

Today: Thm: Let  $G \subseteq \text{Aut}(K)$ ,  $F = \text{Fix } G$   
 $\uparrow$   $\uparrow$   
 finite any  
 gp. field

Then  $K/F$  is Galois!

More precisely,

$$[K : \text{Fix } G] = |G| \text{ and } \text{Aut}(K / \text{Fix } G) = G$$

Recall:

- Primitive Elt. Thm.: Every finite, separable ext'n is simple.  
 (proved for char 0 and finite fields)
- If  $K/F$  field ext'n w/  $F = \text{Fix } G$ , then

$$m_{\alpha, F}(x) = \prod_{\beta \in G\alpha} (x - \beta)$$

Pf of thm when  $\text{char } K = 0$  or  $K$ : finite.

If  $\alpha \in K$ , then  $m_{\alpha, F}(x) = \prod_{\beta \in G\alpha} (x - \beta)$ , so

$$[K : F] = [F(\alpha) : F] = \deg m_{\alpha, F} = |G\alpha| \leq |G|.$$

Now, if  $\alpha$  is a prim. elt. for  $k/F$  i.e.  $k = F(\alpha)$ , then we have

$$|G| \underset{(c)}{\leq} |\text{Aut}(k/F)| \underset{(a)}{\leq} [k:F] \underset{(b)}{\leq} |G|.$$

Therefore, these are all equalities and so

(a)  $k/F$  is Galois

(b)  $[k:F] = |G|$

(c)  $\text{Gal}(k/F) = G$

□

Cor: If  $G_1 \neq G_2$  are finite subgps. of  $\text{Aut}(k)$ , then  $\text{Fix } G_1 \neq \text{Fix } G_2$ .

Pf: By the theorem,

$$G_i = \text{Aut}(k/\text{Fix } G_i).$$

□

Recall:  $K/F$  Galois means  $[K:F] = |\text{Aut}(K/F)|$

Thm:  $K/F$  finite extn. The following are equivalent.

a)  $K/F$  is Galois

b)  $K$  is the splitting field of a sep. poly. in  $F[x]$

c)  $\text{Fix}(\underbrace{\text{Aut}(K/F)}_G) = F$

Pf:

b)  $\Rightarrow$  a) Proved in Lecture 22

a)  $\Rightarrow$  c): Let  $G := \text{Gal}(K/F)$ . Then  $F \subseteq \text{Fix } G \subseteq K$ , and by the first thm. today,  $[K:\text{Fix } G] = |G| = [K:F]$ , so  $F = \text{Fix } G$ .

c)  $\Rightarrow$  b): (We'll prove in the case of simple extns, including Char 0 & finite fields). If  $K = F(\alpha)$ , then since  $F = \text{Fix } G$ ,

$$m_{\alpha, F}(x) = m_{\alpha, \text{Fix } G}(x) = \prod_{\beta \in G\alpha} (x - \beta). \text{ This is a sep.}$$

poly. whose splitting field over  $F$  is  $K$ .  $\square$

Fundamental Thm. of Galois Theory:  $K/F$  Galois,  $G := \text{Gal}(K/F)$ .

There exists a bijection

$$\left\{ \begin{array}{l} \text{Intermediate} \\ \text{fields} \end{array} \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{subgps.} \\ 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

$$\begin{array}{ccc} E & \xrightarrow{\quad} & \text{Aut}(K/E) \\ \text{Fix } H & \xleftarrow{\quad} & H \end{array}$$

Properties:  $(E \leftrightarrow H, E_1 \leftrightarrow H_1, E_2 \leftrightarrow H_2)$

$$1) E_1 \subseteq E_2 \iff H_1 \supseteq H_2$$

$$2) [K:E] = |H| \text{ and } [E:F] = \underbrace{|G:H|}_{\text{index}}$$

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

$$4) E/F \text{ is Galois } \iff H \trianglelefteq G$$

↙ normal subgp.

