

Midterm almost graded

Rest of h/w 5 will be posted soon

Today: characterize Galois ext's, and fund. thm. of Galois theory

Thm 13:  $K/F$  Galois  $\Leftrightarrow K$  is the splitting field of some sep. poly /  $F$ .

Pf:  $\Leftarrow$ : Prop 5.

$\Rightarrow$ : Let  $G = \text{Gal}(K/F)$ ,  $p(x) \in F[x]$  irred,  $\alpha \in K$  root of  $p$ .

Let  $\alpha_1, \dots, \alpha_r$  (rsh) denote the Galois conjugates of  $\alpha$ .

Since elts. of  $G$  are automorphisms,  $\alpha_1, \dots, \alpha_r$  are roots of  $p$ .

Let

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r) \in K[x] \quad (f(x) | p(x))$$

$$f(x) \in (\text{Fix } G)[x] = F[x] \quad \text{since elts. of } G \text{ permute the roots of } f. \\ \text{(Cor. 10)}$$

permute the roots of  $f$ .

Since  $p$  irred,  $f = p$ , so  $p$ : sep., splits in  $K$

Just need to find a poly. for which  $K$  is the splitting field

Let  $w_1, \dots, w_n$  be a basis for  $K/F$ .

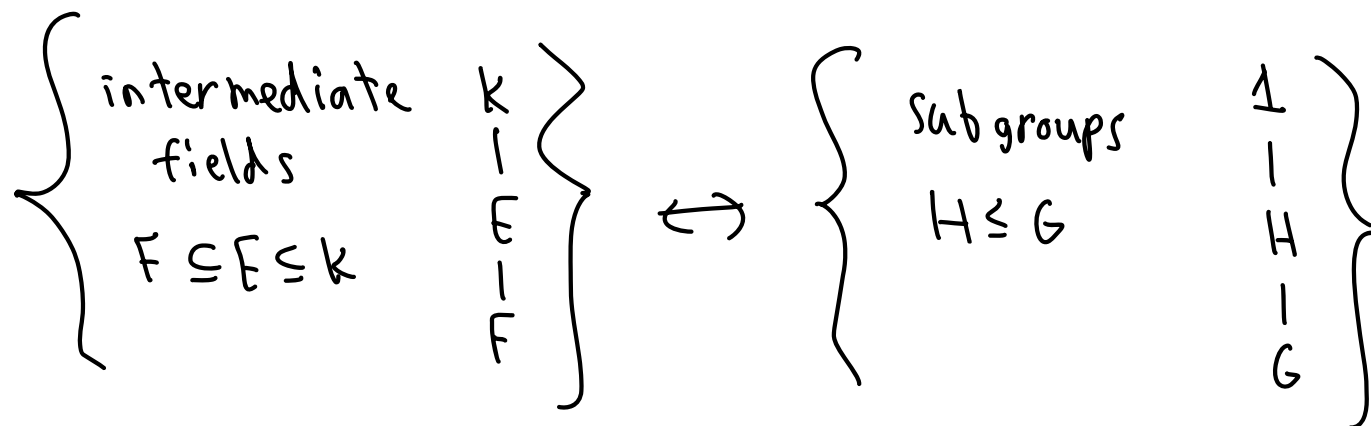
$$P_i := m_{w_i, F}(x)$$

$\prod P_i$  has splitting field  $K$ , removing duplicates gives a sep. poly. whose splitting field is  $K$ .

Cor:  $K/F$  Galois  $\Rightarrow$  every irred. poly in  $F[x]$  w/ a root in  $K$  is sep & splits over  $K$

Thm 14: Fundamental Theorem of Galois Theory:

$K/F$ : Galois ext'n,  $G := \text{Gal}(K/F)$ .  $\exists$  bijection



given by

$$E \longmapsto \text{Aut}(K/E)$$

$$\text{Fix } H \longleftarrow H$$

"Galois correspondence".

It has the following properties ( $E \leftrightarrow H, E_1 \leftrightarrow H_1, E_2 \leftrightarrow H_2$ )

(1) (Inclusion reversal):  $E_1 \subseteq E_2 \Leftrightarrow H_1 \supseteq H_2$

(2)  $[K:E] = |H|, [E:F] = |G:H|$

$K$	}	$ H $
$E$		
$F$	}	$ G:H $
$F$		

(3)  $K/E$  is Galois,  $\text{Gal}(K/E) = H$

(4)  $E/F$  is Galois  $\Leftrightarrow H \trianglelefteq G$ .

