Announcements

HW9 posted (due Fri. 4/18 @ 9am)

Late drop deadline is this Friday

Still figuring out the homework grading; thanks for your patience

Midterm 3: Wed 4/23, 7:00-8:30pm, Sidney Lu 1043

Galois groups of polynomials

Recall: The discriminant 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: $D \in F$

(in fact, D can be written in terms of the coefficients of f)

Fix 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 $F \neq 2$ from now on

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: $A_n = \left\{ \begin{matrix} \text{even perms.} \\ \text{of } 1, \dots, n \end{matrix} \right\} \leq S_n$

index 2

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

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

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

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

$\square$

Now let's find some Galois gps.

$f(x) \in F[x]$ sep. of deg. n, $K := Sp_F f$, $G := Gal(K/F)$

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

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

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

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

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

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

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

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

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

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

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

Transitive subgps. of S_3:

S_3 and $A_3 = \mathbb{Z}/3\mathbb{Z} =: C_3$

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

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

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

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

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

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

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

$n=4$ (See D&F p. 627–9 for details)

$f(x)=x^4+ax^3+bx^2+cx+d$

Substitute $y=x+a/4$ to get

$g(y)=y^4+py^2+qy+r$ (where p,q,r are functions of a,b,c,d)

(Same splitting field, same discriminant, same Galois gp.)

If g has a linear factor, see above cases

If g is the product of two irred. quadratic factors w/ disc. D_1 & D_2, then $K=F(\sqrt{D_1},\sqrt{D_2})$ and

- If $\sqrt{D_1}/\sqrt{D_2}\in F$, $K=F(\sqrt{D_1})$, $G\cong C_2$
- Otherwise, $G\cong C_2\times C_2$ (Klein 4-gp.)

If g is irred., then G is a transitive subgp. of S_4

Let g have roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$

Then G must be one of

S_4, A_4

$D_8 = \{1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12)(34)\}$ and conjugates

$V = \{1, (12)(34), (13)(24), (14)(23)\}$

$C = \{1, (1234), (13)(24), (1432)\}$ and conjugates

Let $\left.\begin{aligned} \theta_1 &= (\alpha_1+\alpha_2)(\alpha_3+\alpha_4) \\ \theta_2 &= (\alpha_1+\alpha_3)(\alpha_2+\alpha_4) \\ \theta_3 &= (\alpha_1+\alpha_4)(\alpha_2+\alpha_3) \end{aligned}\right\}$ G permates these

These are the roots of the <u>resolvent cubic</u>

$h(x) := x^3 - 2px^2 + (p^2-4r)x + q^2$

for g.

h has the same discriminant D as g (and f).

and $\mathrm{Gal}(h) \leq \mathrm{Gal}(g) = g$

- If h is irred and $\sqrt{D} \notin F$, then $\mathrm{Gal}(h) = S_3$, and $G \not\subseteq A_4$, so $G = S_4$.
- If h is irred and $\sqrt{D} \in F$, then $\mathrm{Gal}(h) = A_3$, and $G \subseteq A_4$, so $G = S_4$.
- If h splits into linear factors, then $\theta_1, \theta_2, \theta_3 \in F = \mathrm{Fix}\, G$, so $G = V$
- If h has an irred. quadratic factor, then precisely one of $\theta_1, \theta_2, \theta_3$ is in F. Depending on which one, and whether g is irred. over $F(\sqrt{D})$, we have $G = D_8$ or C or a conjugate of one of them.