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 ext'ns 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 $H \trianglelefteq G$, 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/H_{i+1} is isom to a subgp. of G_i/G_{i+1}, so is cyclic.

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

$$1 = J_r \triangleleft J_{r-1} \triangleleft \cdots \triangleleft J_0 = G/H$$

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

$$1 = H_s \triangleleft \cdots \triangleleft H_0 \overset{\text{"}H\text{"}}{=} \pi^{-1}(J_r) \triangleleft \pi^{-1}(J_{r-1}) \triangleleft \cdots \triangleleft \pi^{-1}(J_0) = G$$

cyclic

$\square$

Example, leading to the next lemma: $K = Sp_{\mathbb{Q}}(x^3-2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

Galois w/ Gal. gp. S_3

Galois w/ Gal. gp. C_3

Galois w/ Gal. gp C_2

$$\begin{array}{ccc} K & \cdots & 1 \\ 3\,\big| & & 3\,\big| \\ \mathbb{Q}(\zeta_3) & \cdots & C_3 \\ 2\,\big| & & 2\,\big| \\ \mathbb{Q} & \cdots & S_3 \end{array}$$

$$\left.\begin{array}{c} 1 \\ 3\,\big| \\ C_3 \end{array}\right\} C_3 \qquad \left.\begin{array}{c} C_3 \\ 2\,\big| \\ S_3 \end{array}\right\} C_2 \qquad \left.\begin{array}{c} 1 \\ \big| \\ S_3 \end{array}\right\} S_3$$

$$\mathrm{Gal}(K/K) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$$

$$1 \trianglelefteq C_3 \trianglelefteq S_3$$

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.,

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

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

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

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

$\square$

* Some maps $\alpha \mapsto \alpha \zeta_n^k$ might not lead to valid automorphisms, but all valid automorphisms are determined by the integer k

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

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. $\beta^n \in F$, and $F(\beta) \subseteq K$.

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 $\mathrm{Aut}(K/F(\beta)) = \mathrm{id}$.

Therefore, we just need $\alpha \in K$ with $L(\alpha) \neq 0$. This follows from D&F Thm 14.7: elts. of $\mathrm{Gal}(K/F)$ are linearly independent functions, so the function $\alpha \mapsto L(\alpha)$ cannot be the zero function

$\square$