$f \in F[x]$ separable $\quad f = f_1(x) \cdots f_r(x)$, $f_i(x)$ irreducible $\forall i$ lect 17

each $f_i(x)$ has simple roots only in $\forall$ extension of F

take the splitting field E of F. Then any $\alpha \in E$ is separable $/F$,

that is, $irr(\alpha, F, x)$ has only simple roots (in E or in any extension of F),

$g(x) =$
roots $=$ deg $irr(\alpha, F, x)$.

f separable $\Rightarrow$ E/F is Galois (normal since E is splitting field & separable)

$\Updownarrow$

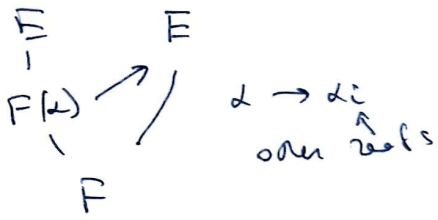
$|Gal(E/F)| = [E:F]$

$\Downarrow$

$g(x)$ has simple roots only (otherwise not enough automorphisms

$\Downarrow$

$irr(\alpha, F, x)$ is separable $\forall \alpha \in E$.



Use one separable polynomial f to build an extension E/F (splitting field) $\Rightarrow$

$\forall$ elements of E are separable $/F$.

Similar to our result on splitting field: god splitting field from one polynomial $\Rightarrow$ can get it for any collection of generators of E. E/F

Thm (primitive element theorem).
Let F be a perfect field & E a finite extension of F.
Then there exists $\alpha \in E$ such that $E = F(\alpha)$

perfect = char 0 or $F^p = F$ (char $p \neq 0$)

Same proof as the one we gave in char 0.

Over a perfect field any finite extension is separable.

Thm also works for finite separable extensions.

E/F Galois (normal + separable) $\quad H \subset \mathrm{Gal}(E/F)$ subgroup

$F \subset E^H \subset E$ fixed field.

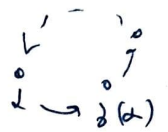
Prop: $\forall \alpha \in E$, $\deg_{E^H} \alpha \leq |H|$

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

monic

$\deg f = |H|$

# of factors $= |H|$



orbit of α under H.

Claim: Coefficients of $f(x)$ are in E^H,

that is $f(x) \in E^H[x]$.

Let $\tau \in H$. We know $f(x) \in E(x)$,

can act by τ on $f(x)$ (on all coefficients)

$E \supset H \quad E[x] \supset H$

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

as β runs o.v. H, $\tau\beta$ runs over H

$$= \prod_{\gamma \in H} (x - \gamma(\alpha)) = \prod_{\beta \in H} (x - \beta(\alpha)) = f(x). \quad \Rightarrow f(x) \in E^H[x]$$

relabel γ back to β

$\Rightarrow \mathrm{irr}(\alpha, E^H, x) \mid f(x) \Rightarrow \deg g(x) \leq \deg f(x) = |H|$

$g(x)$ $\qquad$ $\deg_{E^H} \alpha$

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

Remark: $\forall$ finite $F \subset \bar{F}$

$|\mathrm{Gal}(\bar{F}/F)| \leq (\bar{F} : F)$

inequality

(= for Galois (normal + separable))

Example: $H = \{1, \beta\}$ $\quad \mathbb{C} \supset \beta$ complex conj

$\mathbb{R} = \mathbb{C}^H \qquad z \mapsto \bar{z}$

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

$f(x) = (x - \alpha)(x - \bar{\alpha}) =$

$= x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$

real coefficients

$\alpha + \bar{\alpha} = 2a$

$\alpha\bar{\alpha} = a^2 + b^2$

$\tau(x) = x$

Remark: Can use primitive element theorem ($\forall$ finite separable extension)

E/E^H is generated by some $\alpha \in E$, $E = E^H(\alpha)$.

$\Rightarrow \deg(E/E^H) = [E : E^H] \leq |H| \Rightarrow [E : E^H] = |H|$

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

Corollary E/F Galois, $H \subset Gal(E/F) \Rightarrow [E : E^H] = |H|$.

(In fact, true for $\forall E$, $H \subset Aut(F)$ finite group, don't need F. Rotman Thm 7.9 p. 78)

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

$|G| = [E:F]$

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

$K \rightsquigarrow H = Gal(E/K) \subset G \rightsquigarrow E^H$ ← everything fixed by H., $K \subset E^H$

(sub-field)

E/K is Galois too $\Rightarrow [E:K] = |H|$. By corollary $[E:E^H] = |H| \Rightarrow$

$K = E^H$:

subfield $K \rightsquigarrow$ subgroup $H = Gal(E/K) \rightsquigarrow$ subfield $E^H = K$ back to K

Subgroup $H \subset G \rightsquigarrow$ subfield $K = E^H \rightsquigarrow Gal(E/K) \supset H$

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

$[E:E^H] = |H|$ $\Rightarrow$ back to H.