In this case,  $\text{Gal}(E/F) \cong G/H$

(5)  $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$

$E_1 E_2 \leftrightarrow H_1 \cap H_2$

Pf: Cor 11:  $\text{Aut}(K/\text{Fix } H) = H$

Thm 13  $\Rightarrow K/E$  is Galois, so Cor 10  $\Rightarrow \text{Fix } \text{Aut}(K/E) = E$

Since applying the maps in either order gives the identity, they are inverse bijections

Prop 4  $\Rightarrow$  (1)

(3) follows from above reasoning

(3) & Tower law  $\Rightarrow$  (2)

(5)  $e \in E_1 \cap E_2 \Rightarrow e$  fixed by  $H_1 \cup H_2 \Rightarrow e$  fixed by  $\langle H_1, H_2 \rangle$

$h \in \langle H_1, H_2 \rangle \Rightarrow h = h_1 h_2 \dots h_n$ ,  $h_i \in H_1$  or  $h_i \in H_2$

each  $h_i$  fixes  $E_1 \cap E_2$  so  $h$  fixes  $E_1 \cap E_2$

$E_1, E_2 \cap H_1 \wedge H_2$  similar (see D & F)

(4) Let  $\text{Emb}(E/F) = \left\{ \tau: E \xrightarrow[\text{inj.}]{} K \mid \tau(f) = f, f \in F \right\}$

We'll show that  $|\text{Emb}(E/F)| = [E:F] \stackrel{(2)}{=} [G:H]$

If  $\sigma \in \text{Gal}(K/F)$ ,  $\sigma|_E \in \text{Emb}(E/F)$

If  $\tau \in \text{Emb}(E/F)$ ,  $K$  is a splitting field

for  $\tau(E)$ , so Thm 13.27:  $\sigma: K \xrightarrow{\sim} K \in G$

$$\begin{array}{ccc} & | & | \\ & \tau & \sigma|_E \end{array}$$

If  $\sigma, \sigma' \in G$ , then  $\sigma|_E = \sigma'|_E \Leftrightarrow$

$$\sigma^{-1}\sigma' \in H (= \text{Fix } E) \Leftrightarrow \sigma H = \sigma' H$$

$$\text{So } |\text{Emb}(E/F)| = [G:H] = [E:F].$$

Now,  $E/F$  Galois  $\Leftrightarrow |\text{Aut}(E/F)| = [E:F] = |\text{Emb}(E/F)|$

$$\Leftrightarrow E = \sigma(E) \text{ for all } \sigma \in G.$$

$$\Leftrightarrow H = \sigma H \sigma^{-1} \text{ for all } \sigma \in G \text{ (since } \sigma(E) \Leftrightarrow \sigma H \sigma^{-1})$$

$$\Leftrightarrow H \trianglelefteq G$$

When this happens,  $G/H \cong \text{Gal}(E/F)$  since  
 $G/H$  inherits its gp. structure from  $G$

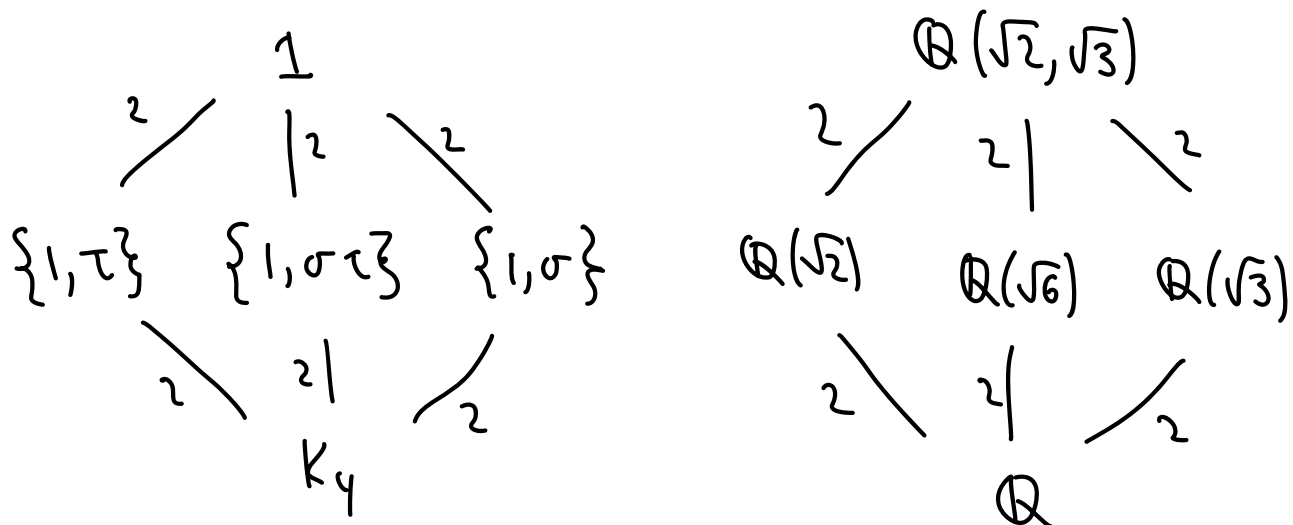
---

Examples:

