Project due today 2pm
Office hour today 11:30 - 12:30

Thm 32: Let $s_1, \ldots, s_n$ be indeterminates.
Then, $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in F(s_1, \ldots, s_n)[x]$
is sep. w/ Galois gp. S_n.

Last time: proved this w/ the root as the indets.

Pf: Let $x_1, \ldots, x_n$ be the roots of f. Then $s_1, \ldots, s_n$ are the elementary symm. polys in $x_1, \ldots, x_n$.

Claim: no poly. relations over F btwn. $x_1, \ldots, x_n$.

Pf: If so, let $p(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ s.t. $p(x_1, \ldots, x_n) = 0$.

Let $\tilde{p}(t_1, \ldots, t_n) = \prod_{\sigma \in S_n} p(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$.

Since $p \mid \tilde{p}$, $\tilde{p}(x_1, \ldots, x_n) = 0$, but $\tilde{p}$ is sym. in the x's, and so gives a poly. rel'n btwn. $s_1, \ldots, s_n$ by Fun. Thm. of Sym. Funs.

But by assumption, $s_1, \ldots, s_n$ are indeterminates.

Thus, same setting as Prop 30 $\Rightarrow$ done. $\square$

Conclusion: if no alg. rel'ns btwn coeffs., Gal. gp. in S_n.

Over $\mathbb{Q}$, happens most of the time. Over $\mathbb{F}_p$, can't happen.

Def: Let $f(x) \in F[x]$ be monic w/ roots $\alpha_1, \ldots, \alpha_n$. The <u>discriminant</u> of f is

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

Prop: f is separable $\Leftrightarrow D \neq 0$

Pf: f insep $\Leftrightarrow \exists\, i,j$ s.t. $\alpha_i = \alpha_j \Leftrightarrow D = \prod_{i<j} (\alpha_i - \alpha_j)^2 = 0$ $\square$

$s_i(\alpha_1, \ldots, \alpha_n)$ not nec. alg. indep.

Note that $D \in F(s_1, \ldots, s_n) = \mathrm{Fix}\, S_n$

Prop 33: Suppose char $F \neq 2$, and let $\sigma \in S_n$.

Then $\sigma \in A_n$ (alternating gp.) if and only if σ fixes

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

Pf: If $\sigma = (ab)$, $a < b$, then

$$\sigma(\sqrt{D}) = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = (\alpha_b - \alpha_a) \prod_{\substack{i<j \\ (i,j)\neq(a,b)}} (\alpha_i - \alpha_j) = -\sqrt{D}$$

The result follows since $\sigma \in A_n \Leftrightarrow \sigma$ can be written as a prod of an even num. of 2-cycles. $\square$

Cor: $Gal(f) \leq A_n \Leftrightarrow \sqrt{D} \in F$.

Assume char $F \neq 2$ or 3

<u>Degree 2</u>:

$$f(x) = x^2 + bx + c = (x-\alpha)(x-\beta)$$

$$D = (\alpha - \beta)^2 = s_1^2 - 4s_2 \qquad s_1(\alpha,\beta) = \alpha + \beta = -b$$

$$= b^2 - 4c \qquad s_2(\alpha,\beta) = \alpha\beta = c$$

- Since $\deg f = 2$, $Gal(f) \leq S_2$

$$\alpha, \beta = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

- f sep. $\Leftrightarrow b^2 - 4c \neq 0$
- $\alpha, \beta \in F \Leftrightarrow Gal(f) = 1$

$\Leftrightarrow Gal(f) \leq A_2 = 1$

$\Leftrightarrow \sqrt{b^2 - 4c} \in F$

Splitting field: $F(\sqrt{D})$

Degree 3:

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

Set $y = x + \frac{a}{3}$ $\quad p = \frac{1}{3}(3b - a^2)$

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

$$f(x) = g(y) := y^3 + py + q$$

"depressed cubic"

f & g have same splitting fields, same disc. since roots off by $\frac{a}{3} \in F$

Roots of g: α, β, γ

$s_1(\alpha, \beta, \gamma) = 0$

$s_2(\alpha, \beta, \gamma) = p$

$s_3(\alpha, \beta, \gamma) = -q$

$$D_y g = 3y^2 + p$$

$$D_y g = (y-\alpha)(y-\beta) + (y-\alpha)(y-\gamma) + (y-\beta)(y-\gamma)$$

$$D_y g(\alpha) = (\alpha - \beta)(\alpha - \gamma)$$

$$D_y g(\beta) = (\beta - \alpha)(\beta - \gamma)$$

$$D_y g(\gamma) = (\gamma - \alpha)(\gamma - \beta)$$

$$D = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$$

$$= -D_y g(\alpha) \cdot D_y g(\beta) \cdot D_y g(\gamma)$$

$$= -(3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)$$

$$= -27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) - 3p^2(\alpha^2 + \beta^2 + \gamma^2) - p^3$$