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

$$5) E_1 \cap E_2 \leftrightarrow \underbrace{\langle H_1, H_2 \rangle}_{\text{subgp. of } G} \text{ and } E_1 E_2 \leftrightarrow H_1 \cap H_2$$

gen'd by  $H_1, H_2$

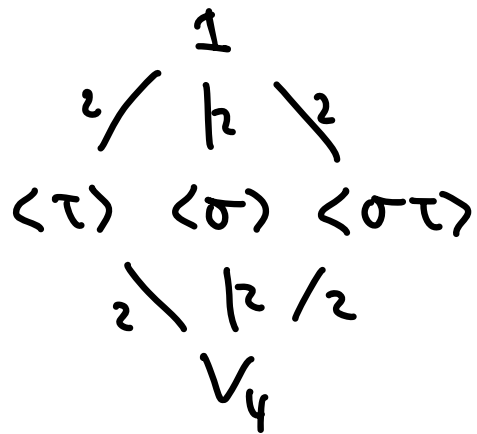
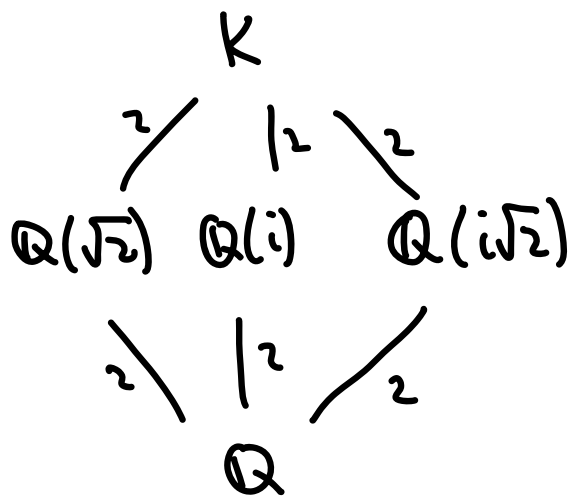
Examples:

a)  $K = \mathbb{Q}(\sqrt{2}, i) =$  splitting field for  $(x^2 - 2)(x^2 + 1)$

$K/\mathbb{Q}$  is Galois,  $\text{Gal}(K/\mathbb{Q}) = \langle \tau, \sigma \rangle \cong V_4$  (Klein 4-grp.)

$\tau: i \mapsto -i, \sqrt{2} \mapsto \sqrt{2}$

$\sigma: \sqrt{2} \mapsto -\sqrt{2}, i \mapsto i$



Since  $V_4$  is abelian, every subext'n is Galois

b)  $K = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha}, \underbrace{\zeta_3}_{\zeta}) = \text{splitting field of } x^3 - 2 \in \mathbb{Q}[x]$   
 $\beta = \zeta\alpha, \gamma = \zeta^2\alpha$

$\text{Gal}(K/\mathbb{Q}) \cong S_3$  (all permutations of  $\alpha, \beta, \gamma$ )

$\cong \langle \sigma, \tau \rangle$  where

$$\begin{aligned} \downarrow: \alpha &\mapsto \alpha \\ &\zeta \mapsto \zeta \end{aligned}$$

$$\begin{aligned} \tau: \alpha &\mapsto \alpha \\ &\zeta \mapsto \zeta^2 \end{aligned}$$

$$\begin{aligned} \sigma: \alpha &\mapsto \zeta\alpha \\ &\zeta \mapsto \zeta \end{aligned}$$

$$\begin{aligned} \sigma\tau = \tau\sigma^2: \alpha &\mapsto \zeta^2\alpha \\ &\zeta \mapsto \zeta^2 \end{aligned}$$

$$\begin{aligned} \sigma^2: \alpha &\mapsto \zeta^2\alpha \\ &\zeta \mapsto \zeta \end{aligned}$$

$$\begin{aligned} \sigma^2\tau = \tau\sigma: \alpha &\mapsto \zeta\alpha \\ &\zeta \mapsto \zeta^2 \end{aligned}$$

