Solvability by radicals

Recall: $f(x) \in F[x]$ is __solvable by radicals__ 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 __solvable__ if

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

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

Remark: Galois gps. of extns of finite fields are always cyclic, and polys are always solvable by radicals (just take a finite field of the correct degree).

Assume char $F = 0$ henceforth

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.

Today: series of lemmas leading up to this result

Lemma 1:

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

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

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

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

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

cyclic

$\square$

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

$$
\begin{array}{ccc}
K & & 1 \\
3 \mid & & 3 \mid \\
\mathbb{Q}(\mathfrak{z}_3) & \leftrightarrow & C_3 \\
2 \mid & & 2 \mid \\
\mathbb{Q} & & S_3
\end{array}
$$

$\mathrm{Gal}(K/K) \vartriangle \mathrm{Gal}(K/\mathbb{Q}(\mathfrak{z}_3)) \vartriangle \mathrm{Gal}(K/\mathbb{Q})$

$\quad\quad 1 \vartriangle \quad\quad C_3 \quad\quad \vartriangle S_3$

Lemma 2: If $F \leq E \leq K$ w/ K/F, E/F Galois, then

$\mathrm{Gal}(K/E)$, $\mathrm{Gal}(E/F)$ soluable $\Rightarrow \mathrm{Gal}(K/F)$ soluable

Pf: Since E/F Galois, by property 4 of the Fun. Thm.,

$\mathrm{Gal}(K/E) \vartriangle \mathrm{Gal}(K/F)$ and $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)\big/ \mathrm{Gal}(K/E)$

By part b of Lemma 1, $\mathrm{Gal}(K/F)$ is solvable.

$\square$

Lemma 3: If $a \in F$, $K = Sp_F \, x^n - a$, then $Gal(K/F)$ 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

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

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

Furthermore, the map
$$Gal(K/E) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$(\alpha \mapsto \alpha \, \zeta_n^k) \longmapsto k$$

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

Lemma 4: K/F Galois w/ $\text{Gal}(K/F) = C_n$. 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 $\alpha \in K$:

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

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
$$\sigma^i(\beta) = \zeta^{-i} \beta \neq \beta \quad \text{for all } 1 \leq i < n, \text{ so}$$
$\text{Aut}(K/F(\beta)) = \text{id}$.

By D&F Thm 14.7, elts. of $\text{Gal}(K/F)$ 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

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

cyclic quotients

Let $k_i = \text{Fix } G_i$, 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/

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

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.

$\square$