Thm (Main Thm of Galois Theory) For a Galois extension $F \subset E$

1) There is a bijection

subfields K, $F \subset K \subset E$ $\quad\Longleftrightarrow\quad$ subgroups $H \subset G = Gal(E/F)$

$K \longmapsto H = Gal(E/K)$

$E^H \longleftarrow H$

2) This bijection is order-reversing

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

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

$\forall H \subset G \quad [E : E^H] = |H|$, $[E^H : F] = (G : H)$ index

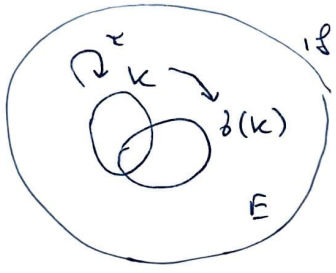
3) $$|\mathrm{Gal}(E/k)| = [E:k] = \frac{[E:F]}{[k:F]}$$

4) For $F \subset k \subset E$, k is a normal extension of F iff $H \lhd G$.

$\mathrm{Gal}(E/k) \subset \mathrm{Gal}(E/F)$ is a normal subgroup. Then
H $\quad$ G

k/F is Galois and $\mathrm{Gal}(k/F) = \mathrm{Gal}(E/F)/\mathrm{Gal}(E/k)$.

For 4: if k is not normal, $\sigma(k) \neq k$ for some σ



if $\tau \in \mathrm{Gal}(E/k)$, $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(E/\sigma(k))$.

$$\mathrm{Gal}(E/\sigma(k)) = \sigma\,\mathrm{Gal}(E/k)\,\sigma^{-1}.$$

Conjugate subgroups

$\sigma H \sigma^{-1} = H \ \forall \sigma \in G \iff H \lhd G$ normal $\iff k/F$ is normal.

Example 1) $F=\mathbb{Q}$ $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$ $G=Gal(E/\mathbb{Q})$

$(x^2-2)(x^2-3)$

$\sqrt{2} \to -\sqrt{2}$ $\quad \sqrt{3} \to -\sqrt{3}$

σ_1 fixes $\sqrt{3}, -\sqrt{3}$ $\quad \sigma_2$ fixes $\pm\sqrt{2}$

$G \cong C_2 \times C_2$ klein V_4 group.

G

5 subgroups $\langle\sigma_1\rangle$ $\langle\sigma_2\rangle$ $\langle\sigma_1\sigma_2\rangle$

$\sigma_1\sigma_2$: fixes $\sqrt{6}$.

H is one of $\mathbb{R} \times 5$ $\quad \{1\}$.

$E = E^{\{1\}}$

Subfields

E

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

$\mathbb{Q}$

$\mathbb{Q}(\sqrt{2}) = E^{\langle\sigma_2\rangle}$ $\quad \mathbb{Q}(\sqrt{6}) = E^{\langle\sigma_1\sigma_2\rangle}$

$\mathbb{Q}(\sqrt{3}) = E^{\langle\sigma_1\rangle}$

$\mathbb{Q} = E^{C_2 \times C_2}$

No other subfields!

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ basis in E

Corollary: any $\alpha = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, $\alpha \notin \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$

generates E

$E = \mathbb{Q}(\alpha)$

simple extension.

$\text{irr}(\alpha, \mathbb{Q})$ has degree 4. Get lots of irreps, f.

E is a splitting field of any of these irreps.

$f(x)$ has 4 roots in E.

Often easier to build E using intermediate fields.

$\alpha = \sqrt{2}+\sqrt{3}$ root of $x^4-10x+1$ ← 4 roots

$\alpha = \beta_1 = \sqrt{2}+\sqrt{3}$, $\beta_2 = -\sqrt{2}+\sqrt{3}$, $\beta_3 = \sqrt{2}-\sqrt{3}$, $\beta_4 = -\sqrt{2}-\sqrt{3}$.

Then $\sigma_1 : \beta_1 \leftrightarrow \beta_2$, $\beta_3 \leftrightarrow \beta_4$. , $\sigma_2 : \beta_1 \leftrightarrow \beta_3$, $\beta_2 \leftrightarrow \beta_4$. , $\sigma_3 : \beta_1 \leftrightarrow \beta_4$, $\beta_2 \leftrightarrow \beta_3$.

$\sigma_1 : (12)(34)$ $\quad \sigma_2 : (13)(24)$ $\quad \sigma_3 : (14)(23)$

β_1
$4 \leftrightarrow 3$
$\beta_2 \updownarrow \quad \updownarrow \sigma_2$
$1 \leftrightarrow 2$
β_3

this is a different embedding of $C_2 \times C_2 \subset S_4$.

