lect 21

Today's office hours: 20 min late

$\boxed{4:20-5:20}$ pm, (overlap Isis' OH)

5–6pm

take-home quiz tomorrow (you'll have a day or two to solve).

I, IX

follow Friedman NGT IV or Rotman

II D_4

x^4-2

Last time:

Thm char F = 0. If $\sqrt{f(x)} \in F[x]$ solvable by radicals, E/F splitting field $\Rightarrow$ $G = Gal(E/F)$ solvable ("glued" from abelian groups)

$x^n - a$, $x^{n_1} - a_1$, $x^{n_2} - a_2$..

In fact $\Leftarrow$

(a little more work; in char 0 in presence of of roots of unity any cyclic extension is radical $x^n - a$

$\underset{\text{abelian} \to \text{solvable}}{\cup}$

(Friedman, Prop. 11.6, IV, page 44)

char F = 2

$\boxed{x^2 + x + a}$

$y = x + \frac{1}{2}$

F

$x^p + x + a$

Need to give eq'n of deg ≥ 5 s.t. $G = Gal(E/F)$ is not solvable

$F = \mathbb{Q}$

deg = 5, $G = A_5, S_5$.

(Rotman).

Thm $f(x) = x^5 - 4x + 2$ /$\mathbb{Q}$ is not solvable in radicals

Eisenstein cr. f is irreducible/$\mathbb{Q}$

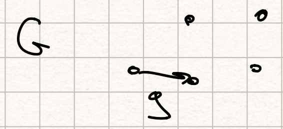
E - split. field, no mult. roots

$\underline{\alpha_1, \dots \alpha_5}$ $\mathbb{Q} \subset E \subset \mathbb{C}$

$\uparrow$ alg. closed

$G = Gal(E/\mathbb{Q}) \subset S_5$

acts transitively on roots, since f is irreducible



transitive $\Rightarrow 5 \mid |G|$.

$G \times X \longrightarrow X$

$|X| = 5$ $\underline{|G| = |X| \cdot |Stab_G(x)|}$ $|x| \mid |G|$

$5 \mid |G|$.

$p \mid |G| \Rightarrow G$ has el't of order p.

$G \subset S_5$ $\underline{p=5}$ $\underline{(12345)} \in G$

$z \mapsto \bar{z}$

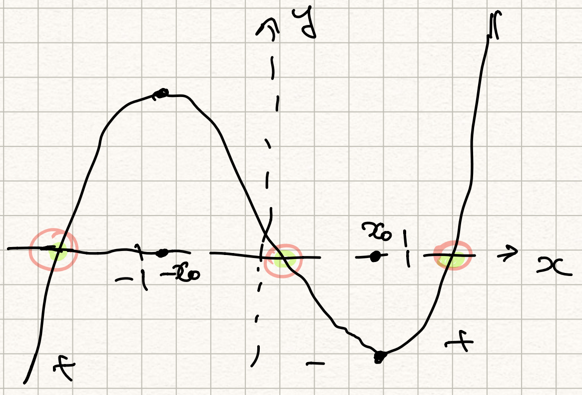
$\mathbb{Q} \subset \underline{E} \subset \mathbb{C}$

$f(x) = x^5 - 4x + 2 \leftarrow$ has some real roots

$f'(x) = 5x^4 - 4$ $f'(x) = 0$ $5x^4 = 4$ $x^4 = \frac{4}{5}$ $x = \pm\sqrt[4]{\frac{4}{5}}$

x $\sqrt[4]{\frac{4}{5}} \approx 0.946 \approx 1.$

$\underline{x_0 = \sqrt[4]{\frac{4}{5}}}$



$f(x_0)$

$\mathbb{C} \xrightarrow{-} \mathbb{C}$ acts on roots

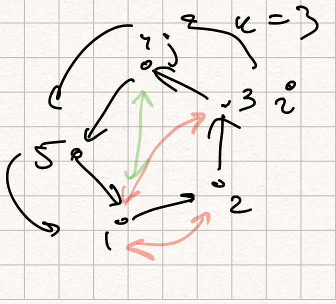
$3 \mapsto \bar{8}$

3 roots are fixed

2 roots are permuted.

— restricts to an element of G

— is a transposition $\underline{(ik)}$



G – contains 5-cycle, transposition

$\sigma = \underline{(12345)}$ $(1\ i)$ $i \in \{2, 3\}$.

