Lecture 39: Galois Groups of Polynomials

§14.6 of [DF]

F.T.G.T. K/F Galois, $G = Gal(K/F)$.

$$\left\{\begin{matrix}\text{subfields}\\ F \subseteq E \subseteq K\end{matrix}\right\} \xleftrightarrow{\text{bijection}} \left\{\begin{matrix}\text{subgroups}\\ H \leq G\end{matrix}\right\}$$

$$E \longmapsto G_E := Gal(K/E)$$

$$K_H \longleftarrow H$$

Suppose K is the splitting field of a separable $f(x) \in F[x]$. If $\alpha_1, \dots, \alpha_n \in K$ where $n = \deg(f)$ are the roots of f, then $K = F(\alpha_1, \dots, \alpha_n)$ and $Gal(K/F) \leq S_n$ by its action on the α_i.

Goal: Extract $Gal(K/F)$ from f.

Start with the generic example where $G = S_n$.

Fix a field F. Consider $K = F(x_1, \dots, x_n)$ = rat'l fns in the x_i $= Frac(F[x_1, \dots, x_n])$. Note $Aut(K) \geq S_n$ where S_n acts on K by permuting the x_i according to their subsripts.

Ex: $F = \mathbb{F}_2$, $n = 4$

$$(123) \circ \frac{x_1^2 + x_2 x_3}{x_1 + x_4} = \frac{x_2^2 + x_3 x_2}{x_2 + x_4}$$

Set $L = K_{S_n}$ so that $\mathrm{Gal}(K/L) = S_n$

field of symmetric functions

Example elts:

- F
- $s_1 = x_1 + x_2 + \cdots + x_n$
- $s_n = x_1 x_2 \cdots x_n$
- $s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$

elementary symmetric functions

$$\begin{array}{c} K \\ \Big| \; n! \\ L \\ \Big| \\ L' \end{array}$$

Thm: $L = F(s_1, \ldots, s_n)$.

Pf: Set $L' = F(s_1, \ldots, s_n)$. Have $L' \subseteq L$ and $[K : L] = |S_n| = n!$ So it suffices to show $[K : L'] \leq n!$, which follows as K is the splitting field of this deg n poly in $L'[t]$:

$$\prod_{i=1}^{n} (t - x_i) = t^n - (x_1 + \cdots + x_n) t^{n-1} + \cdots + (-1)^n x_1 \cdots x_n$$

$$= t^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \quad ▨$$

Suppose $f(x) \in F[x]$ is separable and K/F a splitting field. The <u>discriminant</u> of f is

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

where the α_i are the roots of f in K.

Note $D \in F$ as any $\sigma \in Gal(K/F)$ permutes the α_i. View D as a symmetric fn of the roots, the theorem tells us that it can be written in terms of the coeffs of f.

<u>Ex</u>: $\deg f = 2$

$$D = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = (x_1+x_2)^2 - 4x_1x_2$$
$$= (s_1)^2 - 4s_2$$

So if $f(x) = x^2 + \underbrace{b}_{-s_1}x + \underbrace{c}_{s_2}$, have $D = b^2 - 4c$

where have we seen this before?

<u>Ex</u>: $f(x) = x^3 + ax^2 + bx + c$.

Turns out $D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$.

Note that D is a square in K, namely $\sqrt{D} = \prod_{i<j} (\alpha_i - \alpha_j)$

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

Suppose $G = Gal(K/F) = S_n$. Then

$\exists\, \sigma \in G$ with $\sigma(\sqrt{D}) = -\sqrt{D}$, e.g. $\sigma = (12)$.

If $\underbrace{\text{char} \neq 2}_{\text{standing assumpt.}}$, this means $\sqrt{D} \notin F$. Can be refined to

$\boxed{\text{Thm: } \sqrt{D} \in F \Leftrightarrow G \leq A_n.}$

<u>n=2</u>: $f \in F[x]$ irred of deg 2. Then $[K:F] = 2$ and $Gal(K/F) \cong S_2$. So $K = F(\sqrt{D})$.

<u>Know already</u>: Roots of $x^2 + bx + c$ are $\dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$.

<u>n=3</u>: $f(x)$ irred and sep. of deg 3. Have $G \leq S_3$

<u>Q</u>: Could $G = \langle (12) \rangle$. <u>A</u>. No, as have to be able to take any root of f to any other.

So poss are $G = \langle (123) \rangle \cong C_3 \Leftrightarrow [K:F] = 3$

$\Leftrightarrow D$ is a square in F.

and $G = S_3 \Leftrightarrow [K:F] = 6 \Leftrightarrow D$ is <u>not</u> a square in F.

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

$\underbrace{\begin{array}{l} x^3 - 3x - 1 \\ x^3 - 3x + 1 \end{array}}_{\text{both irreducible as no roots in } \mathbb{F}_2.}$ $\begin{array}{l} \text{has } D = 81 = 3^4 \Rightarrow G = C_3 \\ \text{has } D = -135 = -3^3 \cdot 5 \Rightarrow G = S_3. \end{array}$

$n=4$: $f(x)$ irred and separable of deg 4.

Know G acts transitively (= only one orbit) on $\{\alpha_1, \ldots, \alpha_n\}$ since f is irred. The transitive subgroups of S_4 are (up to conjugation):

$$S_4,\ A_4,\ C_4 = \langle (1234) \rangle,\ K = \langle (12)(34), (13)(24) \rangle$$
$$\text{and } D_8 = \langle (1234), (12)(34) \rangle$$

[Q: what are some nontransitive subgps?]

$\sqrt{D} \in F$: $G \leq A_4$ so $G = A_4$ or K.

$\sqrt{D} \notin F$: $G = S_4, C_4,$ or D_8.

Can distinguish these by looking at the resultant cubic whose roots are

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

$$\begin{array}{c} K \\ | \\ L = F(\theta_1, \theta_2, \theta_3) \\ |\ \text{Galois} \\ F \end{array}$$

See §14.6 for the formula.

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

Pf: Have $[L:F] = 6$, so 6 divides $[K:F]$, which excludes C_4 and D_8. ▨