$E^{\langle\sigma_1\rangle}$: $\beta_1+\beta_2$, σ_1-invariant $\quad E^{\langle\sigma_2\rangle}$ $\quad \beta_1+\beta_3 = 2\sqrt{2}$

$= 2\sqrt{3}$

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

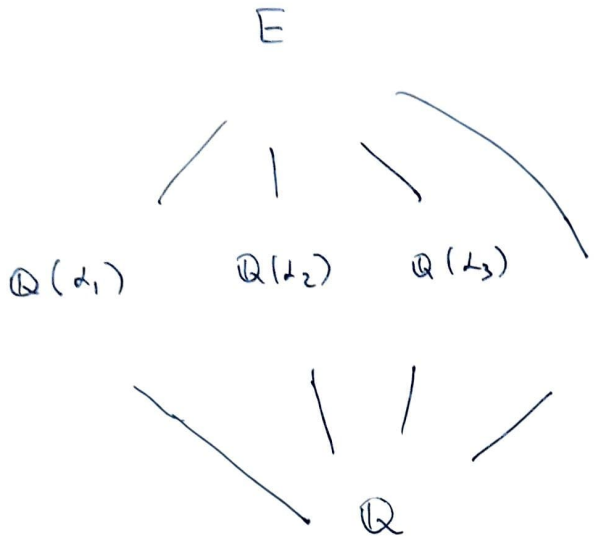
σ_3: $\beta_1+\beta_4 = 0$ does not help $\quad \sigma_3(\beta_1) = -\beta_1 \Rightarrow \sigma_3(\beta_1^2) = \beta_1^2 = 5+2\sqrt{6}$. $\Rightarrow E^{\langle\sigma_3\rangle} = \mathbb{Q}(\sqrt{6})$.

$E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ splitting field of $x^3 - 2$ $\quad \omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$

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

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

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



$G = Gal(E/\mathbb{Q}) \simeq S_3$

α_3 all permutations

$\alpha_1 \quad \alpha_2$

$Gal(E/\mathbb{Q}(\alpha_1)) = \{1, (23)\}$, $Gal(E/\mathbb{Q}(\alpha_2)) = \{1, (13)\}$,

$Gal(E/E) = \{1\}$ $\quad Gal(E/\mathbb{Q}) = S_3$

$Gal(E/\mathbb{Q}(\omega)) = A_3$ - even permutations

which are normal ?

field K	$H = Gal(E/K)$	$\lvert H\rvert = [E:K]$	$[K:F] = (G:H)$ (index)	Normal ?
$\mathbb{Q}$	S_3	6	1	Yes
$\mathbb{Q}(\alpha_1)$	$\{1, (23)\}$	2	3	No
$\mathbb{Q}(\alpha_2)$				
$\mathbb{Q}(\alpha_3)$				
$\mathbb{Q}(\omega)$				
E				

complete the table

what would change if we use polynomial $x^3 - 5$? $x^3 - 7$?

$E = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ 3 primes. $f = (x^2-p_1)(x^2-p_2)(x^2-p_3)$ splitting field

$\sqrt{p_3} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$.

$\Rightarrow [E:\mathbb{Q}] = 8$.

know all subfields of $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$

$\mathbb{Q}(\sqrt{p_3})$ is not one of them

$\pm\sqrt{p_1}, \pm\sqrt{p_2}, \pm\sqrt{p_3}$ roots of f $\quad G = \mathrm{Gal}(E/\mathbb{Q})$ $\quad |G| = 8$.

$\Rightarrow G = C_2 \times C_2 \times C_2$ abelian.

subgroups $\longleftrightarrow$ subfields.

7 subgroups of index 2 (order 2) $\longleftrightarrow$ 7 subfields of degree 2

7 subgroups of index 4 (order 2) $\longleftrightarrow$ 7 subfields of deg 4

$\mathbb{Q}(\sqrt{p_1})$, $\mathbb{Q}(\sqrt{p_2})$, $\mathbb{Q}(\sqrt{p_3})$, $\mathbb{Q}(\sqrt{p_1p_2})$, $\mathbb{Q}(\sqrt{p_1p_3})$, $\mathbb{Q}(\sqrt{p_2p_3})$, $\mathbb{Q}(\sqrt{p_1p_2p_3})$.

$H \subset C_2 \times C_2 \times C_2$ $\quad |H| = 4$, $\quad H \simeq C_2 \times C_2$, H kernel of hom. $\varphi: G \to C_2$

$\parallel$

G

8 homomorphisms

7 have kernel of order 4.

(surjective homomorphisms)