E/F Galois (normal + separable)

$G = Gal(E/F)$ $\quad H \subset G$

$F \subset E^H \subset E$

$E^H = \{a \mid h(a) = a \ \forall a \in H\}$.

$E^H(\alpha)$

Remember $\forall$ fin $F \subset E$
$|G| \leq [E:F]$
$= $ for Galois

Prop $\forall \alpha \in E$, $\deg_{E^H} \alpha = [E^H(\alpha) : E^H] \leq |H|$

H-invariants in E, subfield

$F \subset E^H \subset E^H(\alpha) \subset E$

$f(x) = \prod_{\delta \in H} (x - \delta(\alpha))$

poly in x, deg $= |H|$

monic.

$f(x) \in E[x]$

$(x-\alpha)(x-\delta(\alpha))$

E E

α δ $\delta(\alpha)$

$H\alpha \subset E$

$\uparrow$ orbit of α under H

Example

$E = \mathbb{C}$ $\quad H = \{1, \delta\}$ $\quad \delta(z) = \bar{z}$

$\mathbb{R} = \mathbb{C}^H$

$(x-\alpha)(x-\delta(\alpha))$

$= (x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}[x]$.

$\alpha, \bar{\alpha} \to \mathbb{R}$

Coeff $\alpha + \bar{\alpha} = 2a \in \mathbb{R}$

$\alpha\bar{\alpha} \in \mathbb{R}$

$\alpha = a + bi$ $\quad a^2 + b^2$

$\bar{\alpha} = a - bi$

Claim Coeffs. of $f(x)$ are in E^H.

H-invariant subfield

$H \subset G \subset E$ $\quad X \circlearrowleft G$

H acts on $E[x]$ acts by identity on x

$\tau \in H$. $\quad \tau(a+bx+cx^2) = \tau(a)+\tau(b)x+\tau(c)x^2$

$$\tau(f(x)) = \tau\left(\prod_{\delta\in H}(x-\delta(\alpha))\right) = \prod_{\delta\in H}\tau(x-\delta(\alpha)) = \prod_{\delta\in H}(x-\tau(\delta(\alpha)))$$

$$= \prod_{\delta\in H}(x-\underbrace{\tau\delta}_{\gamma}(\alpha))$$

(τ fixed, δ varies; as δ runs over H, $\gamma = \tau\delta$ runs over H)

$$= \prod_{\gamma\in H}(x-\gamma(\alpha)) = \prod_{\delta\in H}(x-\delta(\alpha)) = f(x)$$

rename γ into δ

$\tau = 1 \quad x-\alpha \mid f(x)$

all coefficients of f are in E^H.

Compare $f(x)$ $g(x) = \mathrm{irr}(\alpha, E^H, x)$

α - root of $g(x)$, $f(x)$ $\quad f(\alpha)=0$, $g(\alpha)=0$

$\Rightarrow g(x) \mid f(x) \Rightarrow \deg g \le \deg f = |H|$.

$E^H \subset E^H(\alpha) \subset E$

$\curvearrowright = \deg g(x)$.

$\Rightarrow \deg g(x) \leq |H|$. □

Use primitive element thm $\exists \alpha$

$E = E^H(\alpha) \Rightarrow [E:E^H] = \deg g \leq |H|$.

$[E:E^H] \leq |H|$

$H \hookrightarrow E^H$

$|H| \leq [E:E^H]$

E/E^H is Galois since E/F is Galois

$F \subset E^H \subset E$

Corollary If E/F Galois, $H \subset Gal(E/F)$

$\Rightarrow [E:E^H] = |H|$

Remark: always holds $[E:E^H] = |H|$ for any finite group H acting on a field E

Fix E/F Galois $G = Gal(E/F)$.

$|G| = [E:F]$.

Take $F \subset K \subset E$ intermediate field.

$K \rightarrow H = Gal(E/K) \rightarrow E^H$.

H: G, potentially may get more el's in E^H

E^H: everything fixed by H.

$K \subset E^H$

E/k is Galois $\Rightarrow [E:k] = |H|$.

