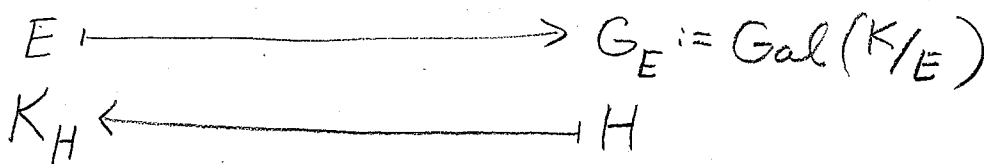
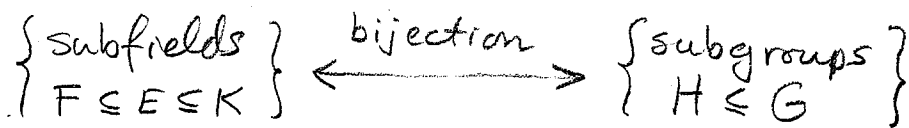


Lecture 39: Galois Groups of Polynomials

①

F.T.G.T. K/F Galois, $G = \text{Gal}(K/F)$

§14.6 of [DF]



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 $\text{Gal}(K/F) \leq S_n$ by its action on the α_i .

Goal: Extract $\text{Gal}(K/F)$ from f .

Start with the generic example where $G = S_n$

Fix a field F . Consider $K = F(x_1, \dots, x_n) = \text{rat'l fns in the } x_i$
 $= \text{Frac}(F[x_1, \dots, x_n])$. Note $\text{Aut}(K) \cong S_n$

where S_n acts on K by permuting the x_i according to their subscripts.

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

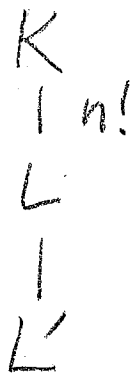
$$(123) \cdot \frac{x_1^2 + x_2 x_3}{x_1 + x_4} = \frac{x_2^2 + x_3 x_2}{x_2 + x_4}$$

Set $L = K_{S_n}$ so that $\text{Gal}(K/L) = S_n$
↖ field of symmetric functions

Example elts:

- F
- $S_1 = X_1 + X_2 + \dots + X_n$
- $S_n = X_1 X_2 \dots X_n$
- $S_k = \sum_{i_1 < i_2 < \dots < i_k} X_{i_1} X_{i_2} \dots X_{i_k}$

elementary symmetric functions.



Thm: $L = F(S_1, \dots, S_n)$.

Pf: Set $L' = F(S_1, \dots, S_n)$. 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 $L'[t]$:

$$\begin{aligned}
 \prod_{i=1}^n (t - X_i) &= t^n - (X_1 + \dots + X_n)t^{n-1} + \dots + (-1)^n X_1 \dots X_n \\
 &= t^n - S_1 X^{n-1} + S_2 X^{n-2} + \dots + (-1)^n S_n \quad \square
 \end{aligned}$$

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

$$D = \prod_{i < j} (\alpha_i - \alpha_j)^2 \quad \text{where the } \alpha_i \text{ are the roots of } f \text{ in } K.$$

Note $D \in F$ as any $\sigma \in \text{Gal}(K/F)$ 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 .

Ex: $\deg f = 2$

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

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

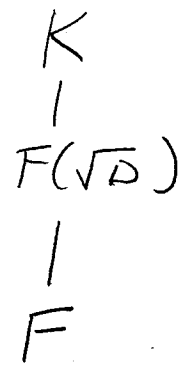
Ex: $f(x) = x^3 + ax^2 + bx + c$

where have we seen this before?

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

Note that D is a square in K ,

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



Suppose $G = \text{Gal}(K/F) = S_n$. Then

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

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

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

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

Know already: Roots of $x^2 + bx + c$ are $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$.

n=3: $f(x)$ irred_{and sep.} of deg 3. Have $G \leq S_3$

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

So poss are $G = \langle (123) \rangle \cong C_3 \iff [K:F] = 3$
 $\iff D$ is a square in F .

and $G = S_3 \iff [K:F] = 6 \iff D$ is not a square in F .

Ex: $F = \mathbb{Q}$

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

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

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

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

Know G acts transitively (= only one orbit) on $\{\alpha_1, \dots, \alpha_n\}$ 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 .

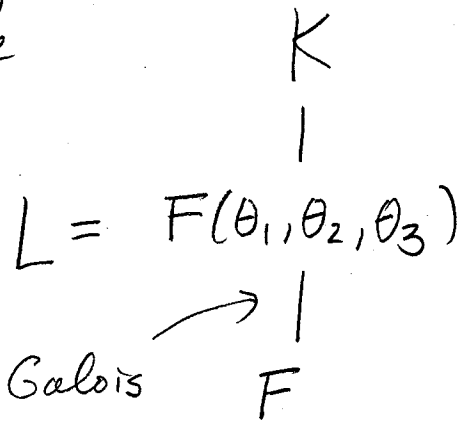
$\sqrt{D} \notin F$: $G = S_4, C_4,$ or D_8 .

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

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

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

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



See §14.6 for the formulae.

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

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