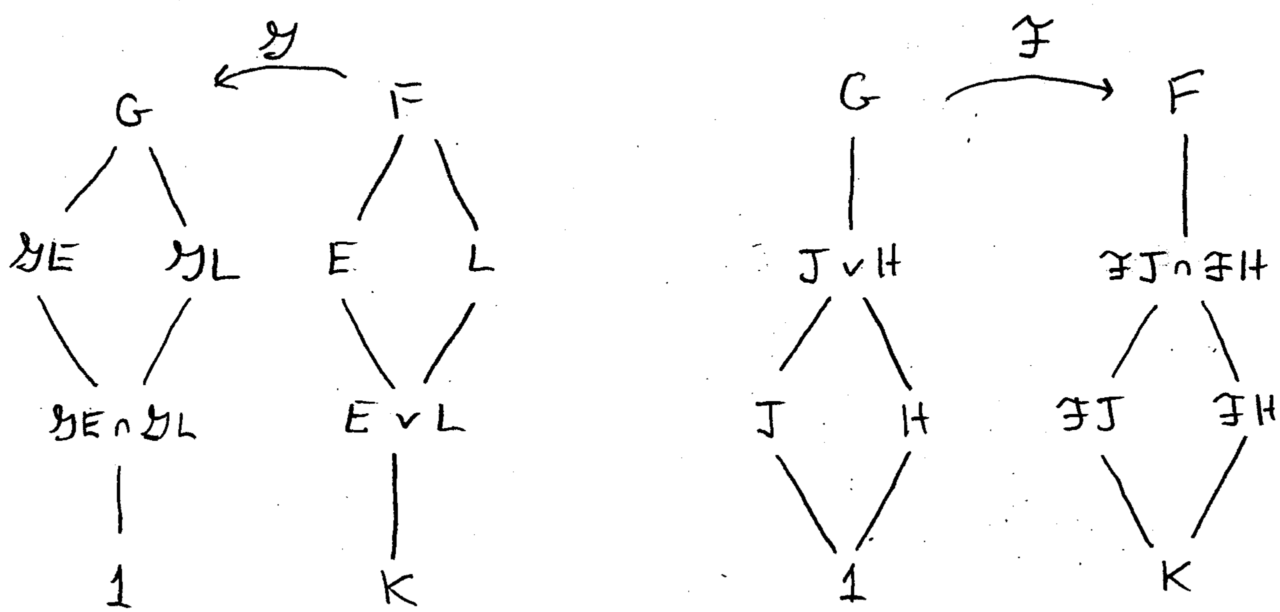
**Def:** If $G$ is a group, and $J, H \leq G$, define the join of $J$ & $H$ to be $J \vee H = \langle J \cup H \rangle$:

i.e, "smallest subgroup of $G$ containing $J$ and $H$."

**Exercise:** Suppose $F \subseteq E, L \subseteq K$, and $J, H \leq G = Gal(K/F)$.

Then (1) $\mathcal{G}(E \vee L) = \mathcal{G}E \cap \mathcal{G}L$ and $\mathcal{F}(J \vee H) = \mathcal{F}J \cap \mathcal{F}H$

(2) $[E \vee L : F] \leq [E:F][L:F]$.



<u>Prop 4.4</u>: Suppose $F \subseteq K_1, K_2 \subseteq L$ and $K_i/F$ is an extension by radicals $(i=1,2)$. Then $K_1 \vee K_2$ is an extension by radicals.

<u>Pf</u>: If $K_1 = F(a_1,\dots,a_m)$ and $K_2 = F(b_1,\dots,b_n)$, then
$K_1 \vee K_2 = F(a_1,\dots,a_m,b_1,\dots,b_n)$. $\square$

<u>Prop 4.5</u>: If $K/F$ is a separable extension by radicals, and $L/F$ is a Galois closure, then $L/F$ is a separable extension by radicals.

<u>Pf</u>: <u>Recall</u>: $L$ is a splitting field for $\mathcal{F} = \{m_{a_i}(x)\}$ over $F$, where $\{a_1,\dots,a_n\}$ is an $F$-basis for $K$.

Set $G = \mathrm{Gal}(L/F)$.

Prop 3.3 $\Rightarrow$ $\{\phi(a_i) : \phi \in G,\ 1 \le i \le n\}$ spans $L$ over $F$.

If $G = \{\phi_1,\dots,\phi_k\}$, set $K_i := \phi_i(K)$.

Then $L = K_1 \vee K_2 \vee \dots \vee K_k$. Apply Prop 4.4. $\square$

<u>Thm 4.6</u> (Galois): Suppose char $F = 0$, and $f(x)$ is solvable by radicals. Then the Galois group of $f(x)$ is solvable.