$\tau = (12), (13)$

Lemma (Hofman, G39, p. 128). If $G \subset S_5$,

G contains a 5-cycle & a transposition $\Rightarrow G = A_5$.

$$\alpha^k(i) = 1$$

$$\alpha^k \tau \alpha^{-k} = \underset{\uparrow G}{(j1)} \qquad j \neq i \qquad\qquad (1i),(1j) \to \underbrace{(1ij)}_{\text{order } 3} \in G$$

$$\overset{2}{(1i)},\ \overset{5}{\alpha},\ \overset{3}{(1ij)} \qquad 2,3,5 \mid |G| \qquad 30 \mid |G|$$

$$G \subset S_5$$

$$\underline{30} \quad \underline{120}$$

$$\underline{X} = \overset{120}{S_5}/\overset{30}{G} \qquad S_5 \xrightarrow{\text{action on}} X$$

$$S_5 \times X \to X.$$

$$\begin{tikzcd} \underset{\text{simple}}{A_5} \subset S_5 \arrow[r] & S_4 \end{tikzcd} \qquad \ldots\ldots \Rightarrow G = S_5 \qquad \square$$

$$\Rightarrow G \text{ of } \underline{x^5 - 4x + 2} \text{ is } \boxed{S_5}$$

$\Uparrow$ Cannot be solved in radicals

E/F splitting field $f \in F[x]$ $\quad \alpha_1 \ldots \alpha_n$ in E

2^n

$$f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) =$$

$$= x^n - \underline{(\alpha_1 + \ldots + \alpha_n)}\, x^{n-1} + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n)\, x^{n-2} -$$

$$\| \qquad\qquad\qquad \|$$

$$s_1 \text{ (or } e_1) \qquad\qquad s_2$$

$$s_2 = \sum_{1 \le i < j \le n} \alpha_i \alpha_j \qquad \binom{n}{2} = \frac{n(n-1)}{2}$$

$$s_3 = \overset{\binom{n}{3}}{\sum_{i<j<k}} \alpha_i \alpha_j \alpha_k$$

$$- (\alpha_1\alpha_2\alpha_3 + \ldots \quad) x^{n-3} + \ldots + (-1)^n \overset{s_n}{\alpha_1 \ldots \alpha_n}$$

√ ① $s_1 = \alpha_1 + \quad + \alpha_n = \sum_{i=1}^{n} \alpha_i$ n terms

deg ↗ $\sigma(\alpha_i\alpha_j) = \alpha_{i'}\alpha_{j'}$

√ { ② $S_2 = \alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n = \underbrace{\sum_{1 \le i < j \le n} \alpha_i\alpha_j}$ $\binom{n}{2}$ terms

⋮

(k) $\underline{S_k} = \alpha_1 \dots \alpha_k + \dots = \sum_{1 \le i_1 < i_2 \dots < i_k \le n} \alpha_{\underline{i_1}} \alpha_{\underline{i_2}} \dots \alpha_{\underline{i_k}}$ $\binom{n}{k}$ terms

(n) $s_n = \underline{\alpha_1 \dots \alpha_n}$ ± S_k are coefficients of $f(x)$.

$(-1)^k S_k$

$$f(x) = x^n - s_1 x^{n-1} + S_2 x^{n-2} - \dots + (-1)^n s_n$$

$G = \mathrm{Gal}(E/F)$ acts by permutations of α_i's.

G fixes S_k, all k.

↘ symmetric f's of $\alpha_1 \dots \alpha_n$

$\sigma(S_k) = S_k$

2 ways to think about this.

I) $s_k \in F$ coeff. $\alpha_i \in \underline{E}$

II) α_i's are formal variables $R \circlearrowleft S_n$

$h \in \underline{R = F[\alpha_1 \dots \alpha_n]}$ $\sigma = (123)$

S_n acts on R by permuting α_i

$$\begin{tikzcd} & \alpha_3 \arrow[dl] \\ \alpha_1 \arrow[dr] & \\ & \alpha_2 \arrow[uu] \end{tikzcd}$$

Sym ⊂ R ring of symmetric functions. $\sigma(\alpha_1^4 \alpha_2 \alpha_3^2) =$

$h \in$ Sym iff $\sigma(h) = h$ $\forall \sigma \in S_n$ $\alpha_2^4 \alpha_3 \alpha_1^2$

$s_1, s_2 . \ s_n \in R$ $\sigma(s_k) = s_k$.

