Lecture 27: Galois groups of polynomials.

$K =$ splitting field of an irreducible separable $f(x) \in F[x]$, with roots $\alpha_1, \ldots, \alpha_n$.

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

$$\sqrt{D} = \prod_{i<j} (\alpha_i - \alpha_j) \in K$$

$$\begin{array}{c} K \\ | \\ F(\sqrt{D}) \\ | \\ F \end{array}$$

$$\boxed{\mathrm{Char}\, F \neq 2}$$

<u>Goal</u>: Find $G = \mathrm{Gal}(K/F)$ as a subgroup of S_n.

<u>Prop</u>: When $\deg f = n$ is two, then $K = F(\sqrt{D})$ and $G = S_2$.

<u>Prop</u>: When $n = 3$ then

(a) If D is a square in F, i.e. $\sqrt{D} \in F$, then $G = \langle (1\,2\,3) \rangle$

(b) If D is not a square, then $G = S_3$.

<u>Ex</u>: $F = \mathbb{Q}$

$x^3 - 3x - 1$ has $D = 81 = 3^4 \Rightarrow G = C_3$

$x^3 - 3x + 1$ has $D = -135 = -3^3 \cdot 5 \Rightarrow G = S_3$

Both irreducible as no roots in $\mathbb{F}_2$.

Any $\sigma \in S_n$ is a product of transpositions (ij), we call σ even or odd depending on how many you need.

<u>Note</u>: A cycle of odd length is even. $(123) = (13)(12)$

— — even — odd: $(12), (1234)$

Gives a homomorphism $S_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$; the kernel is the subgp A_n of even permutations.

$\uparrow$ Alternating group.

<u>Thm</u>: $\sqrt{D} \in F \iff G \leq A_n$.

<u>Proof</u>: A transposition $(k\ell)$ sends $\sqrt{D}$ to $-\sqrt{D}$ since

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

and the terms that switch sign are (if $k < \ell$)

$$\left.\begin{array}{ll} (\alpha_k - \alpha_j) & \text{with } k < j < \ell \\ (\alpha_i - \alpha_\ell) & \text{with } k < i < \ell \end{array}\right\} \text{same number!}$$

and $(\alpha_k - \alpha_\ell)$

As char $\neq 2$, get $\sigma \in S_n$ fixes $\sqrt{D}$ iff σ is even. Hence $\sqrt{D} \in F \iff \sigma(\sqrt{D}) = \sqrt{D}$ for all $\sigma \in G \iff G \leq A_n$. $\square$

<u>Note</u>: $D = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^n \prod_{i \neq j} (\alpha_i - \alpha_j)$ is independent of how we number the roots of f, but $\prod_{i<j} (\alpha_i - \alpha_j)$ does depend on this choice.

<u>Def</u>: A subgroup $H \leq S_n$ is <u>transitive</u> if $\forall$ pair i,j $\exists \sigma \in H$ with $\sigma(i) = j$. <u>Ex</u>: $\langle (1234) \rangle$ in S_4 but not $\langle (12)(34) \rangle$

<u>Lemma</u>: As f is irreducible, $G \leq S_n$ is transitive.

<u>Thm</u>: When $\deg f = 4$, then $\sqrt{D} \notin F \Rightarrow G = S_4, D_8, C_4$.

<u>Pf</u>: The transitive subgroups of S_4 are (up to conjugation)

$$S_4,\ A_4,\ C_4 = \langle (1234) \rangle,\ K = \langle (12)(34), (13)(24) \rangle$$

$$D_8 = \langle (1234), (12)(34) \rangle$$

Of these, A_4 and K are subgps of K and hence are excluded by the prev. thm. $\square$

To distinguish S_4, D_8, C_4 consider the <u>resultant cubic</u> whose roots are

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

$$\begin{tikzcd} K \arrow[d, dash] \\ L = F(\theta_1,\theta_2,\theta_2) \arrow[d, dash, "\text{Galois}"'] \\ F \end{tikzcd}$$

If $f(x) = x^4 + px^2 + qx + r$, then the θ_i are roots of $h(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$

<u>Note</u>: Can reduce to f of this form by a substitution $f(x - \frac{a}{4})$ where $f(x) = x^4 + ax^3 + \cdots$.

Check form of h by grinding it out.

<u>Thm</u>: If $\sqrt{D} \notin F$ and $Gal(L/F) = S_3$, then $Gal(K/F) = S_4$

<u>Pf</u>: If $Gal(L/F) = S_3$, then 6 divides $[K:F] = |Gal(K/F)|$. This excludes C_4 and D_8. $\square$