<u>Remark</u>: The converse holds as well. (See Thm 4.10.)

<u>Pf</u>: Let $F = L_0 \subseteq L_1 \subseteq \dots \subseteq L_k = K$ be a sequence of simple radical extensions, with $L_i = L_{i-1}(a_i)$, $a_i^{n_i} \in L_{i-1}$, such that there is a splitting field $L$ for $f(x)$ over $F$, $L \subseteq K$.

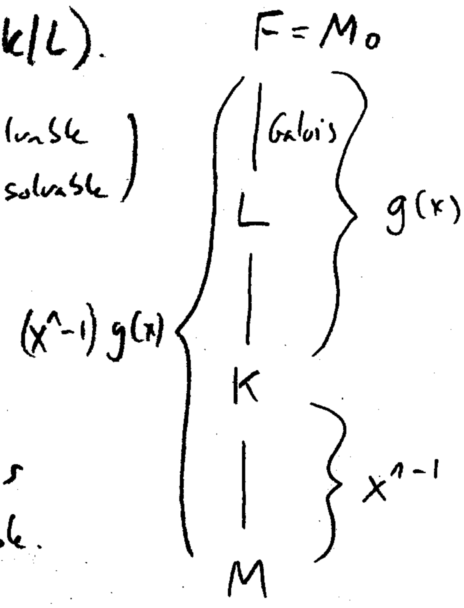
Prop 4.5 $\Rightarrow$ WLOG we may assume that $K/F$ is Galois (otherwise just take $K$ to be the Galois closure).

Let $G = Gal(L|F)$, the Galois group of $f(x)$.

By FTGT, $Gal(L|F) \cong Gal(K|F) / Gal(K|L)$.

By Thm 5.4 (Groups), ($G$ solvable $\Leftrightarrow$ $N$ solvable and $G/N$ solvable)

$Gal(K/F)$ solvable $\Longleftrightarrow$ $Gal(K/L)$ solvable and $Gal(L/F)$ solvable.




* We want to show $Gal(L/F)$ is solvable, thus it suffices to show that $Gal(K/F)$ is solvable.

Set $n = n_1 n_2 \cdots n_k$ and let $M$ be the splitting field for $x^n-1$ over $K$.

Let $\omega$ be a primitive $n^{th}$ root of unity in $M$ (i.e, $M = K(\omega)$.)

<u>Note:</u> $F(\omega)$ contains all $n_i^{th}$ roots of unity for $1 \leq i \leq k$.

Since $K/F$ is Galois, $K$ is the splitting field for some $g(x)$ over $F$.

Clearly, $M$ is a splitting field for $(x^n-1)g(x)$ over $F$.

Therefore, $M|F$ is Galois.

By FTGT, $Gal(K/F) \cong Gal(M|F) / Gal(M|K)$.

and $Gal(M/F)$ solvable $\Longleftrightarrow$ $Gal(M|K)$ solvable <u>and</u> $Gal(K/F)$ solvable

* Suffices to show that $Gal(M|F)$ is solvable.

Let $M_0 = F$, $M_1 = F(\omega)$, $M_2 = M_1(a_1)$, ..., $M_{k+1} = M_k(a_k) = M$.

We now have the chain of subfields

$$\begin{array}{lccccccc}
 & F \subseteq F(\omega) & \subseteq F(\omega, a_1) & \subseteq F(\omega, a_1, a_2) & \subseteq \cdots \subseteq & F(\omega, a_1, \dots, a_k) & = M \\
\text{i.e,} & L_0 \subseteq L_0(\omega) & \subseteq L_1(\omega) & \subseteq L_2(\omega) & \subseteq \cdots \subseteq & L_k(\omega) & = M \\
\text{i.e,} & M_0 \subseteq M_1 & \subseteq M_2 & \subseteq M_3 & \subseteq \cdots \subseteq & M_{k+1} & = M
\end{array}$$

* Key: Each $M_{i+1} = M_i(a_i)$ contains a root $a_i$ of $x^{n_i} - b_i$ and the $n_i^{th}$ roots of unity.