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

f is $\begin{cases} \text{prod. of 3 linear factors} \longrightarrow \mathrm{Gal}(f) = 1 \\ \text{linear} \cdot \text{irred. quadratic} \longrightarrow \mathrm{Gal}(f) = \mathbb{Z}/2\mathbb{Z} \\ \text{irreducible} \end{cases}$

$$\underset{\substack{\uparrow \\ \text{order} \geq 3}}{A_3 \leq} \mathrm{Gal}(f) \leq S_3$$

So $\mathrm{Gal}(f) = A_3$ iff $D = -4p^3 - 27q^2$ is a square

Splitting field of f: $F(\alpha, \sqrt{D})$

if $\sqrt{D} \in F$, just $F(\alpha)$, automs are $\alpha \mapsto \alpha, \beta, \gamma$

if $\sqrt{D} \notin F$, also have autom $\sqrt{D} \mapsto -\sqrt{D}$.

Degree 4

$f(x) = x^4 + ax^3 + bx^2 + cx + d = g(y) := y^4 + py^2 + qy + r$

$y = x + a/4$ $\quad p = \frac{1}{8}(-3a^2 + 8b)$ $\quad q = \frac{1}{8}(a^3 - 4ab + 8c)$

$$r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d)$$

roots: $\alpha, \beta, \gamma, \delta$ $\quad G := \mathrm{Gal}(g)$, K = splitting field of g

If $g(y)$ = linear $\cdot$ cubic, see cubic case above

If $g(y) =$ irred. quad $\cdot$ irred quad., $K = F(\sqrt{D_1}, \sqrt{D_2})$

If $\frac{\sqrt{D_1}}{\sqrt{D_2}} \in F$, $K = F(\sqrt{D_1})$, $G = \mathbb{Z}/2\mathbb{Z}$

otherwise, $G = K_4$

Now assume g irred.

Since G transitive, $G \leq S_4$, must have

$G =$ one of: S_4, A_4,

$D_8 = \langle (1324), (13)(24) \rangle$, or $\sigma D_8 \sigma^{-1}$,

$V_4 = \langle (12)(34), (14)(23) \rangle$,

or $C = \langle (1324) \rangle$, or $\sigma C \sigma^{-1}$

Important tool: <u>resolvent</u> cubic

Let

$$\left.\begin{aligned} \theta_1 &= (\alpha+\beta)(\gamma+\delta) \leftarrow \text{Fixed by } D_8 \\ \theta_2 &= (\alpha+\gamma)(\beta+\delta) \leftarrow \text{Fixed by another } D_8 \\ \theta_3 &= (\alpha+\delta)(\beta+\gamma) \leftarrow \text{Fixed by another } D_8 \end{aligned}\right\} \text{Fixed by } K_4$$

$s_1(\theta_1, \theta_2, \theta_3) = 2p$ $\quad s_2(\theta_1, \theta_2, \theta_3) = p^2 - 4r$

$s_3(\theta_1, \theta_2, \theta_3) = -q^2$

So $h(x) := (x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$

$$\left.\begin{aligned} \theta_1 - \theta_2 &= -(\alpha-\delta)(\beta-\gamma) \\ \theta_1 - \theta_3 &= -(\alpha-\gamma)(\beta-\delta) \\ \theta_2 - \theta_3 &= -(\alpha-\beta)(\gamma-\delta) \end{aligned}\right\} \text{prod}^2 \text{ of these} = D \quad (!)$$

So disc of g = disc of $h = 16p^4r - 4p^3q^2$

$-128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$

Splitting field of $h \subseteq$ Splitting field of g

Cases:

A) h irred, $\sqrt{D} \notin F$.

$G \nsubseteq A_4$

$\mathrm{Gal}(h) \nsubseteq A_3$ (so $\mathrm{Gal}(h) = S_3$)

So $G = S_4$

B) h irred, $\sqrt{D} \in F$.

$G \leq A_4$

$\mathrm{Gal}(h) = A_3$

$|G| \geq \mathrm{lcm}(4,3) = 12 = |A_4|$

so $G = A_4$

c) h = linear · linear · linear

$\theta_1, \theta_2, \theta_3 \in F = \text{Fix}\, G$

So $G \subseteq K_4$ and since $|G| \geq 4$, $G = K_4$

D) h = linear · irred. quad

One of $\theta_1, \theta_2, \theta_3 \in F$, say θ_1

$G \nsubseteq K_4$

$G \subseteq D_8$

$|G| \geq 4$

So $G = D_8$ or $G = C$

Claim: $G = D_8$ iff $g(y)$ irred over $F(\sqrt{D})$

Pf: $F(\sqrt{D}) = \text{Fix}(G \cap A_4)$

$D_8 \cap A_4 = K_4$ transitive on roots $\to g$ irred.

$C \cap A_4 = \mathbb{Z}/2\mathbb{Z}$ not trans on roots $\to g$ red.