Solvability by radicals

Recall:

Def: $f(x) \in F[x]$ is <u>solvable by radicals</u> if $\exists$

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = Sp_F f$$

where $K_{i+1} = K_i(\alpha_i)$ w/ α_i a root of $x^{n_i} - a_i$

Def: A finite gp. G is <u>solvable</u> if

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

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

Assume char $F = 0$

Thm (Galois):

a) $f(x)$ is solvable by radicals $\iff$ Gal f is a solvable gp

b) $\exists$ a degree 5 poly. which is not solvable by radicals.

Lemma 1:

a) If $H \leq G$, then G solvable $\Rightarrow$ H solvable

b) If $H \trianglelefteq G$, then H solvable, G/H solvable $\Rightarrow$ G solvable

Pf:

a) Let $\{1\} = G_s \triangleleft G_{s-1} \triangleleft \cdots \triangleleft G_0 = G$

where G_i/G_{i+1} is cyclic, and let $H_i = H \cap G_i$

Then $H_{i+1} \triangleleft H_i$ and H_{i+1}/H_i is isom to a subgp. of G_{i+1}/G_i, so is cyclic.

b) $$1 = H_s \triangleleft H_{s-1} \triangleleft \cdots \triangleleft H_0 = H$$

$$1 = J_r \triangleleft J_{r-1} \triangleleft \cdots \triangleleft J_r = G/H$$

If $\pi : G \to G/H$, then

$$1 = H_s \triangleleft \cdots \triangleleft H_0 = \pi^{-1}(J_r) \triangleleft \pi^{-1}(J_{r-1}) \triangleleft \cdots \triangleleft \pi^{-1}(J_1) = G$$

cyclic

$\square$

Example: $K = Sp_{\mathbb{Q}}(x^3-2)$

$$\begin{tikzcd}
K \arrow[d, dash, "3"'] & & 1 \arrow[d, dash, "3"'] \\
\mathbb{Q}(\zeta_3) \arrow[d, dash, "2"'] & \leftrightarrow & C_3 \arrow[d, dash, "2"'] \\
\mathbb{Q} & & S_3
\end{tikzcd}$$

$$\begin{array}{ccccc}
\mathrm{Gal}(K/K) & \triangleleft & \mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) & \triangleleft & \mathrm{Gal}(K/\mathbb{Q}) \\
1 & \triangleleft & C_3 & \triangleleft & S_3
\end{array}$$

Lemma 2: If $F \subseteq E \subseteq K$ w/ K/F, E/F Galois, then $\mathrm{Gal}(K/E), \mathrm{Gal}(E/F)$ solvable $\Rightarrow \mathrm{Gal}(K/F)$ solvable

Pf: Since E/F Galois, by Property 4 of the Fun. Thm., $\mathrm{Gal}(K/E) \triangleleft \mathrm{Gal}(K/F)$ and $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F) / \mathrm{Gal}(K/E)$

By part b of earlier prop, $\mathrm{Gal}(K/F)$ is solvable. $\square$

Remark: Galois gps. of ext'ns of finite fields are always cyclic, so always solvable by radicals (just take a finite field of the correct degree).

Lemma 3: Let char $F=0$. If $a \in F$, $K = Sp_F\, x^n - a$, then $\mathrm{Gal}(K/F)$ is solvable.

Pf: K is the splitting field of a sep. poly, so K/F is Galois. In particular, if α is a root of $x^n - a$, then the roots are

$$\{\alpha \zeta_n^k \mid 0 \leq k < n\}$$

Let $E = F(\zeta_n)$. $\mathrm{Gal}(E/F)$ is abelian since it's isom. to a subgp. of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Furthermore, the map

$$\begin{aligned} \mathrm{Gal}(K/E) &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ (\alpha \mapsto \alpha \zeta_n^k) &\longmapsto k \end{aligned}$$

is an inj. homom., so $\mathrm{Gal}(K/E)$ is cyclic. By the lemma, $\mathrm{Gal}(K/F)$ is solvable.

$\square$

Lemma 4: K/F Galois w/ $\mathrm{Gal}(K/F) = C_n$. If $\zeta_n \in F$, then $K = F(\alpha)$ for some $\alpha \in K$ with $\alpha^n \in F$.

Pf sketch: Consider the Lagrange resolvent of $\alpha \in K$:

$$\beta := L(\alpha) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) \qquad \begin{array}{l}\zeta := \zeta_n \\ \sigma: \text{gen.}\end{array}$$

Since $\sigma(\zeta) = \zeta$,

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

So $\sigma(\beta^n) = \beta^n$ i.e. $\beta^n \in F$.

Conversely, if $\beta \neq 0$, then $F(\beta) = K$ since $\sigma^i(\beta) = \zeta^{-i}\beta \neq \beta$ for all $1 \le i < n$, so $\mathrm{Aut}(K/F(\beta)) = \mathrm{id}$.

By D&F Thm 14.7, elts. of $\mathrm{Gal}(K/F)$ are linearly independent, so $\exists\, \alpha$ s.t. $L(\alpha) \neq 0$.

$\square$

Pf of Galois' Thm part a:

If $f \in F[x]$ is solvable by radicals, then

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s \supseteq K = Sp_F f$$

w/ $K_{i+1} = K_i(\alpha_i)$, with α_i a root of $x^{n_i} - a_i$, $a_i \in K_i$

Let

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

where $L_{i+1} = Sp_{L_i}(x^{n_i} - a_i)$. Then $K_i \subseteq L_i$ $\forall i$, so

$Sp_F f \subseteq K_s \subseteq L_s$. By Lemma 3, $Gal(L_{i+1}/L_i)$

is solvable, so by Lemma 2, $Gal(L/F)$ is solvable. Since K/F is Galois, by the Fun. Thm. prop. 4, $Gal(K/F)$ is a quotient of $Gal(L/F)$,

so by Lemma 1, it is solvable

Conversely, if $G = Gal(K/F)$ is solvable

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

cyclic quotients

Let $K_i = \mathrm{Fix}\, G_i$, and

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

K_{i+1}/K_i is Galois by Fun. Thm. prop 4 w/

$$\mathrm{Gal}(K_{i+1}/K_i) \cong \mathrm{Gal}(K/K_i)/\mathrm{Gal}(K/K_{i+1})$$
$$= G_i/G_{i+1} \cong C_{n_i} \text{ for some } i.$$

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

We have

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

adjoin roots of 1

By Lemma 4, $K_{i+1}' = K_i'(\alpha)$, α a root of $x^{n_i} - a_i$, $a_i \in K_i'$,

so f is solvable by radicals.

$\square$