Applications

III : Proof of Galois' Great Theorem

Def'n (solvable by radicals)

A polynomial $f(x) \in F[x]$ is solvable by radicals if its splitting field K_f is contained in some radical extension.

Def'n (Solvable group)

A group G is called solvable if there is a sequence of subgroups

$$\{e_G\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{n-1} \leq H_n = G$$

so that $H_i \triangleleft H_{i+1}$ for all $0 \leq i < n$ and H_{i+1}/H_i is cyclic.

BIG RESULT!

Thm (Galois' Great Theorem)

Let $\mathrm{char}(F) = 0$, let $f(x) \in F[x]$, and let K_f be its splitting field. Then f is solvable by radicals iff $\mathrm{Gal}(K_f/F)$ is solvable.

New Stuff

Prove this result

We'll need

<u>Thm</u> (Kummer Theory)

Let $n \in \mathbb{N}$ and suppose F contains a primitive n^{th} root of unity ω_n. Then for an extension E/F has $Gal(E/F) \hookrightarrow \mathbb{Z}_n$ iff E is the splitting field for some $x^n - c \in F[x]$.

Note: we already know "$\Leftarrow$". We'll do "$\Rightarrow$" next time.

__Pf__ (Galois' Great Theorem)

Let's first assume $f(x) \in F[x]$ is solvable by radicals. We'll try to prove that $\mathrm{Gal}(K_f/F)$ is a solvable group.

By assumption we have a radical tower containing K_f:

$$
\begin{tikzcd}
 & & & & & K_f \arrow[d, hook] \\
F \arrow[r, hook] & E_1 \arrow[r, hook] \arrow[d, equal] & E_2 \arrow[r, hook] \arrow[d, equal] & \cdots \arrow[r, hook] & E_{s-1} \arrow[r, hook] & E_s = E \arrow[d, equal] \\
 & F(\sqrt[n_1]{e_1}) & E_1(\sqrt[n_2]{e_2}) & & & E_{s-1}(\sqrt[n_s]{e_s})
\end{tikzcd}
$$

We'll extend this picture by adjoining a $\left(N = \prod_{i=1}^{s} n_i\right)^{th}$ root of unity.

$$\begin{tikzcd}
\tilde F = F(\omega) \arrow[r, hook] & \tilde E_1 \arrow[r, hook] \arrow[d, phantom, sloped, "="] & \tilde E_2 \arrow[r, hook] \arrow[d, phantom, sloped, "="] & \cdots \arrow[r, hook] & \tilde E_{s-1} \arrow[rr, hook] & & \tilde E_s = \tilde E = \tilde E_{s-1}(\sqrt[n_s]{e_s}) \\
& \tilde F(\sqrt[n_1]{e_1}) & \tilde E_1(\sqrt[n_2]{e_2}) & & & K_f \arrow[ur, hook] \arrow[dr, hook] & \\
F \arrow[uu, hook] \arrow[r, hook] & E_1 \arrow[u, hook] \arrow[r, hook] \arrow[d, phantom, sloped, "="] & E_2 \arrow[u, hook] \arrow[r, hook] \arrow[d, phantom, sloped, "="] & \cdots \arrow[r, hook] & E_{s-1} \arrow[uu, hook] \arrow[rr, hook] & & E_s = E \arrow[uu, hook] \arrow[d, phantom, sloped, "="] \\
& F(\sqrt[n_1]{e_1}) & E_1(\sqrt[n_2]{e_2}) & & & & E_{s-1}(\sqrt[n_s]{e_s})
\end{tikzcd}$$

Note: for all $1 \le i \le s$, the field $\tilde F$ has a primitive n_ith root of unity ($\omega^{n_1 \cdots n_{i-1} n_{i+1} \cdots n_s}$). Hence for all i we get $\mathrm{Gal}(\tilde E_i / \tilde E_{i-1})$ is a subgroup of $\mathbb{Z}_{n_i}$ (hence cyclic) by Kummer Theory.

Our strategy: try to prove $\mathrm{Gal}(\tilde{E}/F)$ is solvable in order to argue $\mathrm{Gal}(K_f/F)$ is solvable.

(Recall: since K_f/F is Galois, we get that

$$\mathrm{Gal}(\tilde{E}/F) \big/ \mathrm{Gal}(\tilde{E}/K_f) \simeq \mathrm{Gal}(K_f/F).$$

Our deepish Theorem from last time said quotients of solvable groups are solvable.)

