Solvability

Work over $\mathbb{Q}$. A polynomial $f(x) \in \mathbb{Q}[x]$ is solvable by radicals if $\exists k \in \mathbb{N}$ and a sequence of fields

$F_0 \subseteq \cdots \subseteq F_k$ s.t.:

i) $F_0 = \mathbb{Q}$ and F_k contains the splitting field of $f(x)$

ii) $\forall\, 1 \le i \le k$, $\exists\, \alpha_i \in \mathbb{C}$, $m_i \in \mathbb{N}$ s.t. $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{m_i} \in F_{i-1}$.

There is a close connection between solvability by radicals and solvable groups:

A group G is solvable if $\exists k \in \mathbb{N}$ and a sequence of subgroups $H_k \le H_{k-1} \le \cdots \le H_0$ with:

i) $H_k = \{id\}$, $H_0 = G$,

ii) $\forall\, 1 \le i \le k$, $H_i \trianglelefteq H_{i-1}$ and H_{i-1}/H_i is Abelian.

In order to tell whether or not a group is solvable, look at its commutator subgroups:

$\forall g, h \in G$, the commutator of g and h is

$$[g,h] = g^{-1}h^{-1}gh.$$

The commutator subgroup of G, denoted G' or $G^{(1)}$ is

$$G' = \langle [g,h] \mid g,h \in G \rangle.$$

Lemma: i) $G' \trianglelefteq G$ and G/G' is Abelian.

ii) If $H \trianglelefteq G$ and G/H is Abelian, then $G' \leq H$.

Pf: i) Suppose $g' \in G'$, $g \in G$,

$$g g' g^{-1} = g'(g'^{-1} g g' g^{-1}) = g' [g', g^{-1}] \in G'$$

$\Rightarrow G' \trianglelefteq G$.

Suppose $gG', hG' \in G/G'$ then

$$(gG')(hG') = ghG' = hg[g,h]G'$$

$$= hgG' = (hG')(gG')$$

$\Rightarrow G/G'$ is Abelian.

ii) $\forall g,h \in G$, $(gh)H = (hg)H \Rightarrow [g,h] \in H$. $\blacksquare$

Def: $\forall i \geq 2$, let $G^{(i)} = (G^{(i-1)})'$.

Thm: G is solvable iff $G^{(\ell)} = \{id\}$ for some $\ell \in \mathbb{N}$.

Pf: If $G^{(\ell)} = \{id\}$ for some ℓ, then it follows from the def that G is solveable.

For the other direction, suppose G is solvable with $H_0, \ldots, H_k$ as in the def. Then $H_1 \trianglelefteq G$ and G/H_1 is Abelian $\Rightarrow G' \leq H_1$. Similarly, $H_2 \trianglelefteq H_1$ and H_1/H_2 Abelian $\Rightarrow G^{(2)} \leq H_2$.

Continuing, $G^{(i)} \leq H_i$ for each i, so $G^{(k)} = \{id\}$. ☒

Cor: If G is solvable and $\varphi: G \to H$ is a homom. then $\varphi(G)$ is solvable.

Pf: Let $\tilde{G} = \varphi(G)$. Then $\tilde{G}^{(i)} = \varphi(G^{(i)})$.

But G is solvable $\Rightarrow G^{(\ell)} = \{id\}$ for some ℓ

$\Rightarrow \tilde{G}^{(\ell)} = \varphi(G^{(\ell)}) = \{id\} \Rightarrow \tilde{G}$ is solvable. ☒

Thm: Suppose $f \in \mathbb{Q}[x]$ is solvable by radicals, and let K be its splitting field over $\mathbb{Q}$. Then $\mathrm{Gal}(K/\mathbb{Q})$ is solvable.

f solv. by rads:

$$\begin{array}{ll}
K \subseteq F_k = F_{k-1}(\alpha_k), & \alpha_k^{m_k} \in F_{k-1} \\
\quad \vdots & \quad \vdots \\
F_2 = F_1(\alpha_2), & \alpha_2^{m_2} \in F_1 \\
\quad | & \\
F_1 = F_0(\alpha_1), & \alpha_1^{m_1} \in F_0 = \mathbb{Q} \\
\quad | & \\
F_0 = \mathbb{Q} &
\end{array}$$

Before proving this:

Ex: (cont. #6 from Lecture 17)

$f(x) = x^5 - 4x + 2$, K = spl. field of f of $\mathbb{Q}$,

$G = \mathrm{Gal}(K/\mathbb{Q}) = S_5$.

Claim 1: $G' = A_5$.

Pf: $\forall\, \sigma, \tau \in G$, $[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau \in A_5 \Rightarrow G' \subseteq A_5$.

$[(i\,j), (j\,k)] = (i\,j)(j\,k)(i\,j)(j\,k) = (i\,k\,j)$,

so G' contains all 3-cycles $\Rightarrow G' = A_5$. $\blacksquare$

(3-cycles generate A_5)

Claim 2: A_5 is simple.

Conclusion: S_5 is not solvable $\Rightarrow f$ is not solvable by radicals.

On the way to proving the Thm:

Lemma: Suppose $K = F(\alpha)$ for some $\alpha \in K$ with $\alpha^m \in F$. If F contains all mth roots of unity then K/F is Galois and $\mathrm{Gal}(K/F)$ is Abelian.

Pf: K is the splitting field of $x^m - \alpha^m \in F[x]$, so K/F is Galois. Elements of $\mathrm{Gal}(K/F)$ are determined by where they map α, and the choices are $\alpha \mapsto \alpha \zeta_m^i$ for some i.

Suppose $\sigma, \tau \in \mathrm{Gal}(K/F)$, $\sigma(\alpha) = \alpha \zeta_m^i$, $\tau(\alpha) = \alpha \zeta_m^j$.

Then $(\sigma\tau)(\alpha) = \sigma(\alpha \zeta_m^j) = \sigma(\alpha)\sigma(\underbrace{\zeta_m^j}_{\in F}) = \sigma(\alpha)\zeta_m^j$

$$= \alpha \zeta_m^{i+j} = \cdots = (\tau\sigma)(\alpha)$$

$\Rightarrow \mathrm{Gal}(K/F)$ is Abelian. $\boxtimes$