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

$$\text{Let } \sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Then  $G = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong K_4$   
 Klein 4



$$\text{Fix} \{1, \tau\} = \mathbb{Q}(\sqrt{2})$$

$$\text{Fix} \{1, \sigma\} = \mathbb{Q}(\sqrt{3})$$

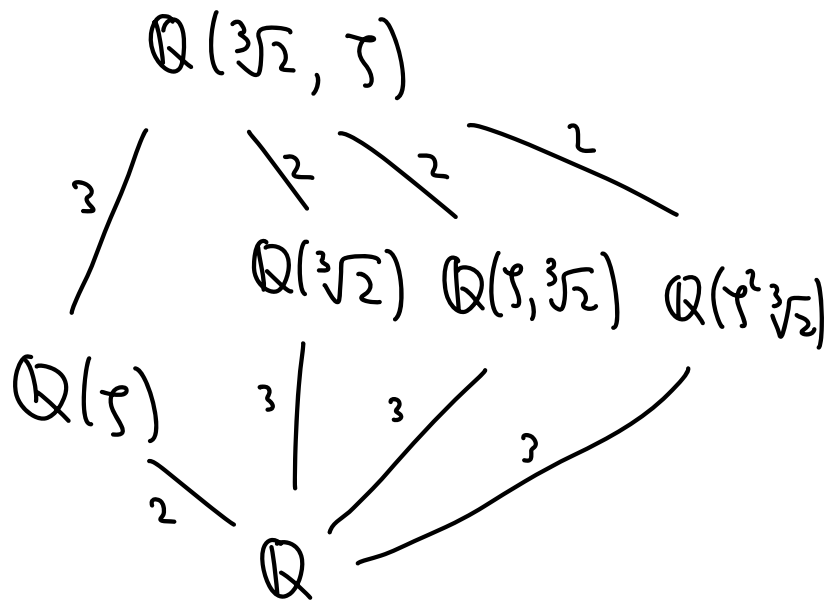
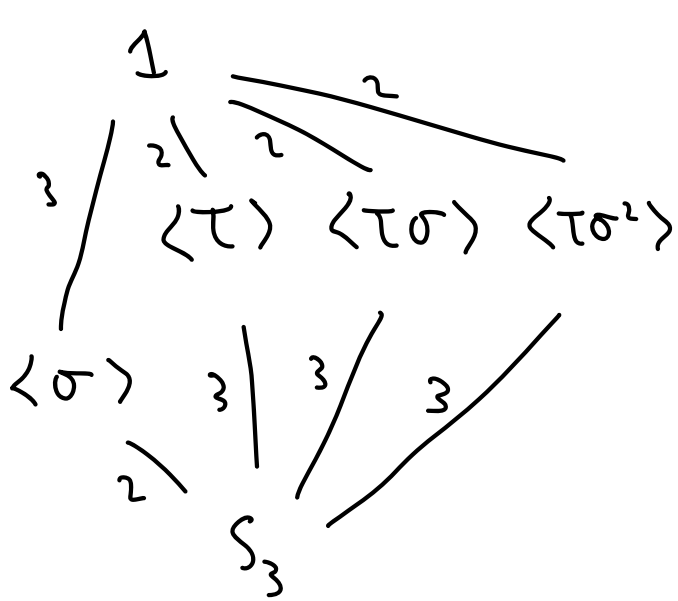
$$\text{Fix} \{1, \sigma\tau\} = \mathbb{Q}(\sqrt{6})$$

2)  $\mathbb{Q}(\sqrt[3]{2}, \wp)/\mathbb{Q}$ ,  $\wp = \wp_3$

$$\sigma: \begin{cases} \sqrt[3]{2} \mapsto \wp \sqrt[3]{2} \\ \wp \mapsto \wp \end{cases}$$

$$\tau: \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \wp \mapsto \wp^2 = -1 - \wp \end{cases}$$

$$G = \langle \sigma, \tau \rangle \cong S_3$$



$$\text{Fix } \langle \tau \sigma \rangle = \text{Fix} \begin{cases} \sqrt[3]{2} \mapsto \tau^2 \sqrt[3]{2} \\ \tau \mapsto \tau^2 \end{cases} = \mathbb{Q}(\tau \sqrt[3]{2})$$

Since  $\tau \sqrt[3]{2} \mapsto \tau^2 \sqrt[3]{2} \cdot \tau^2 = \tau \sqrt[3]{2}$

Which ext'ns are Galois?

$\mathbb{Q}(\sqrt[3]{2}, \tau) / E$  for any  $E$  above

$\mathbb{Q}(\tau) / \mathbb{Q}$  since  $\langle \sigma \rangle$  is a normal subgrp.  
(index 2)

None of the others, since not normal subgps.

e.g.  $\sigma \tau \sigma^{-1} = \tau \sigma \notin \langle \tau \rangle$