Galois Thm (All fields are char 0)

E/F — finite field ext

$Gal(E/F)$ = gp of all F-aut of E. (Galois gp)

e.g. $\mathbb{C}/\mathbb{R}$ $Gal(\mathbb{C}/\mathbb{R}) = \{1, \gamma\}$ ← complex conj

If σ a arb $\mathbb{R}$-aut of $\mathbb{C}$, $\sigma(i) = \pm i$ → b/c $\mathbb{R}$ aut

$\sigma(a+bi) = a + b\sigma(i)$

if $\sigma(i) = i \Rightarrow \sigma \equiv id$

$\sigma(i) = -i \Rightarrow \sigma \equiv \gamma$

e.g. $E = F(\sqrt{\delta})$ $\delta \neq \square$ in F

$\exists$ F-aut $\gamma : E \to E$ s.t. $\gamma(\sqrt{\delta}) = -\sqrt{\delta}$

This follows from min poly of $\sqrt{\delta}$ is $x^2 - \delta$ its 2 roots are $\pm\sqrt{\delta}$

$Gal(E/F) = \{1, \gamma\}$

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

quad ext

$\mathbb{Q}(\sqrt{2},\sqrt{3})$

$\mathbb{Q}(\sqrt{2})$

$\mathbb{Q}$

By prev $\exists$ $\mathbb{Q}(\sqrt{2})$-aut

$\sigma : \mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{3})$

s.t. $\sigma(\sqrt{3}) = -\sqrt{3}$ also $(\sigma(\sqrt{2}) = \sqrt{2})$

This is also a $\mathbb{Q}$ aut of $\mathbb{Q}(\sqrt{2},\sqrt{3})$

$\Rightarrow \sigma \in Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

Also $\exists$ $\gamma \in Gal(\text{—})$ so $\gamma(\sqrt{3}) = \sqrt{3}$

$\gamma(\sqrt{2}) = -\sqrt{2}$

also have $\sigma \circ \gamma$ which flips both

This is all so $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong (\mathbb{Z}/2)^2$

Why is this all, if $\theta \in Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

We know, $\theta(\sqrt{2})^2 = 2 \Rightarrow \theta(\sqrt{2}) = \pm\sqrt{2}$, $\theta(\sqrt{3}) = \pm\sqrt{3}$

$\exists$ i, j so θ agrees w/ $\gamma^i\sigma^j$ on $\sqrt{2}, \sqrt{3}$

$\Rightarrow \theta = \gamma^i\sigma^j$ as $\sqrt{2}, \sqrt{3}$ gen

Eg $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$

If $\sigma \in \mathrm{Gal}(-)$ then $\sigma(\sqrt[3]{2})^3 = 2$

$\Rightarrow \sigma(\sqrt[3]{2})$ is a cube root of 2 in $\mathbb{Q}(\sqrt[3]{2})$

Since $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $\sqrt[3]{2}$ is the only cube root of 2 in this field

$\Rightarrow \sigma(\sqrt[3]{2}) = \sqrt[3]{2} \Rightarrow \sigma = id$

Thm if E/F is a finite extension, then

$\#\mathrm{Gal}(E/F) \mid [E:F]$

Def E/F is a Gal ext if $\#\mathrm{Gal}(E/F) = [E:F]$

Eg
- quadratic extn are Galois
- $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is Galois
- $\mathbb{Q}(\sqrt[3]{2})$ is not Galois.

Def Given E/F and a subgp $H \subset \mathrm{Gal}(E/F)$

define $E^H = \{a \in E \mid \sigma(a) = a \ \forall \sigma \in H\}$

↳ fixed field of H

eg $E/F = \mathbb{C}/\mathbb{R}$ $\quad H = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$

$E^H = \{a \in \mathbb{C} \mid \bar{a} = a\} = \mathbb{R}$

E^H is a subfield of E, containing F.

