No class Monday (4/8)

Rest of HW8 posted

Recall: $K = F(x_1, \dots, x_n)$, $\underbrace{\text{Fix } S_n}_{\text{ring of sym. funs.}} = F(e_1, \dots, e_n)$

elem. sym. funs.

$$e_k(x_1, \dots, x_k) = \sum_{i_1 < \dots < i_k} x_{i_1} \cdots x_{i_k}$$

If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ has roots $\alpha_1, \dots, \alpha_n$,

$$a_k = (-1)^{n-k} e_{n-k}(\alpha_1, \dots, \alpha_n)$$

So if $K = Sp_F f = F(\alpha_1, \dots, \alpha_n)$, then $e_k(\alpha_1, \dots, \alpha_n) \in F$

Another way to view this: if $k \in K$ is fixed under any permutation of $\alpha_1, \dots, \alpha_n$, then since $Gal(K/F) \leq S_n$, $k \in \text{Fix}(Gal(K/F)) = F$.

Def: The <u>discriminant</u> of $f(x) \in F[x]$ is

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

where α_i are the roots of F in $K := Sp_F(f)$

Prop: $D = 0 \iff f$ is inseparable.

Prop: $D \in F$

E.g.:

a) $f = f_{gen}^{(2)}(x) = (x - x_1)(x - x_2)$

$$D = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2$$
$$= (x_1 + x_2)^2 - 4x_1x_2$$
$$= e_1^2 - 4e_2$$

So if

$f(x) = x^2 + \underbrace{b}_{-e_1}x + \underbrace{c}_{e_2}$, then $D = b^2 - 4c$ (!)

b) If $f(x) = x^3 + ax^2 + bx + c$,

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

Take a sqrt:

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

$$\begin{array}{c} K = F(\alpha_1, \dots, \alpha_n) \\ | \\ F(\sqrt{D}) \\ | \\ F = F(D) \end{array}$$

Assume char $F \neq 2$

If $G := \mathrm{Gal}(K/F) = S_n$

then $\exists \sigma \in D$ w/ $\sigma(\sqrt{D}) = -\sqrt{D}$. Thus, $\sqrt{D} \notin F$

e.g. $\sigma = (12)$

Recall: $A_n = \left\{ \begin{array}{c} \text{even perms.} \\ \text{of } 1, \dots, n \end{array} \right\} \underset{\text{index } 2}{\leq} S_n$

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

Pf: $\sigma(\sqrt{D}) = \sqrt{D} \iff \sigma$ is even, so

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

$$\iff \sqrt{D} \in \mathrm{Fix}\, G = F \qquad \square$$

Now let's find some Galois gps.

$f(x) \in F[x]$ $\quad K := Sp_F f \quad G := Gal(K/F)$

$n=2$: $f(x) = x^2 + bx + c$

If f red., $K = F$, $G = id = A_2$

If f irred., then $[K:F] = 2$, $G = \mathbb{Z}/2\mathbb{Z} \cong S_2$

$K = F(\sqrt{D}) = F(\alpha_1 - \alpha_2) = F(\sqrt{b^2-4c})$

$\left(\text{Roots are } \dfrac{-b \pm \sqrt{b^2-4c}}{2} \right)$

$n=3$: $f(x) = x^3 + ax^2 + bx + c \qquad G \leq S_3$

If f red., see case above

Assume f irred. S_3 has lots of subgps. What could G be?

Def: A group G acts transitively on a set A if $Ga = A$ for any/all $a \in A$.

Prop: If $f \in F[x]$ irred., $K = Sp_F f$, $Gal(K/F)$ acts transitively on the set of roots of f.

Pf: Let $G\alpha = \{\alpha_1, .., \alpha_k\}$. If $\sigma \in G$, σ permutes $G\alpha$, so $\sigma(e_i(\alpha_1, \dots, \alpha_k)) = e_i(\sigma(\alpha_1), .., \sigma(\alpha_k))$

$$= e_i(\alpha_1, \dots, \alpha_k)$$

This means that $e_i(\alpha_1, .., \alpha_k) \in \text{Fix } G = F$, so

$$\prod_{i=1}^{k} (x - \alpha_i) = x^k - e_1(\alpha_1, .., \alpha_k) + \dots + (-1)^k e_k(\alpha_1, .., \alpha_k) \in F[x].$$

Since this divides f, it must equal f, so G acts transitively $\square$

Trans. subgps. of S_3: S_3 and $A_3 = \mathbb{Z}/3\mathbb{Z} = C_3$

$G = A_3 \iff [K:F] = 3$

$\iff \sqrt{D} = \sqrt{a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc} \in F$

$G = S_3 \iff [K:F] = 6 \iff \sqrt{D} \notin F$

E.g: $F = \mathbb{Q}$

$x^3 - 3x - 1 \quad D = 81 \quad \sqrt{D} = 9 \in \mathbb{Q} \Rightarrow G = C_3$

$x^3 - 3x + 1 \quad D = -135 \quad \sqrt{D} \notin \mathbb{Q} \Rightarrow G = S_3$

both irred. since no roots in $\mathbb{F}_2$

See D&F p.627-9 for Galois gp. of a quartic