$[E:E^H] = |H|$

$F \subset K \subset E^H \subset E$

$|H|$ over $E^H \subset E$; 1 over $F \subset K$

$[E:K] = [E:E^H]\,[E^H:K]$

$|H| \quad |H| \quad 1$

$E^H = K$.

subfield K $\rightarrow$ subgroup H $\rightarrow$ $E^H = K$.

$H \subset G$ subgroup $\rightsquigarrow$ subfield $K = E^H \rightarrow \underline{\mathrm{Gal}(E/k)}$, $\underline{H}$

$[E:K] = |\mathrm{Gal}(E/k)|$

$[E:E^H] = |H|$.

$\Rightarrow \mathrm{Gal}(E/k) = H$.

$\Rightarrow$ get a bijective correspondence between subfields and subgroups.

Rmk (Main Theorem of Galois Theory)

For a Galois extension $F \subset E$, $\mathrm{Gal}(E/F)$

1) $\exists$ a bijection

subfields K $\rightleftharpoons$ subgroups $H \subset G$

$F \subset K \subset E$

$K \longmapsto H = \mathrm{Gal}(E/k)$

$E^H \longmapsto H$

2) This bijection is order-reversing

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

$F \subset K_1 \subset K_2 \subset E \Rightarrow Gal(E/K_2) \subset Gal(E/K_1)$

3) $\forall H \subset G \quad [E : E^H] = |H| \quad |G|$

$[E^H : F] = (G : H)$ index

$F \subset E^H \subset E$

index of H in G ; order of H

$|Gal(E/K)| = [E:K] = \frac{[E:F]}{[K:F]}$

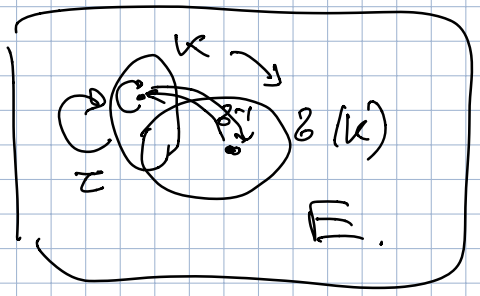
$[E:K] = |Gal(E/K)|$

$[K:F]$

4) $F \subset K \subset E$, K is a normal extension of F iff $Gal(E/K) \subset Gal(E/F)$ is a normal subgroup, $H \triangleleft G$. Then K/F is Galois &

$Gal(K/F) = Gal(E/F) / Gal(E/K)$

Part 4):

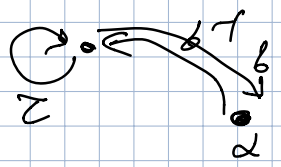


if K is not normal

$\exists \sigma \quad \sigma(K) \neq K$.

if $\tau \in Gal(E/K)$

$\sigma\tau\sigma^{-1}$ – fixes $\sigma(K)$



$\tau \in Gal(E/K) \iff$

$\sigma\tau\sigma^{-1} \in Gal(E/\sigma(K))$.

$Gal(E/K)$, $Gal(E/\sigma(K))$ are conjugate in G

$Gal(E/\sigma(K)) = \sigma\, Gal(E/K)\, \sigma^{-1}$

$\sigma H \sigma^{-1} = H \;\forall \sigma \in G \iff H \lhd G$ normal $\iff$

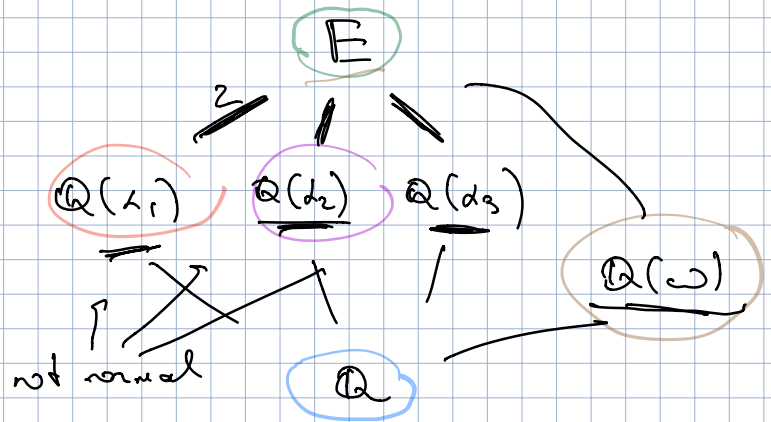
K/F is normal.