Prop Say E/F is Galois & $G = \mathrm{Gal}(E/F)$

$\Rightarrow E^G = F$

Pf Since, G fixes everything in E^G

$G \subset \mathrm{Gal}(E/E^G)$

$\#G \quad [E:F] \quad \leq [E:E^G] \overset{\text{tower}}{=} \dfrac{[E:F]}{[E^G:F]}$

$\Rightarrow [E^G:F] = 1$

if E/F is NOT Galois we have $\mathrm{Gal}(E/F) \subsetneq \mathrm{Gal}(E/K)$

Appl E/F is Gal w/ gp G given any $a \in E$ then

$\prod_{\sigma \in G} \sigma(a)$ is fixed by G (would permute τ) $\Rightarrow \in E^G = F$

i.e $\tau \in G$

$\tau(\prod \sigma(a)) = \prod (\tau\sigma)(a)$

$\tau\sigma$ is a perm

$= \prod \sigma'(a)$

Thm if $f(x) \in F[x]$ is any poly then the splitting field for f is Galois.

Conversely if E/F is Galois then E is the splitting field of some poly.

Say E is the splitting field of $f(x)$.

Obs 1 $G = Gal(E/F)$ this permutes the roots of f

if $\sigma \in G$ and $\alpha \in E$ is a root of f

Then $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$ $\Rightarrow \sigma(\alpha)$ is a root

Fact: $f \in F[x]$ $\rightarrow$ passes through all

Obs 2 The action of G in the roots is faithful.

Reason: if we know how $\tau \in G$ acts on roots $\Rightarrow$ we know σ b/c roots gen E.

Say $f(x) = (x - a_1) \cdots (x - a_n)$

and assume no repeated roots

Above $\Rightarrow$ $G \subseteq S_n$ (perms of $1, \dots, n$)

Thm The action of G on the roots is trans

$\Leftrightarrow$ the poly is irred

#1 if $f(x) = g(x)h(x) \Rightarrow$ G maps roots of g to g, h to h
(G not irred)

$\Rightarrow$ G not trans

If f is irred, say α root of f.

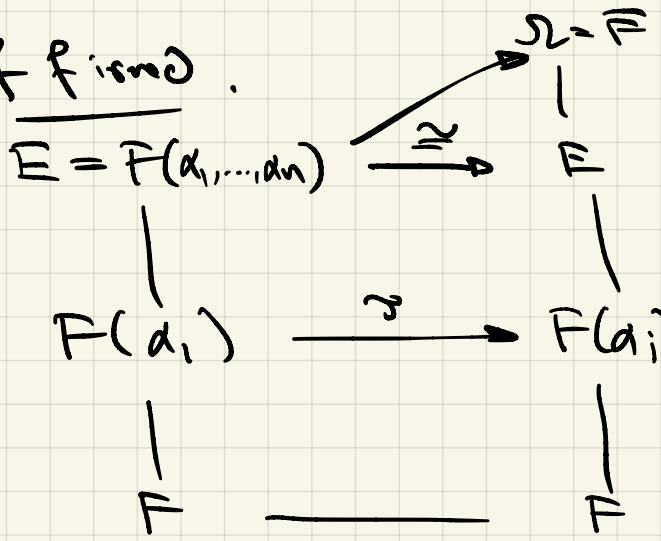
Let $\alpha_1, \dots, \alpha_m$ is the G orbit of α

Consider, $g(x) = (x-\alpha_1)\cdots(x-\alpha_m)$ & $g(x) \mid f(x)$

G fixes coeff of g $\Rightarrow$ $g \in F[x]$
(it'll just permute $\alpha_1, \dots, \alpha_m$)

Since $g \mid f$ & f irred $\rightarrow$ $g = f$ $\Rightarrow$ $m = n$ so trans!

#11 if f irred.



$\exists$ F isom σ st $\sigma(\alpha_1) = \alpha_i$ by stem field. end

from earlier, $\exists$ ext of σ

from $E \to \Omega$