S_k are called <u>elementary</u> symmetric polynomials.

Thm $\underline{Sym = F[s_1, \dots, s_n]}$. $F[s_1 . \, s_n] \subset Sym$

$\supset$

$\sigma(hg) = \sigma(h)\,\sigma(g) = hg$

Some work to show any symm. polyn is a f'n of $s_1 \dots s_n$

$\underline{n=2}$ $F[\alpha_1, \alpha_2]$ $s_1 = \alpha_1 + \alpha_2$, $s_2 = \alpha_1 \alpha_2$

$(12)(\alpha_1^2 + \alpha_2^2) = \alpha_2^2 + \alpha_1^2$

$\alpha_1^2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 = s_1^2 - 2s_2$

$\alpha_1^3 + \alpha_2^3 = (\alpha_1 + \alpha_2)^3 - 3(\alpha_1^2\alpha_2 + \alpha_1\alpha_2^2) = (\alpha_1 + \alpha_2)^3 - 3\alpha_1\alpha_2(\alpha_1 + \alpha_2)$

$= s_1^3 - 3 s_1 s_2 \in F[s_1, s_2]$. power $p_m = \alpha_1^m + \alpha_2^m + . + \alpha_n^m$

$\alpha_1^3 \alpha_2^0$

Ex 1) Show by ind $\alpha_1^m + \alpha_2^m \in F[s_1, s_2]$

2) prove the theorem

deg=3

$\underline{n=3}$ $\alpha_1^2 \alpha_2 \xrightarrow{\text{symm}} \boxed{\alpha_1^2 \alpha_2} + \alpha_1^2\alpha_3 + \alpha_2^2\alpha_1 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 + \alpha_3^2\alpha_2 = w$

$\underset{s_2}{(\alpha_1\alpha_2 + \dots)}\ \underset{s_1}{(\alpha_1 + ..)}$

6 terms

$(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)(\alpha_1 + \alpha_2 + \alpha_3) = (\alpha_1^2\alpha_2 + \dots) + 3\alpha_1\alpha_2\alpha_3$

$\underset{\overset{\shortparallel}{s_2}}{}$ 2 1 $\underset{\overset{\shortparallel}{s_1}}{}$ w 3 $\overset{\shortparallel}{s_3}$

s_1^3

$$\boxed{w = s_2 s_1 - 3 s_3}$$

$\uparrow$ $\uparrow$

$\underline{n=2}$ $Sym = F[x_1 + x_2, x_1 x_2]$

$\cap$

$F[x_1, x_2]$

$\deg \alpha_i = 1$

$Sym \subset F[\alpha_1 .. \alpha_n]$

$\cong$

$F[s_1, s_2, .. s_n]$

$\deg s_1 = 1 ..$ $\deg s_k = k$

I) $\alpha_i \in E.$ $\qquad s_k \in F \qquad (-1)^k s_k$

$x^2 + \overset{s_1}{\boxed{b}}x + \overset{s_2}{\boxed{c}}$ $\qquad \alpha_1 + \alpha_2 = \boxed{-b}, \ \alpha_1\alpha_2 = \boxed{c.}$

$\|$

$(x-\alpha_1)(x-\alpha_2)$ $\qquad \mathcal{D} = b^2 - 4c = (\alpha_1 - \alpha_2)^2$

$\|$

$x^2 \boxed{-(\alpha_1+\alpha_2)}x + \boxed{\alpha_1\alpha_2}$ $\qquad \sqrt{\mathcal{D}} = \underset{\uparrow}{\pm}(\alpha_1 - \alpha_2) \qquad \sqrt{\mathcal{D}} = \alpha_1 - \alpha_2$

$\alpha_1 \leftrightarrow \alpha_2$

$$\begin{cases} \alpha_1 - \alpha_2 = \sqrt{\mathcal{D}} \\ \alpha_1 + \alpha_2 = -b \end{cases} \to \quad 2\alpha_1 = -b + \sqrt{\mathcal{D}} \qquad \alpha_1 = \frac{-b+\sqrt{\mathcal{D}}}{2}.$$

