Thm (Galois)

Let char $F=0$. Then $f(x)\in F[x]$ is soluble by radicals if and only if $Gal(f)$ is soluble.

expressible by algebraic combination of (elts of F and roots of elts of F).

eg. $f(x)=x^n-2\in\mathbb{Q}[x]$, then the roots of $f(x)$ are $2^{\frac{1}{n}}, 2^{\frac{1}{n}}w^j$, where $1\le j\le n-1$ and $w=e^{\frac{2\pi i}{n}}$.

irreducible

Def. ① Let $F=F_0<F_1<\cdots\cdots<F_n=E$, where $F_i=F_{i-1}(\alpha_i)$ s.t. $\alpha_i^{p_i}\in F_{i-1}$ with p_i prime.

Then the chain is called a radical tower, and E is a radical extension.

② Let $f(x)\in F[x]$. Then $f(x)$ is said to be soluble by radicals if the splitting field of f is contained in a radical extension.

eg. Let $F_0<F_1<F_2$, where $F_0=\mathbb{Q}$, $F_1=F_0(\sqrt{2})$, $F_2=F_1(\alpha^{\frac{1}{2}})$ with $\alpha=\sqrt{2}$.

Then $F_0\lhd F_1$ and $F_1\lhd F_2$. However, $F_0 \not\lhd F_2=F_0(2^{\frac{1}{4}})$.

w.r.t $x^2-\alpha$.

$a\in Gal(F_2/F_1)$ s.t. $\alpha^a=-\alpha$. $(x^2-\alpha)^a=x^2-\alpha^a=x^2+\alpha$.

the roots of $x^2+\alpha$ are $\sqrt{-\alpha}$ and $-\sqrt{-\alpha}$.

$\sqrt{-\alpha}=i2^{\frac{1}{4}}$

Thus $L=F_2(\sqrt{-1})=\mathbb{Q}(i,2^{\frac{1}{4}})$ is a normal extension of $\mathbb{Q}=F_0$.

Lemma. Let F contain all the n-th roots of unity.

Then each radical extension of F can be extended to a normal extension of F.

eg. $F=\mathbb{Q}$, $f(x)\in F[x]$, irr, deg n. $E=\mathbb{Q}(w_1,w_2,\cdots,w_t)$, where w_i is a p_i-th root of unity, with $p_i\le n$, prime. Then $f(x)\in E[x]$, and f is soluble by radicals over $\mathbb{Q}=F$

$\Leftrightarrow$ f is soluble by radicals over E.

or the roots of f is expressible over $\mathbb{Q}$ $\Leftrightarrow$ the roots of f is expressible over E.

Theorem. If $f(x)\in F[x]$ is soluble by radicals, (F contains p_i-th roots of unity) then $Gal(f)$ is a soluble group.

Proof: Let E be the splitting field of $f(x)$ over F.

Then $E\le L$ for some radical extension of F.

By the lemma, we may assume the L is a normal extension of F, so

$F = F_0 < F_1 < \cdots < F_m = L$, where $F_i = F_{i-1}(\alpha_i)$ s.t. $\alpha_i^{p_i} \in F_{i-1}$.

Since F contains all the p_i-th roots of unity, $F_{i-1} \lhd F_i$.

Let $G_i = Gal(L:F_i)$, then $G_i = Gal(L:F_i) \lhd Gal(L:F_{i-1}) = G_{i-1}$.

So $G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$.

Further, $G_{i-1}/G_i = Gal(L:F_{i-1})/Gal(L:F_i) \cong Gal(F_i : F_{i-1}) \cong C_{p_i}$.

So $G = Gal(L:F_0)$ is soluble, and so is $Gal(f) = Gal(E:F)$. $\square$.

<u>Theorem</u>. If $Gal(f)$ is a soluble group, then $f(x)$ is soluble by radicals.

($f(x) \in F[x]$, F contains the p_i-th roots of unity)

<u>Proof</u>: As $G = Gal(f)$ is soluble, we have $G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$.

where $G_{i-1}/G_i \cong C_{p_i}$ with p_i prime.

Let E be the splitting field of f over F. Let $F_i = \{a \in E \mid a^{G_i} = a\}$.

Then $F < F_1 < F_2 < \cdots < F_m = E$, and F_i is a normal extension of F_{i-1}.

Since F contains the p_i-th roots of unity, i.e. F contains all of the roots of $x^{p_i}-1$,

we have $F_i = F_{i-1}(\alpha_i)$ s.t. $\alpha_i^{p_i} \in F_{i-1}$. So E is a radical extension of F, and

f is soluble by radicals. $\square$.

<u>Def</u>. E is called a cyclic extension of F if $E = F(\alpha)$ and $Gal(E/F)$ is cyclic.

E is a cyclic extension of F

$\Leftrightarrow$ $E = F(a^{\frac{1}{n}})$ s.t. $a \in F$.

$\Updownarrow$

E is a splitting field of $x^n - a$. s.t. either ① $a = 1$ or ② F contains the roots of $x^n - 1$.

$f = x^n - 2$. $\alpha = 2^{\frac{1}{n}}$. $w = e^{\frac{2\pi i}{n}}$.

$E = F(\alpha, w)$,

$= F(w)(\alpha)$,

$F < F(w) < F(\alpha)$

$$\begin{array}{ccccc} F_0 & < & F_1 & < & F_2 \\ & \uparrow & & \uparrow & \\ & \text{cyclic} & & \text{cyclic.} & \end{array}$$