$\Rightarrow$ Each $M_{i+1} = M_i(a_i)$ contains all roots of $x^{n_i} - b_i$

$\Rightarrow$ $M_{i+1}/M_i$ is Galois.

$$\begin{tikzcd}
H_0 = Gal(M/F) \arrow[r, bend left, "\mathcal{F}"] \arrow[d, dash] & M_0 \arrow[d, dash] \\
H_1 = Gal(M/M_1) \arrow[d, dash] & M_1 \arrow[d, dash] \\
H_2 = Gal(M/M_2) \arrow[d, dash] & M_2 \arrow[d, dash] \\
\vdots \arrow[d, dash] & \vdots \arrow[d, dash] \\
H_{k+1} = Gal(M/M_{k+1}) & M_{k+1} = M \arrow[l, bend left, "\mathcal{G}"]
\end{tikzcd}$$

** Props 4.1 & 4.3 $\Rightarrow Gal(M_{i+1}/M_i)$ is abelian.

Define $H_0 = Gal(M/F)$

$H_i = Gal(M/M_i) \leq Gal(M/F)$, etc.

Note: $M/M_i$ and $M_{i+1}/M$ are Galois

Apply FTGT:

$Gal(M/M_{i+1}) = H_{i+1} \trianglelefteq Gal(M/M_i) = H_i$

and $H_i/H_{i+1} \cong Gal(M_{i+1}/M_i)$ which is abelian.

By definition, $Gal(M/F)$ is solvable

$\Rightarrow$ $Gal(K/F)$ is solvable

$\Rightarrow$ $Gal(L/F)$ is solvable. $\square$

Example: Let $f(x) = x^5 + 5x^3 - 20x + 5 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein $(p=5)$.

By calculus, $f(x)$ has exactly 3 real roots $a_1, a_2, a_3$.

Let $a_4, a_5$ be the complex (conjugate) roots.

Let $K \subseteq \mathbb{C}$ be a splitting field for $f(x)$ over $\mathbb{Q}$.

Then $5 \mid [K:\mathbb{Q}] = |G| \Rightarrow G$ contains a "5-cycle" $\sigma$ (Cauchy).

Also, by Thm 3.5(c), complex conjugation restricted to $K$ is a $\mathbb{Q}$-automorphism, fixing $a_1, a_2, a_3$, and $a_4 \leftrightarrow a_5$.

This element $\tau$ is a "2-cycle" of $G$.

Basic group theory fact: Any $n$-cycle and 2-cycle generate $S_n$.

Therefore, $G \cong S_5$, which is not solvable ($S_5 \trianglerighteq A_5 \trianglerighteq 1$; $A_5$ is simple but not abelian).

Thus, $f(x)$ is not solvable by radicals.

* Similarly, any degree-$p$ polynomial (prime $p \geq 5$) with exactly $p-2$ real roots is not solvable by radicals.

For the converse of Thm 4.6, we need some more tools.

Def: Suppose $F$ contains a primitive $n^{th}$ root of unity, and $K = F(a)$ is a simple Galois extension, $[K:F] = n$, and $G = Gal(K/F) = \langle \phi \rangle$ has order $n$. If $\omega \in F$ is an $n^{th}$ root of unity, then define the Lagrange resolvent of $\omega$ and $a$ to be

$$L(\omega, a) = a + \omega\phi(a) + \omega^2\phi^2(a) + \dots + \omega^{n-1}\phi^{n-1}(a).$$

Exercise: $\phi(L(\omega,a)) = L(\omega,\phi(a)) = \omega^{-1}L(\omega,a)$.

Cor: $\phi(L(\omega,a)^n) = \phi(L(\omega,a))^n = (\omega^{-1}L(\omega,a))^n = L(\omega,a)^n$

* i.e, $L(\omega,a)^n$ is fixed by every $\phi \in Gal(K|F)$

$\Rightarrow L(\omega,a)^n \in F$.

Prop 4.7: Suppose $\omega \in F$ is a primitive $n^{th}$ root of unity $K = F(a)$ a Galois extension with $[K:F]=n$, and cyclic Galois group $G = Gal(K|F) = \langle \phi \rangle$. Then for some $i$, $L(\omega^i, a) \in K \setminus F$.

Pf: Recall that $\sum_{i=0}^{n-1} \omega^i = 0$. (See Remark, p. 2).

$$\sum_{i=0}^{n-1} L(\omega^i,a) \underset{\text{Exercise}}{=} \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \omega^{ij}\phi^j(a) \underset{\text{Rearrangement}}{=} \sum_{j=0}^{n-1} \phi^j(a) \underbrace{\sum_{i=0}^{n-1} (\omega^j)^i}_{=0 \text{ except for } j=0.}$$

$$= \phi^0(a) \sum_{i=0}^{n-1} (\omega^0)^i = an.$$

Since $F$ contains a primitive $n^{th}$ root of unity, char $F \nmid n$, so $n1 \neq 0 \Rightarrow na \in K \setminus F$.

