Lecture 28: Solving equations by radicals

- \( x^2 + bx + c \) has solutions \( b \pm \sqrt{D} \)
- \( x^3 + px + q \)
  \[ A = \sqrt[3]{-\frac{27}{2}q^2 + \frac{3}{2}\sqrt{-3D}}, \quad B = \sqrt[3]{0 - C} \]
  where \( AB = -3p \). [Note \( D = -4p^3 - 27q^2 \) and
  \( (AB)^3 = -(3p)^3 \).] Then the roots are
  \[ \alpha = \frac{A + B}{3}, \quad \beta = \frac{\sqrt[3]{A} + \sqrt[3]{B}}{3}, \quad \gamma = \frac{\sqrt[3]{A} + \sqrt[3]{B}}{3} \]
- For quartics, there is an even worse formula.

**Thm:** There is no such formula for poly of degree \( \geq 5 \), i.e. expressions of the roots in terms of only the
  operations: +, \( \times \), \( \div \), \( - \), \( \sqrt{\cdot} \).

**Def:** \( f(x) \in F(x) \) is solvable by radicals if there
  are fields
  \[ F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = K = \text{Splitting field of } f(x) \]
  where \( K_{i+1} = K_i(\alpha_i) \) with \( \alpha_i \) a root of \( x^{n_i} - a_i \).
Every quadratic, cubic, or quartic poly is solv. by radicals.

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

[Q: How many know what a solvable group is?]

Ex: $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is irreducible. Set $G = \text{Gal}(K/F)$ where $K$ is the splitting field.

Claim $G = S_5$

As $f$ is irreducible, $5 \mid 161 = [K: \mathbb{Q}]$. By Sylow, $G$ has an elt of order 5, and so $G$ contains a 5 cycle. Now $f$ has 3 real roots $\alpha_1, \alpha_2, \alpha_3$ and 2 roots $\alpha_4, \alpha_5$ in $\mathbb{C} \setminus \mathbb{R}$ (N.B. that $f'(x) = 5x^4 - 6$ has only two real roots, $\alpha_4, \alpha_5$).

Thus $T = \frac{\text{restriction of } \mathbb{Z} \to \mathbb{Z}}{\mathbb{Z}}$ in $G$ corresponds to the permutation $(45)$. As $G$ contains a 5-cycle and a transposition, it must be $S_5$. 

\[ f(x) \]
**Def:** A finite group is **solvable** if

\[ \{1\} = G_5 \triangleleft G_4 \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G \]

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

**Ex:**
- Cyclic groups \( C_n \):
  - Abelian groups. E.g. \( G = C_2 \times C_4 \times C_8 \) where we can take

\[ \{1\} \triangleleft C_2 \times \{1\} \times \{1\} \triangleleft C_2 \times C_4 \times \{1\} \triangleleft G \]

\( G_3 \quad G_2 \quad G_1 \quad G_0 \)

since \( G_0 / G_1 \cong C_8 \), \( G_1 / G_2 \cong C_4 \), \( G_2 / G_3 \cong C_2 \).

- \( D_{2n} \) since have

\[ 1 \triangleleft C_n \triangleleft D_{2n} \]

subgrp of rotations

- \( B = \{(x,z) \mid x, y \in \mathbb{F}_p^x, z \in \mathbb{F}_p\} \) [on HW!]

- Any gp with \( |G| = p^n \) (DF chap 6.1)

- \( S_4 \).
Non-Ex: \( S_n \) for \( n \geq 5 \).

- Any \( G \) which is simple but not cyclic.
  
  \[ \text{E.g. } G = A_n \text{ for } n \geq 5 \]
  
  \[ G = \text{PSL}_2 \mathbb{F}_p \text{ for } |p| \geq 4. \]

Thm: \( f(x) \in F[x] \) is solvable by radicals \( \iff \text{Gal}(K/F) \) is solvable.

Cor: \( \text{Gal}(K/F) = S_n \Rightarrow \) not solvable by radicals.

Basic Facts:

1. If \( H \leq G \) and \( G \) is solvable, then so is \( H \).
2. If \( H \triangleleft G \) with \( H \) and \( G/H \) solvable, then so is \( G \).

[Cor of 2: \( A_n \) not solvable \( \Rightarrow \) \( S_n \) not solvable.]

Pf for 1: Take \( H_i = H \cap G_i \). Then \( H_{i+1} \triangleleft H_i \), and \( H_{i+1}/H_i \) is isom. to a subgp of \( G_{i+1}/G_i \) and hence is cyclic.
Proof: Let $H_i$ be the subgroups for $H$, and $Q_i$ the subgroups for $Q = G/E$. If $\pi: G \to Q$ is the quotient map, then

$$1 = H_S \triangleleft H_{S-1} \triangleleft \cdots \triangleleft H_0 \triangleleft \pi^{-1}(Q_r) \triangleleft \cdots \triangleleft \pi^{-1}(Q_1) \triangleleft G$$

$$H = \pi^{-1}(Q) = \pi^{-1}(Q_r)$$

shows that $G$ is solvable. \qed

Examples where $\text{Gal}(K/F)$ is solvable:

1. $F(\sqrt[n]{D})$

   Degree is $\varphi(n)$.

2. Cyclotomic Fields: $K = \mathbb{Q}(\zeta_n)$.

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

Consider

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^x \longrightarrow \text{Gal}(K/F)$$

$$a \longmapsto (\sigma_a : S_n \to S_n)$$

This is a homomorphism as $\sigma_{ab}(S_n) = S_n^{ab}$

$$(S_n^b)^a = \sigma_a(S_n^b(S_n)) = S_n^{ab}.$$
This is clearly injective, and is hence surjective as \( |\text{Gal}(K/\mathbb{Q})| = [K: \mathbb{Q}] = \varphi(n) \)
and so the groups have the same numbers of elts.

*Note: While \( \text{Gal}(\mathbb{Q}^{5n}/\mathbb{Q}) \) is abelian, it may not be cyclic, e.g. \( (\mathbb{Z}/8\mathbb{Z})^* \cong \text{Klein 4-gp}. \)