Lecture 28: Solving equations by radicals

- x^2+bx+c has solutions $\dfrac{-b\pm\sqrt{D}}{2}$
- x^3+px+q

  Set $A = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}$, $B = \sqrt[3]{\bigcirc - \bigcirc}$

where $AB=-3p$. [Note $D=-4p^3-27q^2$ and so $(AB)^3 = -(3p)^3$.] Then the roots are

$$\alpha = \frac{A+B}{3} \qquad \beta = \frac{\zeta_3^2 A + \zeta_3 B}{3} \qquad \gamma = \frac{\zeta_3 A + \zeta_3^2 B}{3}$$

- For quartics, there is an even worse formula.

Thm: There is no such formula for polys of degree ≥ 5, i.e. expressions of the roots in terms of only the opperations: $+, \times, \div, -, \sqrt[k]{\ }$.

Def: $f(x) \in F(x)$ is solvable by radicals if there are fields

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K = \text{splitting field of } f(x)$$

where $K_{i+1} = K_i(\alpha_i)$ with α_i a root of $x^{n_i} - a_i$.

[Every quadratic, cubic, or quartic poly is solv. by radicals.]

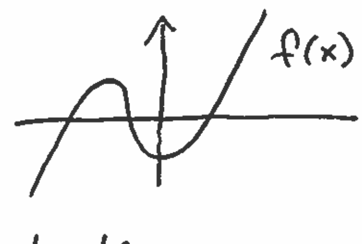
<u>Thm</u>: K the splitting field for $f(x) \in F[x]$ for $n \geq 5$. If $\mathrm{Gal}(K/F) = S_n$, then $f(x)$ is <u>not</u> solvable by radicals.

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

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

<u>Claim</u> $G = S_5$

As f is irreducible, $5 \mid |G| = [K : \mathbb{Q}]$. 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 α_4, α_5 in $\mathbb{C} \setminus \mathbb{R}$ (N.B. that $f'(x) = 5x^4 - 6$ has only two real roots, so:



)

Thus $\tau = \begin{array}{l}\text{restriction} \\ \text{of } z \mapsto \bar{z} \\ \text{to } K\end{array}$ in G cooresponds to the premutation (45). As G contains a 5-cycle and a transposition, it must be S_5.

Def: A finite group is solvable if

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

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

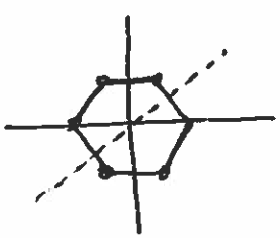
Ex: • Cyclic groups C_n.

• Abelian groups. E.g. $G = C_2 \times C_4 \times C_8$ where we can take

$$\underset{G_3}{\{1\}} \lhd \underbrace{C_2 \times \{1\} \times \{1\}}_{G_2} \lhd \underbrace{C_2 \times C_4 \times \{1\}}_{G_1} \lhd \underset{G_0}{G}$$

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



quotient is C_2.

$$1 \lhd C_n \lhd D_{2n}$$

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 chap 6.1)

• S_4.

<u>Non-Ex:</u> • S_n for $n \geq 5$.

• Any G which is <u>simple</u> but not cyclic.
← only normal subgroups are $\{1\}$ and G

E.g. $G = A_n$ for $n \geq 5$

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

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

<u>Cor</u>: $Gal(K/F) = S_n \Rightarrow$ not solvable by radicals.

<u>Basic Facts</u>:

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.]

<u>Pf of ①</u>: 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.

Pf of ②: Let H_i be the subgroups for H, and Q_i the subgroups for $Q = G/H$. If $\pi : G \to Q$ is the quotient map, then

$$1 = H_s \triangleleft H_{s-1} \triangleleft \cdots \triangleleft H_0 \triangleleft \pi^{-1}(Q_{r-1}) \triangleleft \cdots \triangleleft \pi^{-1}(Q_1) \triangleleft G$$

$$H_0 = H = \pi^{-1}(\{1\}) = \pi^{-1}(Q_r)$$

shows that G is solvable. $\square$

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

① $F(\sqrt{D})$

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

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

Consider

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

$$a \longmapsto \left(\sigma_a : \zeta_n \mapsto \zeta_n^a\right)$$

This is a homomorphism as $\sigma_{ab}(\zeta_n) = \zeta_n^{ab} = (\zeta_n^b)^a = \sigma_a(\sigma_b(\zeta_n))$.

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

<u>Note</u>: While $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian it may not be cyclic, e.g. $(\mathbb{Z}/8\mathbb{Z})^\times \cong$ Klien 4-gp.