Lecture 41: Not solving equations by radicals

§14.7. of [DF]

Def: $f \in F[x]$ is solvable by radicals if there exist $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s$ where each $K_{i+1} = K_i(\alpha_i)$ with α_i a root of $x^{n_i} - a_i \in K_i[x]$ and f splits completely in K_s.

Thm $f \in F[x]$ with $\mathrm{char}(F) = 0$ is solv. by radicals $\iff$ $\mathrm{Gal}(K/F)$ is solvable, where K is a splitfield of f.

Cor: If $\mathrm{Gal}(K/F) = S_n$ for $n \geq 5$ then f is not solvable by radicals.

Lemma: Suppose K is the split field of $f(x) = x^n - a \in F[x]$, where $\mathrm{char}\, F$ is either 0 or coprime to n. Then $\mathrm{Gal}(K/F)$ is solvable.

Pf: Assume char = 0.

Saw last time that $x^n - 1$ splits comp in K;

let ζ_n be a primitive n^{th} root of unity,

$$\begin{array}{c} K = F(\alpha, \zeta_n) \\ | \\ L = F(\zeta_n) \\ | \\ F \end{array}$$

α any root $x^n - a$. Then all the roots of $x^n - a$ are $\alpha \zeta_n^k$ for $0 \le k < n$

Claims ① $Gal(L/F)$ is abelian

② $Gal(K/L)$ is cyclic.

[This proves the lemma using that this implies $Gal(K/F)$ is solvable, as discussed last time.]

Pf of ①: Any two $\sigma, \tau \in Gal(L/F)$ have the form $\sigma(\zeta_n) = \zeta_n^a$ and $\tau(\zeta_n) = \zeta_n^b$.

Hence $\sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = \zeta_n^{ab} = \tau(\sigma(\zeta_n))$,

and so $\sigma\tau = \tau\sigma$.

Pf of ②: Define $\rho : Gal(K/L) \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$(\alpha \longmapsto \alpha \zeta_n^a) \longmapsto a$$

This is injective and a homomorphism, since

$\forall \sigma, \tau \in Gal(K/F)$ we have $\sigma(\tau(\alpha)) =$

$$\sigma(\alpha \zeta_n^{\rho(\tau)}) = \sigma(\alpha)\zeta_n^{\rho(\tau)} = \alpha \zeta_n^{\rho(\sigma)+\rho(\tau)}$$

$$= \alpha \zeta_n^{\rho(\sigma\tau)} \quad \text{as } \sigma|_L = id_L.$$

▨

Cor: If $f(x)$ is solvable by radicals, then $Gal(K/F)$ is solvable.

[One half of Thm on page (1), gives the cor.]

Pf: Suppose $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s$ with $K_{i+1} = K_i(\alpha_i)$ with α_i a root of $x^{n_i} - a_i \in K_i[x]$ and K = split field of $f \subseteq K_s$.

Starting from $L_0 = F$ we will inductively build $L_{i+1} \supseteq K_i L_i$ with L_{i+1}/F Galois with solv. Gal group. This will prove the cor as $K \subseteq L_s$ and $Gal(K/F) = Gal(L_s/F)/Gal(L_s/K)$ as quotients of solvable groups are solvable.

Define L_{i+1} as the splitting field of

$$g_i(x) = \prod_{b \in \{\sigma(a) \mid \sigma \in Gal(L_i/F)\}} (x^{n_i} - b) \quad \text{over } L_i$$

This $L_{i+1} \supseteq K_{i+1} L_i$. Note that $\tau(g_i(x)) = g_i(x)$ for all $\tau \in Gal(L_i/F)$, so $g_i(x) \in F[x]$. Hence L_{i+1} is the split field of $\prod_{j=1}^{i} g_j$ over F and so Galois over F. ▨

[The other half of thm on page 1 is a story for another day... at least we showed there's no quintic formula]

Q: Does every finite group occur as $Gal(K/\mathbb{Q})$ where $K/\mathbb{Q}$ is Galois?

Any such K is the splitting field of some $f(x) \in \mathbb{Q}[x] \Rightarrow Gal(K/\mathbb{Q}) \leq S_n$ where $n = \deg$. However, every finite gp is a subgp of S_n, so this is not a real restriction.

Conj (Inverse Galois Prob). The answer is yes!

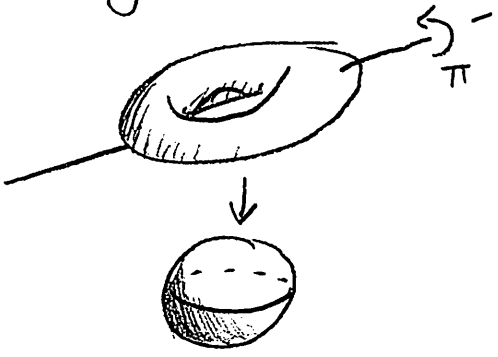
Thm: Given a finite group G, there is a finite $F/\mathbb{Q}$ and a Galois K/F with $\mathrm{Gal}(K/F) \cong G$.

Q: What about $\mathrm{Gal}(K/\mathbb{F}_p)$?

A: Always cyclic, gen by Frobenius.

Thm: Every finite group appears as $\mathrm{Gal}(K/\mathbb{C}(t))$.

Reason: Such $K/\mathbb{C}(t)$ correspond, via algebraic geometry, to geometric objects like



(branched covers of Riemann surfaces)

Now add in topology / analysis...