Lecture 29:

Last time:

Def: $f(x) \in F[x]$ is solvable by radicals if there exist

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s$$ where f splits completely in K_s

and $K_{i+1} = K_i(\alpha_i)$ with α_i a root of $x^{n_i} - a_i \in K_i[x]$.

Def: A finite group is solvable if there exist

$$\{1\} = G_s \triangleleft G_{s-1} \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$$

where each G_i / G_{i+1} is cyclic.

Today:

Thm: $f(x) \in F[x]$ is solvable by radicals iff $\text{Gal}(K/F)$ is solvable, where K is a splitting field for F.

Cor: When $\text{Gal}(K/F) = S_n$ for $n = \deg f$ and $n \geq 5$ then f is not solvable by radicals.

Thus, there is no "quintic formula". This was first shown by Abel in 1823 at the age of 20. He died of tuberculosis 6 years later. Galois himself died at age 20 in a dual in 1832.

Examples with $Gal(K/F)$ solvable

① $F(\sqrt{D})$

② $K = \mathbb{Q}(\zeta_n)$

Pf: K is the splitting field of $\Phi_n(x)$, hence Galois.

Consider

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \longrightarrow Gal(K/\mathbb{Q})$$

$$a \longmapsto (\sigma_a : \zeta_n \mapsto \zeta_n^a)$$

This is a homomorphism as $\sigma_{ab}(\zeta_n) = \zeta_n^{ab} = (\zeta_n^b)^a$

$= \sigma_a(\sigma_b(\zeta_n))$. This is clearly 1-1 and thus

onto since $|Gal(K/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Note: $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is abelian $\Rightarrow$ solvable. but not always

cyclic, e.g. $(\mathbb{Z}/8\mathbb{Z})^\times \cong$ Klein 4-gp.

Key Ex: K = splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ } Note: Definitely solvable by radicals!

$$\begin{array}{c} K \\ 3 \mid \\ L = \mathbb{Q}(\zeta_3) \\ 2 \mid \\ F = \mathbb{Q} \end{array}$$

as L is Galois

$$\{1\} \lhd Gal(K/L) \lhd Gal(K/F)$$

$$Gal(K/L) \cong C_3$$

$$Gal(K/F)/Gal(K/L) \cong Gal(L/F) \cong C_2$$

Thus $\mathrm{Gal}(K/F) \cong S_3 \cong D_6$ is solvable.

<u>Lemma</u>: 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, then so is $\mathrm{Gal}(K/F)$.

<u>Pf</u>: As L/F is Galois, $\mathrm{Gal}(K/L) \triangleleft \mathrm{Gal}(K/F)$ with quotient $\mathrm{Gal}(L/F)$. So have $H \triangleleft G$ with H and G/H solvable $\Rightarrow G$ is solvable. $\square$

<u>Assumption</u>: From now on, char $F = 0$.
[Not needed, but makes proof simpler]

<u>Lemma</u>: If K is the splitting field of $x^n - a \in F[x]$, then $\mathrm{Gal}(K/F)$ is solvable.

$$\begin{array}{c} K = F(\alpha, \zeta_n) \\ | \\ L = F(\zeta_n) \\ | \\ F \end{array}$$

<u>Pf</u>: Fix $\alpha \in K$ with $\alpha^n = a$. Then the roots of $x^n - a$ are $\alpha \zeta_n^k$ for $0 \leq k < n$.

<u>Claim 1</u>: $\mathrm{Gal}(L/F)$ is abelian

Claim 2: $\mathrm{Gal}(K/L)$ is cyclic of order dividing n.

Pf of 1: Any two $\sigma, \tau \in \mathrm{Gal}(L/F)$ have the form $\sigma(\zeta_n) = \zeta_n^a$ and $\tau(\zeta_n) = \zeta_n^b$. Hence $\sigma(\tau(\zeta_n)) = \zeta_n^{ab} = \tau(\sigma(\zeta_n))$.

Pf of 2: Define

$$\rho : \mathrm{Gal}(K/F) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$(\alpha \longmapsto \alpha\zeta_n^a) \longmapsto a$$

This is clearly 1-1 and is a homomorphism since $\forall \sigma, \tau \in \mathrm{Gal}(K/F)$ we have $\sigma(\tau(\alpha))$
$= \sigma(\alpha \zeta_n^{\rho(\tau)}) = \alpha \zeta_n^{\rho(\sigma)+\rho(\tau)}$ as $\sigma|_L = id_L$. ∎

Cor: If $f(x)$ is solvable by radicals, then $\mathrm{Gal}(K/F)$ is solvable.

Pf: Suppose $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s \supseteq K$ (splitting field of $f(x)$.)
with $K_{i+1} = K_i(\alpha_i)$ with α_i a root of $x^{n_i} - a_i$.
Set $L_0 = F$ and then L_{i+1} = splitting field of $x^{n_i} - a_i$ over L_i. Then $K \subseteq L_s = L$ and

$Gal(L/F)$ is solvable by the lemmas. As $Gal(K/F)$ is a quotient of $Gal(L/F)$, it too is solvable. $\square$

<u>Thm</u>: $f(x)$ is solvable by radicals $\iff$ $Gal(K/F)$ is solvable.

<u>Pf</u>: Assume $G = Gal(K/F)$ is solvable by

$$1 = G_s \triangleleft G_{s-1} \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$$

Setting $K_i = K_{G_i}$, get subfields

$$K = K_s \supseteq K_{s-1} \supseteq \cdots \quad \cdots \supseteq K_1 \supseteq K_0 = F$$

where K_{i+1}/K_i is Galois with group $G_{i+1}/G_i \cong C_{n_i}$.

Let $F' = F(\zeta_{n_1}, \ldots, \zeta_{n_s})$. Set $K_i' = K_i F'$

Now $Gal(F'/F)$ is certainly a root extension so it remains to show K_{i+1}'/K_i' is gotten by adjoining a root of some $x^{m_i} - a_i$.

Now $\mathrm{Gal}(K_{i+1}/K_i') \cong \mathrm{Gal}(K_{i+1}/K_{i+1} \cap K_i')$

which is a subgroup of $\mathrm{Gal}(K_{i+1}/K_i)$ and hence cyclic.

Prop 19 in §14.4 of [DF]

So we have reduced to

<u>Lemma</u>: Suppose K/F is Galois with group C_n. If $\zeta_n \in F$, then $K = F(\alpha)$ where $\alpha^n \in F$.

<u>Pf</u>: The Lagrange resultant of $\alpha \in K$ is

$$L(\alpha) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

where $\zeta = \zeta_n$ and σ is a generator for $\mathrm{Gal}(K/F)$.

Note that since $\sigma(\zeta) = \zeta$, we have

$$\sigma(L(\alpha)) = \zeta^{-1} L(\alpha) \Rightarrow \sigma(L(\alpha)^n) = L(\alpha)^n$$
$$\Rightarrow L(\alpha)^n \in F.$$

Moreover, if $L(\alpha) \neq 0$, then $\sigma^i(L(\alpha)) \neq L(\alpha)$ for all $1 \le i \le n-1$ $\Rightarrow L(\alpha)$ is not in any proper subfield of $K \Rightarrow K = F(L(\alpha))$.

So it remains to show $\exists\, \alpha$ for which $L(\alpha) \neq 0$. For this use linear independence of elements of $\mathrm{Gal}(K/F)$, see Thm 7 of §14.2 of [DF]