Lecture 16: Solvability by Radicals

Aim Lecture: Give Galois's nec. criterion for solvability by radicals.

This lecture, char $F=0$.

Galois's Criterion

Recall Thm Lect. 12

Thm 1: Consider radical tower

$$F=F_0 \subset F_1 \subset F_2 \subset \dots \subset F_n = K \quad \dots\dots (*)$$

where $F_{i+1} = F_i(\sqrt[p_i]{\alpha_i})$, $\alpha_i \in F_i$, p_i prime (so p_i are prime divisors of $[K:F]$). Suppose

ⓐ All $x^{p_i}-1$ split in F

& ⓑ K/F is Galois.

Then $G = Gal(K/F)$ is solvable.

Seek to remove hypotheses ⓐ & ⓑ.

Thm 2: Let K/F = field ext$^{\underline{n}}$ s.t. there's a field ext$^{\underline{n}}$ L/K with L/F radical ie. K/F embeds in a radical ext$^{\underline{n}}$. Then $G = Gal(K/F)$ is solvable.

$$\begin{array}{c} L \\ \cup\!\!\mid \\ K \\ \cup\!\!\mid \\ F \end{array}$$

Rem: Thm 2 true for char $F>0$ if one also assumes L/F separable.

Proof: Claim: It suffices to prove thm 2 when $K=L$ & K/F is Galois.

Why? We may replace K/F with K/K^G $\because$ they have the same Galois group &

L/K^G is still radical. $\therefore$ Can assume K/F is Galois.

Let $\tilde{L}$ = Galois closure of L/F.

Now $\tilde{L}/F$ is radical by Lect. 11 Prop^n 2.

Replacing L with $\tilde{L}$, we can assume L/F is Galois.

If thm 2 holds for L/F i.e. $Gal(L/F)$ is solvable, then the quotient $Gal(K/F)$ is solvable too & thm 2 is proved in general. $\square$

Assume hypotheses in Claim. Consider a radical tower in Thm 1 $(*)$. Suppose K is splitting field of $f(x)/F$ & let $g(x) = \prod_{i=1}^{n} (x^{p_i} - 1)$.

$$\begin{tikzcd}
 & K_1 \arrow[dl, dash, "\supseteq"'] \arrow[dr, dash, "\substack{\text{radical Galois}\\ \text{solvable group}}"] & \\
K \arrow[dr, dash, "\text{Gal}"'] & & F_1 \arrow[dl, dash, "\substack{\text{Gal. abelian}\\ \text{Galois group}}"] \\
 & F &
\end{tikzcd}$$

Let K_1 = splitting field of $g(x)/K$

$\quad$ = " " " $f(x)g(x)/F$.

$\therefore K_1/F$ Galois.

Let $F_1 \subseteq K_1$ be splitting field of $g(x)/F$.

K_1/F Galois $\Rightarrow K_1/F_1$ Galois.

K/F radical $\Rightarrow K_1/F_1$ radical.

$\therefore$ Thm 1 $\Rightarrow N = \mathrm{Gal}(K_1/F_1)$ solvable subgroup of $\mathrm{Gal}(K_1/F) =: G_1$.

Also F_1/F Galois $\Rightarrow N \trianglelefteq G_1$ & $G_1/N \simeq \mathrm{Gal}(F_1/F)$ abelian by Lect. 9 Lemma.

Hence G_1 is solvable as must be its quotient $\mathrm{Gal}(K/F)$. $\square$

Insolvability of the general quintic

Let F = field (not nec. char 0)

Def$^{\underline{n}}$: Let $f(x) \in F[x]$ & K = splitting field for $f(x)/F$. The Galois group of $f(x)/F$ is

$$\mathrm{Gal}(f(x)/F) = \mathrm{Gal}(K/F).$$

We say $f(x)$ is solvable by radicals $/F$ if K/F embeds in a radical ext$^{\underline{n}}$.

E.g. 1 $f(x) = x^3 - 2$ is solvable by radicals $/\mathbb{Q}$ $\because$ splitting field $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ is a radical ext$^{\underline{n}}$ of $\mathbb{Q}$. $\mathrm{Gal}(x^3-2/\mathbb{Q}) \simeq S_3$.

E.g. 2. General polynomial.

Let $\alpha_1, \dots, \alpha_n$ be indeterminates to be thought of as roots of a general deg n polynomial. Let

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_n).$$

Consider the general monic deg n poly

$$K[x] \ni g(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$
$$= x^n - a_1 x^{n-1} + a_2 x^{n-2} - \dots + (-1)^n a_n$$

where $a_1 = \alpha_1 + \dots + \alpha_n$,

$a_2 = \sum_{i<j} \alpha_i \alpha_j, \dots, \quad a_n = \alpha_1 \alpha_2 \dots \alpha_n$.

Now S_n permutes the α_i so acts on K.
Furthermore $(\sigma g)(x) = g(x)$ so all $a_i \in K^{S_n}$.
Define $F = \mathbb{Q}(a_1, \dots, a_n)$.

<u>Thm</u> (Abel-Ruffini)

(a) $F = K^{S_n}$ so $\mathrm{Gal}(g(x)/F) = S_n$.

(b) For $n \geq 5$, $g(x)$ is not solvable by by radicals $/\mathbb{Q}(a_1, \dots, a_n)$

Proof: Thm 2 shows (a) $\Rightarrow$ (b) so we prove (a).
We have seen $F \subseteq K^{S_n}$ so it suffices to show $[K:F] \leq [K:K^{S_n}] = |S_n|$.
Now K is clearly the splitting field of $g(x)/F$ so K/F is Galois & $G = \mathrm{Gal}(K/F)$ embeds in S_n. $\therefore$
$[K:F] = |G| \leq |S_n|$. $\square$

<u>Layman's Interpretation:</u> If there were a formula for the gen. quintic (or sextic etc.) using only $+, -, \times, \div, \sqrt[m]{\ }$ & co-eff then that formula shows the α_i & hence K lies in a radical ext$^{\underline{n}}$ of F. $\therefore$ There is no such formula.