Therefore, at least one $L(\omega^i, a) \in K \setminus F$. $\square$

Prop 4.8: Suppose $p \in \mathbb{Z}$ is prime and $F$ contains a $p^{th}$ root of unity, and $K/F$ is Galois with $[K:F]=p$. Then $K/F$ is a simple radical extension.

Pf: Since $[K:F]$ is prime, $K = F(a)$ for any $a \in K \setminus F$, and $G = Gal(K|F)$ is cyclic ($|G| = [K:F] = p$).

By Prop 4.7, $\exists$ Lagrange resolvant $b \in K \setminus F$

By Exercise, $b^p = c \in F$, i.e, $b$ is a root of $x^p - c \in F[x]$. $\square$

Prop 4.9: Suppose $f(x) \in F[x]$ has Galois group $G$ over $F$, and $E|F$ is any extension field. Then the Galois group of $f(x)$ over $E$ is isomorphic to a subgroup of $G$.

Pf: Let $L/E$ be a splitting field for $f(x)$, with roots $a_1, \dots, a_n$.
Then $K = F(a_1, \dots, a_n)$ is a splitting field for $f(x)$ over $F$.
If $\phi \in Gal(L|E)$, then $\phi$ permutes $a_1, \dots, a_n$, so $\phi(K) = K$,
and $\phi = 1_K \iff \phi(a_i) = a_i \ \forall i \iff \phi = 1_L \in Gal(L/E)$.
Thus, $\exists$ $Gal(L/E) \hookrightarrow Gal(K|F)$
$\phi \longmapsto \phi|_K$. $\square$

$$\begin{tikzcd}[column sep=small]
 & L = E(a_1, \dots, a_n) \arrow[dl, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & K = F(a_1, \dots, a_n) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

Thm 4.10 (Galois): Suppose char $F = 0$, $f(x) \in F[x]$, and the Galois group of $f(x)$ is solvable. Then $f(x)$ is solvable by radicals over $F$.

Pf: Let $K$ be a splitting field for $f(x)$ over $F$, set $G = Gal(K|F)$ and say $[K:F] = n$.
Let $L/K$ be a splitting field for $x^n - 1$,
$w \in L$ a primitive $n^{th}$ root of unity.
Set $E = F(w)$, and so clearly
$L/E$ is a splitting field for $f(x)$.
Set $H = Gal(L|E)$
Prop 4.9 $\Rightarrow H \hookrightarrow G = Gal(K|F)$.
$G$ solvable (by assumption) $\Rightarrow H$ solvable.

$$\begin{tikzcd}[column sep=small]
 & L = E(a_1, \dots, a_n) \arrow[dl, dash] \arrow[dr, dash] & \\
E = F(w) \arrow[dr, dash] & & K = F(a_1, \dots, a_n) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

$$\begin{tikzcd}
H_0 = H \arrow[r, bend left, "\mathcal{F}"] \arrow[d, dash] & L_0 = E \arrow[d, dash] \\
H_1 \arrow[d, dash] & L_1 \arrow[d, dash] \\
H_2 \arrow[d, dash] & L_2 \arrow[d, dash] \\
\vdots \arrow[d, dash] & \vdots \arrow[d, dash] \\
H_k = 1 & L_k = L \arrow[l, bend left, "\mathcal{G}"]
\end{tikzcd}$$

By Thm 5.3 (Groups), $H$ has a subnormal series $H = H_0 \geq H_1 \geqslant \cdots \geqslant H_k = 1$ with abelian factors, and we can assume that $H_{i-1}/H$ is cyclic of prime order $p_i$ (by refinement).

Since $E \subseteq L$, set $L_i = \mathcal{F} H_i$, so

$E = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L$, $\quad [L_i : L_{i-1}] = p_i$.

Since $Gal(L/L_i) = H_i \lhd H_{i-1} = Gal(L/L_{i-1})$, $L_i/L_{i-1}$ is Galois, and $L_{i-1}$ contains a primitive $p_i^{th}$ root of unity (which is a power of $\omega$).

By Prop 4.8, $L_i/L_{i-1}$ is a simple radical extension, $i = 1, \dots, k$.

Thus, $L/E$ (i.e, $L_k/L_0$) is an extension by radicals.

Since $F = E(\omega)$, $L/F$ is also an extension by radicals. $\square$

<u>Cor</u> (of Thms 4.6, 4.10): Suppose char $F = 0$ and $f(x) \in F[x]$. Then $f(x)$ is solvable by radicals iff the Galois group of $f(x)$ is solvable.