Lecture

Last time: A finite group G is solvable if $\exists$

$1 = G_s \triangleleft G_{s-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ where

G_i/G_{i+1} is cyclic.

Ex: Abelian gps, D_{2n}, S_4.

Goal:

Thm: Suppose $f \in F[x]$, where char$(F) = 0$. If f is solvable by radicals, then $\mathrm{Gal}(K/F)$ is solvable, where K = ~~field~~ splitting field of $f(x)$.

Examples where $\mathrm{Gal}(K/F)$ is solvable:

1. $K = F(\sqrt{D})$
2. $K = \mathbb{Q}(\zeta_n)$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Note: Not always cyclic, e.g. $(\mathbb{Z}/8\mathbb{Z})^\times = \mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Suppose K is the splitting field of $x^n - a \in F[x]$.

Key: $Gal(K/F)$ is solvable.

Case 1: Suppose $F \supset \mu_n$, the n^{th} roots of 1.

Let $\alpha \in K$ be a root of $X^n - a$. Then

$K = F(\alpha)$, since $F(\alpha) \supseteq \{\zeta_n^k \alpha\} =$ all roots of $X^n - a$.

Consider

$$\mathbb{Z}_n \longrightarrow Gal(K/F)$$

$$k \longmapsto \sigma_k$$

where $\sigma_k(\alpha) = \zeta_n^k \alpha$.

This is a hom, since

$$\sigma_k(\sigma_l(\alpha)) = \sigma_k(\zeta_n^l \alpha) = \zeta_n^k \zeta_n^l \alpha$$
$$= \zeta^{k+l}(\alpha) = \sigma_{k+l}(\alpha)$$

and hence an isom as

$$|Gal(K/F)| = [K:F] = n.$$

So $Gal(K/F)$ is $\mathbb{Z}_n$, hence solvable.

Ex: $K =$ splitting field of $X^3 - 2 \in \mathbb{Q}(x)$

$$\begin{array}{cl} K & \\ | & \\ \mathbb{Q}(\zeta_3) & \mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) = \mathbb{Z}_3 \\ | & \\ \mathbb{Q} & \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) = \mathbb{Z}_2 \end{array}$$

Lemma: Suppose $F \subseteq L \subseteq K$ with K/F and L/F Galois. If $\mathrm{Gal}(K, L)$ and $\mathrm{Gal}(L/F)$ are solvable, so is $\mathrm{Gal}(K/F)$.

Pf: As L/F is Galois, $\mathrm{Gal}(K/L) \triangleleft \mathrm{Gal}(K/F)$ with quotient $\mathrm{Gal}(L/F)$. That is, have $H \triangleleft G$ with H + G/H solvable $\Rightarrow$ G is solv. ∎

General case:

$$\begin{array}{rcl} & K = F(\zeta_n, \alpha) & \\ \mathrm{Gal} = \mathbb{Z}_n \longrightarrow & | & \\ & F(\zeta_n) & \\ & | & \leftarrow \text{Gal is abelian since} \\ & F & \end{array}
\qquad \boxed{\Rightarrow \mathrm{Gal}(K/F) \text{ is solvable}}$$

any two elts σ, τ have the form $\sigma(\zeta_n) = \zeta_n^{\,a}$

$\tau(\zeta_n) = \zeta_n^{\,b}$ ∎

and so $\sigma(\tau(\zeta_n)) = \zeta_n^{\,ab} = \tau(\sigma(\zeta_n))$

Lemma: Suppose α can be expressed via radicals over F. Then $\exists\, L/F$ Galois with $\alpha \in L$ and $Gal(L/F)$ solvable.

Pf: By def, $\alpha \in K$ which has

$$F = K_0 \subseteq K_1 \subseteq \cdots\cdots \subseteq K_s = K$$

where $K_{i+1} = K_i(\alpha)$ where α is a root of $X^{n_i} - a_i$ with $a_i \in K_i$. So consider

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L$$

where L_{i+1} is the splitting field of $X^{n_i} - a_i$.

Then L/F is Galois and each $Gal(L_{i+1}/L_i)$ is solvable. Inductively, this shows that $Gal(L/F)$ is solvable. $\boxed{}$

<u>Pf of Thm:</u> Suppose f is irred, $\alpha \in K$ a root. By assumption, α can be expressed via radicals. Let L be the field given by the lemma. Then $K \subseteq L$. Since

$$Gal(K/F) = Gal(L/F)/Gal(L/K),$$ it follows that $Gal(K/F)$ is solvable.

If f is reducible, apply above to each irred. factor and argue inductively that $Gal(K/F)$ is solvable. $\blacksquare$

<u>Next time</u>: S_n <u>isn't</u> solvable for $n \geq 5$.