$E/\mathbb{Q}$ $\quad x^3-2$ $\quad E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ $\quad \omega = e^{2\pi i/3}$

$\alpha_1 = \sqrt[3]{2}$

$\alpha_2 = \omega\sqrt[3]{2}$

$\alpha_3 = \omega^2\sqrt[3]{2}$



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

$G \to S_3$ ← isom.

$[E:\mathbb{Q}] = 6$

G all perm of $\alpha_1, \alpha_2, \alpha_3$. (23)

S_3

$\mathrm{Gal}(E/\mathbb{Q}(\alpha_1)) \simeq H_1$

$H_1 = \{1, (23)\}$ $\{1, (13)\}$ $\{1, (12)\}$ A_3

$\{1\}$

$\alpha_1 \to \alpha_2 \to \alpha_3 \to \alpha_1$

$\omega = \frac{\alpha_2}{\alpha_1} = \frac{\alpha_3}{\alpha_2}$

$\mathrm{Gal}(E/\mathbb{Q}(\omega)) \simeq A_3$ even permutation.

$= \{1, (123), (132)\}$

These are the only subfields of $\frac{E}{\mathbb{Q}}$.

$\underline{\mathbb{Q}}$

Every element of E generates E

$\alpha \notin$ in these 4 fields $\mathbb{Q}(\alpha) = E$

2) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ $(x^2-2)(x^2-3)$.

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

$\sqrt{2} \leftrightarrow -\sqrt{2}$: σ_1 fixes $\sqrt{3}, -\sqrt{3}$

$\sqrt{3} \leftrightarrow -\sqrt{3}$: σ_2 fixes $\pm\sqrt{2}$

$G \simeq C_2 \times C_2$

$G \simeq C_2 \times C_2$

$\langle \sigma_1 \rangle$ $\langle \sigma_2 \rangle$ $\langle \sigma_1 \sigma_2 \rangle$ C_2

$\{1\}$

$\langle \sigma_1 \rangle = \mathrm{Gal}(E/\mathbb{Q}(\sqrt{3}))$

E

$\mathbb{Q}(\sqrt{3})$ $\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}(\sqrt{6})$

$\mathbb{Q}$

$\sqrt{6} \xrightarrow{\sigma_1 \sigma_2} \sqrt{6}$

$F_2 \subset F_4 \subset F_{16}$

$C_4 \quad C_2 \quad \{1\}$

$\| \quad \langle \delta^2 \rangle$

$\delta(a) = a^2$

$\uparrow$

C_4.

---

p_1, p_2, p_3 – primes $\qquad (x^2-p_1)(x^2-p_2)(x^2-p_3)$

$E = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ $\qquad \deg E/\mathbb{Q}$.

$\cup$

$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ $\Big\}$ 4

$\cup 2$

$\mathbb{Q}(\sqrt{p_1})$

$\cup 2$

$\mathbb{Q}$

if $\sqrt{p_3} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) = K$

then indeed $[E:\mathbb{Q}] = 8$

$\sqrt{p_2} \notin \mathbb{Q}(\sqrt{p_1})$.

$\sqrt{p_3} = a + b\sqrt{p_1} + c\sqrt{p_2} + d\sqrt{p_1 p_2}$ $\quad a, \dots \in \mathbb{Q}$.

if $\sqrt{p_3} \in K$ then $\mathbb{Q}(\sqrt{p_3}) \subset K$

$\cup$ $\quad$ 2 $\quad$ order

$\mathbb{Q}$ $\quad$ index of subgroup $C_2 \times C_2$

$\mathbb{Q}(\sqrt{p_1}), \ \mathbb{Q}(\sqrt{p_2}), \ \mathbb{Q}(\sqrt{p_1 p_2})$

$\not\ni \sqrt{p_3}$ $\quad \not\ni$

$\deg(E/\mathbb{Q}) = 8$.

