

Lecture 28:

75

$K =$ splitting field of an irred poly $f(x) \in F[x]$
with roots $\alpha_1, \alpha_2, \dots, \alpha_n$.

$$D = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in F$$

$$= \prod_{i < j} (\alpha_i - \alpha_j)$$



$G = \text{Gal}(K/F)$ a subgroup of S_n .

Prop: $\sqrt{D} \in F \iff G \leq A_n$

Pf: Any transp. sends $\sqrt{D} \rightarrow -\sqrt{D}$.

So $\sigma \in G$ fixes \sqrt{D} iff σ is even.

Hence $\sqrt{D} \in F \iff \sigma(\sqrt{D}) = \sqrt{D} \forall \sigma \in G \iff G \leq A_n. \quad \square$

We were looking at

Thm: Suppose $n=4$. If $\sqrt{D} \notin F$, then

$$G = S_4, \underbrace{Z_4 \text{ or } D_8}$$

Erra: Omitted last time, but are
mess. by the Prop.

To distinguish these cases need to introduce the resolvent cubic, whose roots are

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \quad \theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$

$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

$$L = F(\theta_1, \theta_2, \theta_3)$$

Galois →



cf $f(x) = x^4 + px^2 + qx + r$, then the θ_i

are the roots of $h(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$

Thm: cf $\sqrt{D} \notin F$ and $\text{Gal}(L/F) = S_3$, then

$$\text{Gal}(K/F) = S_4.$$

Pf: cf $\text{Gal}(L/F) = S_3$, then $6 \mid \text{Gal}(K/F)$, ▣

Solving Equations via radicals:

① $x^2 + bx + c$ has solns $\frac{-b \pm \sqrt{D}}{2}$

② $x^3 + px + q$

Set $A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$, $B = \sqrt[3]{0 - 0}$

where $AB = -3p$. Then, the roots are

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

③ For quartics there's an even worse formula.

And that's it! There's no such formula for quintics, i.e. expressions for the roots using only the ops: +, x, -, ÷, $\sqrt[n]{}$

Def: $f(x) \in F[x]$ is solvable by radicals if the splitting field K can be written

$$F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = K$$

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

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

More generally, if $\text{Gal}(K/F)$ is not solvable, then $f(x)$ is not solv. by radicals. [Q: How many know what a solvable group is.]

Ex: $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$, which is irred.

Let $G = \text{Gal}(K/\mathbb{Q})$ for K the splitting field.

Claim: $G = S_5$.

As f is irred, $5 \mid |G| \xrightarrow{\text{Sylow}} G$ has an elt of order 5 $\Rightarrow G$ contains a 5-cycle.

Plotting shows that $f(x)$ has exactly 3 real roots. (N.B. $f'(x) = 5x^4 - 6$ has only 2 real roots.) Let $\alpha_1, \alpha_2, \alpha_3$ be these real roots. Let α_4 and $\alpha_5 = \bar{\alpha}_4$ be the roots in $\mathbb{C} \setminus \mathbb{R}$. Let $\tau = \text{rest. of complex conj to } K$.

Then $\tau = (45)$. So $G \leq S_5$ has a

five cycle and a transposition $\Rightarrow G = S_5$.