Theorem 0.1 *Let F be a field containing a primitive n^{th} root of 1. Let $E = F[\alpha], \alpha^n = a \in F$ and no smaller power of $\alpha \in F$. Then E/F is Galois extension with $Gal(E/F) \cong \mathbb{Z}/n\mathbb{Z}$.*

Conversely, if E/F is cyclic Galois extension of degree n, then $\exists \alpha \in E$ s.t. $E = F[\alpha], \alpha^n \in F$.

Proof: $(\Longleftarrow)$ $G = Gal(E/F) =< \sigma >$.

$\mu_n(F) =< \zeta >$

Enough to find $\alpha \in E$ s.t. $\sigma(\alpha) = \zeta^{-1}\alpha$.

$\sigma(\alpha^m) = \sigma(\alpha)^m = \zeta^{-m}\alpha^m$

If $m = n$: $\sigma(\alpha^n) = \alpha^n \implies \alpha^n \in F$. $m < n, \sigma(\alpha^m) = \zeta^{-m}\alpha^m \neq \alpha^m$

Consider $\sigma^i : E^\times \to E^\times$.

$\therefore 1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent.

$\Sigma_{i=0}^{n-1}\zeta^i\sigma_i : E^x \to E$ is non zero.

$\exists\gamma$ such that $\alpha := \Sigma_{i=0}^{n-1}\zeta^i\sigma_i(\gamma) \neq 0$.

What is $\sigma(\alpha) =$?

$\sigma(\alpha) = \sigma(\sum_{i=0}^{n-1}\zeta_i^i\sigma^i\alpha)$

$= \sigma_{i=0}^{n-1}\zeta_i\sigma i + 1(\gamma)$

$= \zeta^{-1}\sum_{i=0}^{n-1}\zeta^{i+1}\sigma^{i+1}(\gamma) = \zeta^{-1}\alpha$ ■

Theorem 0.2 *(Galois Solvability Theorem) Let F be a field of char 0. Then an extension is solvable by radicals if and only if L is a subextension of a Galois extension E/F with a solvable Galois group.*

Proof: Recall: $F \subset L$, $F \subset E$ Galois,

Ω E L $E \cap L$ F

$Gal(EL/L) \cong Gal(E/E \cap L) \hookrightarrow Gal(E/F)$.

$(\Longleftarrow)$

$f \in F[x]$ has a solvable Galois group.

$Gal(E/F)$ is solvable, E is the splitting field of f over F.

$Gal(E \cdot F[\zeta]/F[\zeta]) < Gal(E/F)$. (is solvable because it is a subgroup of a solvable groups)

Take ζ primitive $n-th$ root of unity, $n = deg(f!)$.

$\therefore \exists G = G_0 \triangleright G_1 \triangleright G_2 \ldots \triangleright G_m = 1$.

Let K be the splitting field of f over $F[\zeta](= E \cdot F[\zeta])$

Let K_i be the fixed field of G_i, i.e. E^{G_i}.

$F \subset F[\zeta] = K_0 \subset K_1 \subset \ldots \subset K_m = K$.

K_i/K_{i-1} is cyclic $\implies K_i = K_{i-1}[\alpha_{i-1}]$

$\implies$ f is solvable by radicals $E \subset E \cdot F[\zeta] = K$ ■