Last time

- If E/F is a galois extn $\Rightarrow$ E is splitting field of some $f(x) \in F[x]$

conversely for any $f(x) \in F[x]$, its splitting field is Galois

Cor Given any finite ext E/F $\exists$ (finite) Galois ext M/F and an F-emb $E \to M$.

Pf let $E = F(a_1, \dots, a_m)$ (finite) let f_i = min poly of a_i

$f(x) = f_1(x) \cdots f_n(x)$

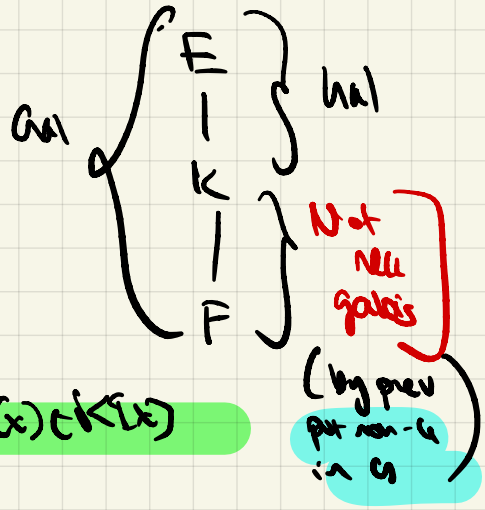
let M = splitting field of f

Rmk 1) $\exists$ "minimal M", this is called Galois Closure of E

2) Cor. is false in pos char.

Cor By we have E/F Galois & K intermediate

$\Rightarrow$ E/K is Galois.



Pf Since E gal $/F \Rightarrow E$ is splitting field of $f \in F[x]$.

Regard $f \in K[x] \Rightarrow E$ splitting field of $f(x) \in K[x]$

$\to E$ gal $/K$

Recall if E/F is Extn & $H \subset \mathrm{Gal}(E/F)$, the fixed field $E^H = \{x \in E \mid \sigma(x) = x \ \ \forall \sigma \in H\}$

Main thm of Gal Theory

E/F is a (finite) Galois Extn.

$\exists$ bij corr $\{$ subgrp of $\mathrm{Gal}(E/F)\} \longrightarrow \{$ Intermediate field $\}$

$H \longrightarrow E^H$ ✓

subgrp of $\mathrm{Gal}(E/F)$ $\longleftarrow$ $\mathrm{Gal}(E/K) \longleftarrow K$ ✓

Say $H \longleftrightarrow K = E^H$

$\#H = [E:K]$

$[Gal(E/F):H] = [K:F]$

} can remember by thinking $H = 1$

$\Rightarrow K = E$

$\Rightarrow [E:K] = 1$

If $H \longleftrightarrow K = E^H$. Then H is normal subgp of $Gal(E/F)$ iff K/F is Gal extn

The corr is order reversing, i.e. if $H_1, H_2 \leq Gal(E/F)$

$\Rightarrow H_1 \subset H_2 \iff E^{H_2} \subset E^{H_1}$

Appl.1 $H_1 \cap H_2$ is the largest subgp $\subset H_1$ & H_2

$\Rightarrow E^{H_1 \cap H_2}$ is the smallest field $\supseteq E^{H_1}$ & E^{H_2}

$\Rightarrow E^{H_1 \cap H_2}$ = Compositum of E^{H_1} & E^{H_2}

field gen'd by E^{H_1} & E^{H_2}

E.g. $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$[E:F] = 4$ $Gal(E/F) = \{1, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$

so $\sigma(\sqrt{2}) = -\sqrt{2}$ $\sigma(\sqrt{3}) = \sqrt{3}$

$\tau(\sqrt{2}) = \sqrt{2}$ $\sigma(\sqrt{6}) = -\sqrt{6}$

Subgrp	int Fields
1	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \tau\sigma\}$	$\mathbb{Q}(\sqrt{6})$ — $\sigma(\sqrt{6}) = \sqrt{6}$
$\{1, \sigma, \tau, \tau\sigma\}$	$\mathbb{Q}$

eg1 $F = \mathbb{Q}$ $E = $ spl fd $x^3 - 2$ $E = \mathbb{Q}(\sqrt[3]{2}, \zeta)$

$[E:F] = 6$ → 2 cube roots

$Gal(E/F) = S_3$

(Galois 3 divides 6) ↪ get other $\sqrt[3]{2}$. ↪ $\zeta = e^{2\pi i/3}$

$DE = \mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})$

↪ divide toget ζ

Subgp	Int
$\{1\}$	E
$\{1, (12)\}$ (strong hyp no)	$\mathbb{Q}(\zeta^2\sqrt[3]{2})$
$\{1, (13)\}$	$\mathbb{Q}(\zeta\sqrt[3]{2})$ } not normal
$\{1, (23)\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, (123), (132)\}$	$\mathbb{Q}(\zeta)$ } normal → $\mathbb{Q}(\zeta)$ gal
S_3	$\mathbb{Q}$

Cor1 if E/F finite extn

=> only ∃ fin many intermediate fields !

Pf) Choose $E \subset M$ where M/F galois

=> {inter of M/F} > {inter of E/F}

↕

{Subgps of $Gal(M/F)$} (finite) → finite

Rmk1 Cor false in pos char.

→

Setup $f(x) \in F[x]$ irred cubic poly. → so Galois

Let E/F be its splitting field, $G = Gal(E/F)$

perm roots ← We know $G \subset S_3$ & acts transitively on the three roots (prev work)

$\Rightarrow G = A_3$ or S_3 (only ones that act trans)

Q) How do we know which one?

A) discr.

Write $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$\delta = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$

$D = \delta^2$ (disc)

for $\sigma \in S_3$ $\sigma\delta$ (permute α_i) $= sgn(\sigma)\,\delta$

$\Rightarrow D$ invariant under σ.

So D is fixed by $Gal(E/F)$ so $D \in F$ (so $\delta \in E$ w/ $\delta^2 \in F$)

In fact, can express D as poly in coeff for f.

E.g. if $f(x) = x^3 + px + q$ → can use the x^2 at

$D = -4p^3 - 27q^2$

Prop $G = A^3 \iff D$ is a square in F.

Pf if $G = A^3 \Rightarrow G$ fixes δ (differ by sgn which is 1 in A^3)

$\Rightarrow \delta \in F$

if D is a sqr in $F \Rightarrow \delta \in F$

$\Rightarrow \delta$ fixed by $G \Rightarrow G = A_3$