$p_1, \dots p_n \qquad \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2} \dots \sqrt{p_n}) = E$

Ex prove by induction that $\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2} \dots \sqrt{p_{n-1}})$

$\|$

K

Otherwise, $\mathbb{Q}(\sqrt{p_n}) \subset K$.

Classify subfields of K ↑ L $\quad \mathbb{Q} \subset L \subset K$

$[L:\mathbb{Q}]=2 \iff H$

---

back to p_1, p_2, p_3. $\quad (x^2-p_1)(x^2-p_2)(x^2-p_3)$

$G \subset \simeq C_2 \times C_2 \times C_2$ $\quad \pm\sqrt{p_1}, \ \pm\sqrt{p_2}, \ \pm\sqrt{p_3}$

$\deg(E/\mathbb{Q}) = 8$. $\quad \sqrt{p_1} \to -\sqrt{p_1}, \ \sqrt{p_2} \to -\sqrt{p_2}$

$\uparrow |G|$.

Subgroups of G ↙ ↘ Intermediate fields $\mathbb{Q} \subset K \subset E$

$H \subset G \quad |H| = 1, 2, 4, 8.$

trivial ↑ ↑ ↑ G $\quad H_1$ 7 subgroups

7 subgroups

$H = \{1, \sigma\} \quad \sigma \in G \setminus \{1\}$.

$[E^H : \mathbb{Q}] = 4$. $\quad [E^{H_1} : \mathbb{Q}] = 2$.

$C_2 \times C_2 \times C_2 \xrightarrow{\varphi} C_2$ $\quad \varphi$ surjective

8 $\quad$ 2

$\ker \varphi \simeq H_1, \quad |H_1| = 4$.

$C_2 \times C_2 \times C_2 \xrightarrow{\varphi} C_2$ $\quad$ 8 homomorphisms

$g_1 \ g_2 \ g_3 \to \{1, g\}$ $\quad$ exclude trivial hom.

7 hom 7 subgroups

$\mathbb{Q} \subset_2 K \subset E$ $\quad \mathbb{Q}(\sqrt{p_1}\cdot\sqrt{p_2}\cdot\sqrt{p_3})$

$\mathbb{Q}(\sqrt{p_1}) \quad \mathbb{Q}(\sqrt{p_2}) \quad i=1,2,3$

$\mathbb{Q}(\sqrt{p_1p_2}) \quad \mathbb{Q}(\sqrt{p_1p_3}) \quad \mathbb{Q}(\sqrt{p_2p_3}) \quad , \mathbb{Q}(\sqrt{p_1p_2p_3})$.

$\sqrt{p_4} \notin E \quad p_4 \notin \{p_1, p_2, p_3\}$ $\quad n \nearrow$ n choices

enough to show $\sqrt{p_4} \notin \mathbb{Q}(\sqrt{n})$

$\Rightarrow$ use induction $\quad p_1 \dots p_n$ — n primes

$E = \mathbb{Q}(\sqrt{p_1} \dots \sqrt{p_n})$

$[E:\mathbb{Q}] = 2^n \qquad G = C_2 \times \dots \times C_2$ (n times)

$\forall \quad \mathbb{Q} \subset_2 K \subset E \qquad \boxed{K = \mathbb{Q}(\sqrt{m})}$

m — product of some of p_i's.

abelian Galois group.

$K \leftrightarrow H \subset G \qquad (G:H) = 2$

$H \subset G \quad |H| = 2 \leftrightarrow K, \quad \mathbb{Q} \subset K \subset_2 E$

under order

E

order of H, always normal extension

K

$|$ Index of H, normal iff $H \lhd G$.

$\mathbb{Q}$