Lecture 29: Solvable Groups

- K/F is a root extension if

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = F$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for $a_i \in K_i$.

- An α which is alg. over F is expressible by radicals if it lies in some root ext K of F.

- $f(x) \in F[x]$ is solvable by radicals if every root is expressible by radicals.

Thm: Let K be the splitting field of $f(x) \in F[x]$. If $Gal(K/F) = S_n$ for $n \geq 5$, then f is not solvable by radicals.

Ex: $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ has $Gal = S_5$.

[More generally, theres a condition on $Gal(K/F)$ called solvability...]

Def: A finite group G is solvable if

$$\{1\} = G_s \lhd G_{s-1} \cdots G_2 \lhd G_1 \lhd G_0 = G$$

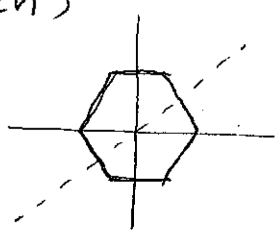
where G_i/G_{i+1} is cyclic.

Ex: • $\mathbb{Z}_n$, Any abelian gp, e.g. with $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$ could take

$$\begin{array}{ccccccc} G_3 & & G_2 & & G_1 & & G_0 \\ \{1\} & \lhd & \mathbb{Z}_2 \times \{0\} \times \{0\} & \lhd & \mathbb{Z}_2 \times \mathbb{Z}_4 \times \{0\} & \lhd & G \end{array}$$

since $G_0/G_1 = \mathbb{Z}_8$, $G_1/G_2 = \mathbb{Z}_4$, $G_2/G_3 = \mathbb{Z}_2$.

• D_{2n}, since have



quot. is $\mathbb{Z}_2$.

$$1 \lhd \mathbb{Z}_n \lhd D_{2n}$$

subgp of rotations

• $B = \left\{ \begin{pmatrix} x & z \\ 0 & y \end{pmatrix} \middle| \; x, y \in \mathbb{F}_p^\times, \; z \in \mathbb{F}_p \right\}$ [on HW!]

• Any gp with $|G| = p^n$ (DF, Ch 6.1)

• S_4

Non Ex:

G is <u>simple</u> if the only normal subgps are 1 and G.

If G is simple and <u>not</u> cyclic, then G is not solvable; e.g. $G = A_n$ for $n \geq 5$

$G = PSL_2 \mathbb{F}_p$ for $|p| \geq 4$

Other examples: S_n for $n \geq 5$.

[Query: How many have seen one of these?]

Basic facts:

① If $H \leq G$ and G is solvable, so is H.

② If $H \triangleleft G$ with H and G/H solvable, then is is G.

Note: So A_n not solv $\Rightarrow$ S_n not solv.

Pf of ①: Take $H_i = G_i \cap H$. Then $H_{i+1} \lhd H_i$ and $H_i/_{H_{i+1}} \cong$ a subgp of $G_i/_{G_{i+1}}$, and hence is cyclic.

Pf of ②: Let H_i be the subgps for H, and Q_i the subgps for $Q = G/_H$.

If $\pi: G \to Q$ is the quotient map, then

$$1 = H_s \lhd H_{s-1} \lhd \cdots \lhd \underset{\substack{\uparrow \\ = H_0 = \pi^{-1}(\{1\}) = \pi^{-1}(Q_r)}}{H} \lhd \pi^{-1}(Q_{r-1}) \lhd \cdots \lhd \pi^{-1}(Q_1) \lhd \overset{\substack{\pi^{-1}(Q_0) \\ \parallel}}{G}$$

shows that G is solvable. ▨

Thm: $f(x) \in F[x]$ is solvable by radicals iff $Gal(K/F)$ is solvable

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

[Proved by Abel in 1821 at the age of 19. Abel died at 26. Galois, was killed in a dual at 21 in 1832...]

What examples have we seen where $Gal(K/F)$ is solvable? ⓪ $F(\sqrt{D})$

① Cyclotomic fields: $K = \mathbb{Q}(\zeta_n)$

$$Gal(K/\mathbb{Q}) = \mathbb{Z}_d \quad \text{where} \quad d = [K:\mathbb{Q}] = \varphi(n)$$

Pf: K is the splitting field of $x^n - 1$, hence Galois.

Consider

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow Gal(K/\mathbb{Q})$$

$$a \longmapsto \sigma_a \quad \text{where } \sigma_a(\zeta_n) = \zeta_n^a$$

This is a homomorphism, since

$$\sigma_{ab}(\zeta_n) = (\zeta_n^b)^a = \sigma_a(\sigma_b(\zeta_n))$$

Clearly injective, and is surjective since the groups have the same order. ▨