So: we'll try to show $Gal(\tilde{E}/F)$ is solvable.

We'll first focus on $\tilde{G} = Gal(\tilde{E}/\tilde{F})$.

(Fun exercise: $\tilde{E}/F$ and $\tilde{E}/\tilde{F}$ are both Galois.)

Note: $\tilde{G} \leq Gal(\tilde{E}/F)$.

We'll show $\tilde{G}$ is solvable.

Let $H_i = Gal(\tilde{E}/\tilde{E}_{s-i})$. So, for example

$$H_0 = Gal(\tilde{E}/\tilde{E}_s) = Gal(\tilde{E}/\tilde{E}) = \{e\}.$$

We then get

$$
\begin{array}{ccccccccccc}
\{e\} & \subseteq & \mathrm{Gal}(\tilde{E}/\tilde{E}_{s-1}) & \subseteq & \mathrm{Gal}(\tilde{E}/\tilde{E}_{s-2}) & \subseteq & \cdots & \subseteq & \mathrm{Gal}(\tilde{E}/\tilde{E}_1) & \subseteq & \mathrm{Gal}(\tilde{E}/\tilde{E}_0) \\
\parallel & & \parallel & & \parallel & & & & \parallel & & \parallel \\
H_0 & \subseteq & H_1 & \subseteq & H_2 & \subseteq & \cdots & \subseteq & H_{s-1} & \subseteq & H_s = \tilde{G}
\end{array}
$$

The fundamental Theorem says $H_i \triangleleft H_{i+1}$ iff

$\tilde{E}_{s-i}/\tilde{E}_{s-i-1}$ is a Galois extension. But Kummer

Theory tells us it is Galois, and even $\mathrm{Gal}(\tilde{E}_{s-i}/\tilde{E}_{s-i-1})$

are subgroups of $\mathbb{Z}_{n_i}$ (and hence cyclic). But note

$$H_{i+1}/H_i = \mathrm{Gal}(\tilde{E}/\tilde{E}_{s-i-1}) \big/ \mathrm{Gal}(\tilde{E}/\tilde{E}_{s-i}) \simeq \mathrm{Gal}(\tilde{E}_{s-i}/\tilde{E}_{s-i-1})$$

which we know is cyclic.

So: $\tilde{G}$ is solvable.

Now to show $\mathrm{Gal}(\tilde{E}/F)$ is solvable, note $\tilde{F} = F(\omega)/F$ is Galois, and so by Galois correspondence we get

$$\underset{\substack{\| \\ \tilde{G}}}{\mathrm{Gal}(\tilde{E}/\tilde{F})} \triangleleft \mathrm{Gal}(\tilde{E}/F).$$

So from previous work we get:

$$\begin{array}{ccccccccccc}
\{e\} & \le & \mathrm{Gal}(\tilde{E}/\tilde{E}_{s-1}) & \le & \mathrm{Gal}(\tilde{E}/\tilde{E}_{s-2}) & \le \cdots \le & \mathrm{Gal}(\tilde{E}/\tilde{E}_1) & \le & \overbrace{\mathrm{Gal}(\tilde{E}/\tilde{E}_0) \le \mathrm{Gal}(\tilde{E}/F)}^{\text{normal subgroup with quotient is } \mathrm{Gal}(\tilde{F}/F)} \\
\| & & \| & & \| & & \| & & \| \\
H_0 & \le & H_1 & \le & H_2 & \le \cdots \le & H_{s-1} & \le & H_s = \tilde{G}
\end{array}$$

Since all "lower layers" of this chain satisfy the solvability property, and since the "new" top layer also satisfies the condition, we have $\mathrm{Gal}(\tilde{E}/F)$ is solvable.

$\blacksquare$

For the second half:

assume $Gal(K_f/F)$ is solvable, and we want f is solvable by radicals.

let $N = [K_f : F]$, and let ω be a $N!$ th of unity.

let $\tilde{F} = F(\omega)$. We can define $\tilde{K}_f = K_f(\omega)$.

<u>Claim:</u> $Gal(\tilde{K}_f/\tilde{F})$ is (isomorphic to) a subgroup of $Gal(K_f/F)$. (Strategy: create injective hom.)