II) $\alpha_1 - \alpha_2 \notin Sym$ $\qquad \sigma = (12) \qquad \sigma(\alpha_1 - \alpha_2) = \alpha_2 - \alpha_1$

not a symm f'n $\qquad (\alpha_1 - \alpha_2)^2 \in Sym$

$n = 3$ $\qquad \delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \qquad \alpha_i - \alpha_j \quad i < j$

$(12)\,\delta = \underset{-1}{(\alpha_2 - \alpha_1)}(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) = -\delta$ $\qquad$ not symm

Ex $\qquad \sigma\,\delta = \underline{\mathrm{sgn}(\sigma)}\,\delta \qquad \mathrm{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$

$\sigma \in S_3$ $\qquad S_n \xrightarrow{\mathrm{sgn}} \{\pm 1\}$

$\Delta = \delta^2 \in Sym \qquad \sigma(\delta^2) = \delta^2$

discriminant $\qquad \Delta = 0$ iff two roots coincide

Thm let $\delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$ $\qquad \binom{n}{2}$ terms.

then $\sigma(\delta) = \mathrm{sgn}(\sigma)\,\delta.$ $\qquad$ | in symm. f'n

$\sigma \in S_n$ $\qquad$ | in field E

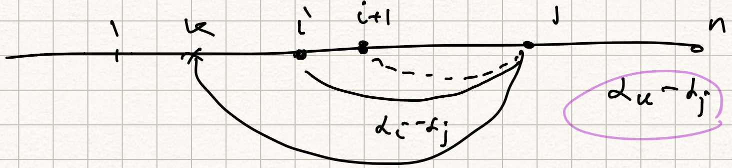
| $\sigma \in Gal(E/F)$

Proof $\qquad \tau_i = (i, i+1)$ $\qquad$ elementary transp.

$\tau_i : \quad \boxed{\alpha_i - \alpha_{i+1}} \mapsto \alpha_{i+1} - \alpha_i = -\boxed{(\alpha_i - \alpha_{i+1}).}$

$$\underline{\alpha_i - \alpha_j} \xrightarrow{\tau_i} \underline{\alpha_{i+1} - \alpha_j} \qquad i<j$$

$j>i+1$ $\qquad\qquad\qquad\qquad$ $i+1<j$



$$\alpha_k - \alpha_j \longmapsto \alpha_k - \alpha_j$$

$k, j \notin \{i, i+1\}$

$$\tau_i(\delta) = -\delta. \Rightarrow \sigma(\delta) = \operatorname{sgn}(\sigma)\,\delta.$$

δ - antisymm. f'n

preserved by even, reversed by odd.

$\underline{\underline{Ex}}$ $\forall$ antisymm. polyn g has the form $g = \delta \cdot \overset{\Uparrow}{h}$

h - symmetric

$\Delta = \delta^2$ — Discriminant $\qquad \sigma(\Delta) = \Delta \ \forall \sigma$

$$\frac{\Delta \in Sym}{\Delta \in F}$$

polyn $\qquad \alpha_1 \ldots \alpha_n$ roots

$$\begin{tikzcd}
 & & E \arrow[d, dash] & F[\alpha_1 \ldots \alpha_n] \arrow[l] \arrow[d, dash] \\
E & f(x) \arrow[ur] & \underline{F} & \underline{Sym} \arrow[l] \\
 & & (-1)^k a_{n-k} & s_k \arrow[l, mapsto]
\end{tikzcd}$$

$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$

$Sym = F[s_1 \ldots s_n]$.

$F = E^G \qquad \Delta \in F \qquad \Delta \in Sym$

$\underline{n=3}$ $\qquad \delta = \underline{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)} \qquad \delta^2 \in F$

$$\underset{\Delta}{\overset{\shortparallel}{\delta^2}} \in F$$

1st step

$$\underline{\underline{\sqrt{\Delta}}} = \underline{\underline{\delta}}$$

$$\begin{tikzcd}
F \arrow[r, phantom, "\subset"] \arrow[rr, bend right, "6"'] & F(\sqrt{\Delta}) \arrow[r, phantom, "\subset"] \arrow[r, bend left] & E
\end{tikzcd}$$

2 $\qquad$ 3

s_1, s_2, s_3

$$\underline{x^3 - s_1x^2 + s_2x - s_3}.$$

$$x^3 + a_2x^2 + a_1x + a_0$$