

Solvability by radicals

Recall:

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

$$F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_s = \text{Sp}_F f$$

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

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

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

Assume $\text{char } F = 0$ henceforth

Thm (Galois):

a) $f(x)$ is solvable by radicals $\iff \text{Gal } f$ 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 $\{1\} = G_s \triangleleft G_{s-1} \triangleleft \dots \triangleleft G_0 = G$

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

$1 = J_r \triangleleft J_{r-1} \triangleleft \dots \triangleleft J_1 = G/H$

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

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

\nwarrow cyclic \nearrow

□

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

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

$$\begin{array}{ccccc}
 \text{Gal}(K/K) & \triangleleft & \text{Gal}(K/\mathbb{Q}(\mathfrak{f}_3)) & \triangleleft & \text{Gal}(K/\mathbb{Q}) \\
 1 & \triangleleft & C_3 & \triangleleft & S_3
 \end{array}$$

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

$\text{Gal}(K/E), \text{Gal}(E/F)$ solvable $\Rightarrow \text{Gal}(K/F)$ solvable

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

$$\text{Gal}(K/E) \triangleleft \text{Gal}(K/F) \text{ and } \text{Gal}(E/F) \cong \text{Gal}(K/F) / \text{Gal}(K/E)$$

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

□

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

Lemma 3: If $a \in F$, $K = S_{p_F} x^n - a$, then $\text{Gal}(K/F)$ 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 $E = F(\zeta_n)$. $\text{Gal}(E/F)$ is abelian since it's isom. to a subgp. of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Furthermore, the map

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

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 $\beta_n \in F$, then $K = F(\alpha)$ for some $\alpha \in K$ with $\alpha^n \in F$.

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

$$\beta := L(\alpha) := \alpha + \gamma \sigma(\alpha) + \gamma^2 \sigma^2(\alpha) + \dots + \gamma^{n-1} \sigma^{n-1}(\alpha) \quad \begin{array}{l} \gamma := \beta_n \\ \sigma: \text{gen.} \end{array}$$

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

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

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

Conversely, if $\beta \neq 0$, then $F(\beta) = K$ since

$$\sigma^i(\beta) = \gamma^{-i} \beta \neq \beta \text{ for all } 1 \leq i < n, \text{ so}$$

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

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

$$F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_s \supseteq K = \text{Sp}_F f$$

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

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


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

$\text{Sp}_F f \subseteq K_s \subseteq L_s$. By Lemma 3, $\text{Gal}(L_{i+1}/L_i)$ is solvable, so by Lemma 2, $\text{Gal}(L/F)$ is solvable. Since K/F is Galois, by the Fun. Thm. prop. 4, $\text{Gal}(K/F)$ is a quotient of $\text{Gal}(L/F)$,

so by Lemma 1, it is solvable

Conversely, if $G = \text{Gal}(K/F)$ is solvable

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


cyclic quotients

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

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

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

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

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

We have

$$F \subseteq F' = K'_0 \subseteq K'_1 \subseteq \dots \subseteq K'_s \supseteq K$$

\uparrow
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.

□