Let $\sigma \in \mathrm{Gal}(\tilde{K_f}/\tilde{F})$ be given. Define $\psi(\sigma) = \sigma|_{K_f}$.

Is $\psi(\sigma) \in \mathrm{Gal}(K_f/F)$? Since σ fixes elements in $\hat{F}$, and since $F \subseteq \tilde{F}$, we have $\psi(\sigma)$ fixes elements in F. To show $\psi(\sigma)$ is an element of $\mathrm{Aut}(K_f)$, we only have to check that $\sigma(K_f) = K_f$.

Since K_f/F is Galois, we know its only conjugate in $\hat{K_f}$ is itself, so $\sigma(K_f) = K_f$.

Let's check injectivity. Let $\sigma_1, \sigma_2 \in \mathrm{Gal}(\tilde{K}_f / \tilde{F})$ be given so that $\psi(\sigma_1) = \psi(\sigma_2)$, Then $\sigma_1 = \sigma_2$.

We know $K_f = F(\alpha_1, \ldots, \alpha_n)$ for appropriate $\alpha_1, \ldots, \alpha_n$, so that $\tilde{K}_f = F(\omega, \alpha_1, \ldots, \alpha_n)$.

Since $\psi(\sigma_1) = \psi(\sigma_2)$, we know $\sigma_1(k) = \sigma_2(k)$ for any $k \in K_f$. In particular we know $\sigma_1(\alpha_i) = \sigma_2(\alpha_i)$ for all $1 \leq i \leq n$. But since $\mathrm{Gal}(\tilde{K}_f / \tilde{F})$ fixes ω, we have $\sigma_1(\omega) = \sigma_2(\omega)$. Since elements of $\mathrm{Gal}(\tilde{K}_f / \tilde{F})$ are determined by their action on generators of $\tilde{K}_f$, we get $\sigma_1 = \sigma_2$.

We now have $\mathrm{Gal}(\tilde{K}_f/\tilde{F})$ is a subgroup of $\mathrm{Gal}(K_f/F)$. Note also $[\tilde{K}_f : \tilde{F}] \le [K_f : F] = N$.

By our deepish Theorem, we get $\mathrm{Gal}(\tilde{K}_f/\tilde{F})$ is solvable: There exist subgroups $\{H_i\}_{i=0}^{\ell}$

$$\{e\} = H_0 \le H_1 \le H_2 \le \cdots \le H_{\ell-1} \le H_\ell = \tilde{G} = \mathrm{Gal}(\tilde{K}_f/\tilde{F})$$

so that $H_i \triangleleft H_{i+1}$ and H_{i+1}/H_i is cyclic.

Now we'll use the Galois correspondence on this chain of subgroups

groups

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{\ell-1} \leq H_\ell = \tilde{G} = \mathrm{Gal}(\tilde{K}_f/\tilde{F})$$

so that $H_i \triangleleft H_{i+1}$ and H_{i+1}/H_i is cyclic.

$$\Big\downarrow \mathcal{F}$$

$$\tilde{K}_f = \tilde{K}_\ell \hookleftarrow \tilde{K}_{\ell-1} \hookleftarrow \tilde{K}_{\ell-2} \hookleftarrow \cdots \hookleftarrow \tilde{K}_1 \hookleftarrow \tilde{F}$$

and $\tilde{K}_{i+1}/\tilde{K}_i$ is Galois and $\mathrm{Gal}(\tilde{K}_f/\tilde{K}_i)\big/\mathrm{Gal}(\tilde{K}_f/\tilde{K}_{i+1}) \cong \mathrm{Gal}(\tilde{K}_{i+1}/\tilde{K}_i)$

Since $\mathrm{Gal}(K_{i+1}/K_i)$ is cyclic, we get from Kummer Theory that $K_{i+1} = K_i(\sqrt[n_i]{k_i})$ for some $k_i \in K_i$. Hence we have

$$\tilde{F} \hookrightarrow \tilde{K}_f \quad \text{is a radical tower.}$$

But $\tilde{F} = F(\omega) = F(\sqrt[N!]{1})$, so in fact

$$F \hookrightarrow \tilde{F} \hookrightarrow \tilde{K}_f \quad \text{is a radical tower}$$

containing K_f. Hence f is solvable. $\blacksquare$