Announcements

No class of office hours Monday

Exam 3: Thurs. 4/18 7:00-8:30pm

Loomis Lab. 144

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

□

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

If f red., see case above

Assume f irred.

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

Thm (Cardono, 1545): The cubic eqn. is solvable by radicals.

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

$$g(y) = f\left(x + \frac{a}{3}\right) = y^3 + py + q \qquad \text{"depressed cubic"}$$

$$p = \frac{1}{3}(3b - a^2) \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c)$$

Let $\zeta = \zeta_3$ $\qquad \zeta^2 + \zeta + 1 = 0$

Let $g(y)$ have roots α, β, γ

Have $e_1 = \alpha + \beta + \gamma = -y^2\text{-coeff} = 0$

$$e_2 = p \qquad e_3 = -q$$

$$0 = \alpha + \beta + \gamma$$

$$\left.\begin{aligned} \theta_1 &:= \alpha + \zeta\beta + \zeta^2\gamma \\ \theta_2 &:= \alpha + \zeta^2\beta + \zeta\gamma \end{aligned}\right\} \text{"Lagrange resolvents"}$$

$$\theta_1 + \theta_2 = 3\alpha$$

$$\zeta^2\theta_1 + \zeta\theta_2 = 3\beta$$

$$\zeta\theta_1 + \zeta^2\theta_2 = 3\gamma$$

$$\sqrt{D} = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma) = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha - \alpha\beta^2 - \beta\gamma^2 - \gamma\alpha^2$$

So if $S = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha + \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$, then

$$\theta_1^3 = \alpha^3 + \beta^3 + \gamma^3 + 3\zeta(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\zeta^2(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 6\alpha\beta\gamma$$

$$= \alpha^3 + \beta^3 + \gamma^3 + \frac{3}{2}S(S+\sqrt{D}) + \frac{3}{2}\zeta^2(S-\sqrt{D}) + 6\alpha\beta\gamma$$

Can show (given that $\alpha+\beta+\gamma=0$)

$$\alpha^3 + \beta^3 + \gamma^3 = -3q, \quad S = 3q$$

So

$$\theta_1^3 = -3q + \frac{3}{2}\zeta(3q+\sqrt{D}) + \frac{3}{2}\zeta^2(3q-\sqrt{D}) - 6q$$

$$= -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D} \qquad \left(\text{since } \begin{array}{l}\zeta+\zeta^2 = -1 \\ \zeta-\zeta^2 = \sqrt{-3}\end{array}\right)$$

Similarly,

$$\theta_2^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}$$

(need $\theta_1\theta_2 = -3p$)

Choose

$$A = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} \qquad B = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}$$

s.t. $AB = -3p$. Then,

$$\alpha = \frac{A+B}{3} \qquad \beta = \frac{\zeta^2 A + \zeta B}{3} \qquad \gamma = \frac{\zeta A + \zeta^2 B}{3}$$

(Quartic formula follows from this and the "resolvent cubic")

Def: $f(x) \in F[x]$ is <u>solvable by radicals</u> if $\exists$

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = Sp_F f$$

where $K_{i+1} = K_i(\alpha_i)$ w/ α_i a root of $x^{n_i} - a_i$

Assume char $F = 0$ (or just let it not divide anything we don't want it to)

Thm (ancients, Cardano, Ferrari): All deg ≤ 4 polys are solvable

Thm (Abel-Ruffini): There is no general formula by radicals for $f_{gen}^{(n)}$, $n \geq 5$.

Thm (Galois):

a) $f(x)$ is solvable by radicals $\iff$ Gal f is a "solvable gp"

b) $\exists$ a degree 5 poly. which is not solvable by radicals.

Def: A finite gp. G is <u>solvable</u> (UK: "soluable") if

$$\{1\} = G_s \triangleleft G_{s-1} \triangleleft \cdots \triangleleft G_0 = G$$

where G_i / G_{i+1} is cyclic.

Examples:

- abelian gps.
- dihedral gps.

$$1 \triangleleft C_n \triangleleft D_{2n}, \quad D_{2n} \leftarrow C_2$$

- p-gps. ($|G| = p^k$)
- S_4: $1 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$, with $S_4 \leftarrow V_4$, $A_4 \leftarrow C_2$, $S_4 \leftarrow C_2$

Non-examples:

- S_n or $\underbrace{A_n \text{ for } n \geq 5}_{\text{no normal subgps: ie. "simple"}}$ (D&F Thm 4.24)
- Other finite simple gps. (e.g. the monster)

Cor: If $n=5$, $K = S_{p_F} f$,

$\mathrm{Gal}(K/f) = S_n$ or $A_n \Rightarrow f$ is not solvable by radicals