

## Announcements:

Midterm 2 graded

Q1: 81%

Median 49/75

Q2: 79%

Mean: 50.3/75

Q3: 50%

Std. dev: 10.6

Q4: 56%

Gradelines: A-/A: 53 to 75 (out of 75)

B+/B/B-: 32 to 53 - E

C+/C/C-: 15 to 32 - E

D+/D/D-: 4 to 15 - E

Sol's posted to website

"Where do I stand" spreadsheet updated

Remarks:

a) Splitting field of any poly. over perfect field is Galois

b) Be careful trying to do "complex number things"  
over fields of char  $p$

Thm A: Let  $G \subseteq \text{Aut}(K)$ ,  $F = \text{Fix } G$

$\nwarrow$                        $\nwarrow$   
 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

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

Now, if  $\alpha$  is a prim. elt. for  $K/F$  i.e.  $K = F(\alpha)$ ,<sup>\*</sup> 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 Thm A,  $G_i = \text{Aut}(K/\text{Fix } G_i)$ . □

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

Thm B:  $K/F$  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" (by example) in Lecture 22

$a) \Rightarrow c)$ : Let  $G := \text{Gal}(k/F)$ . Then  $F \subseteq \text{Fix } G \subseteq k$ , and by Theorem A,  $[k:\text{Fix } G] = |G| = [k:F]$ , so  $F = \text{Fix } G$ .

$c) \Rightarrow b)$ : (We'll prove in the case of simple ext'ns, including  $\text{Char } 0$  & 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  $k$ .  $\square$

Cor: If  $k/F$  is a Galois ext'n and  $f \in F[x]$  is irred. in  $F[x]$  and has a root  $\alpha \in k$ , then  $f$  splits in  $k$ .

Pf: Let  $G = \text{Gal}(k/F)$ . Then  $\text{Fix } G = F$ , so

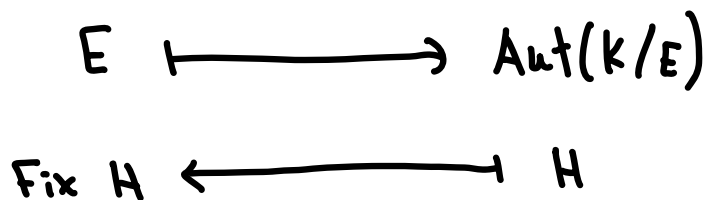
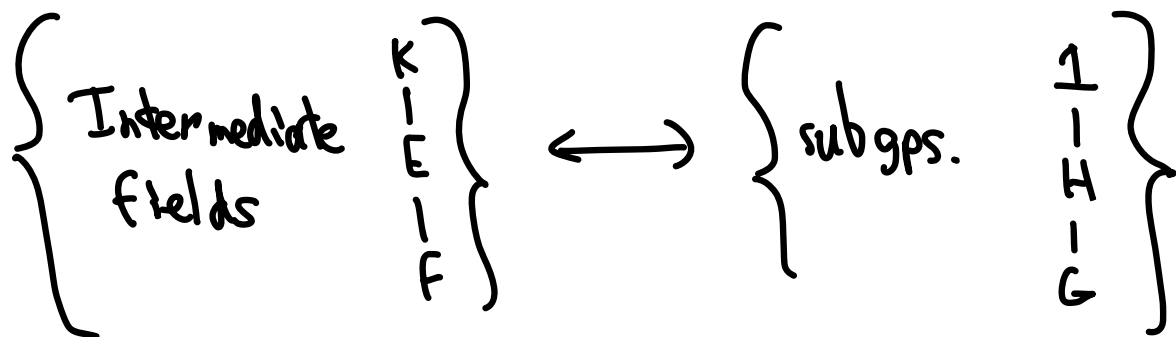
$$f(x) = m_{\alpha, F}(x) = \prod_{\beta \in G\alpha} (x - \beta),$$

and since  $\alpha \in k$ ,  $G \subseteq \text{Aut}(k)$ , each of the other roots  $\beta$  of  $f$  is in  $k$ , so  $f$  splits completely over  $k$ .

$\square$

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

There exists a bijection



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

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

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

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

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

↙ normal subgp.

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

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

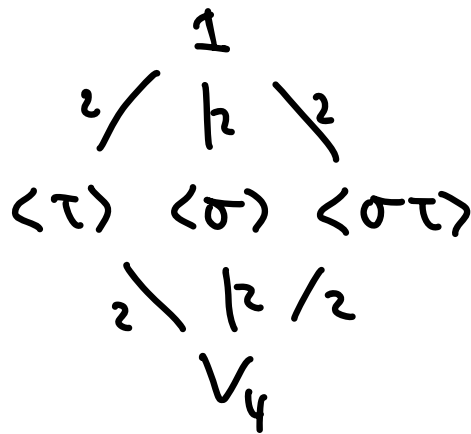
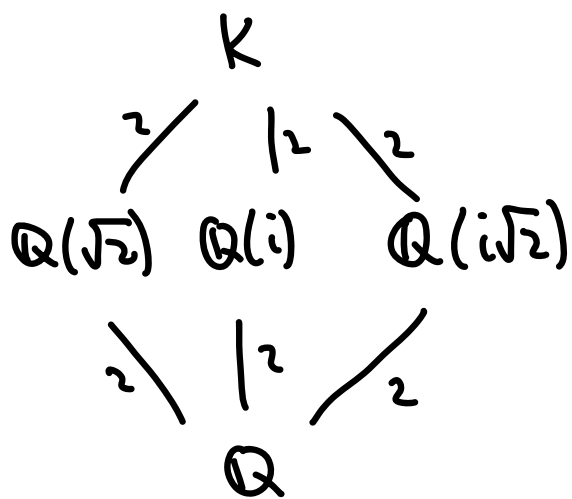
Examples:

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.)  
 $(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$

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

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



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

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

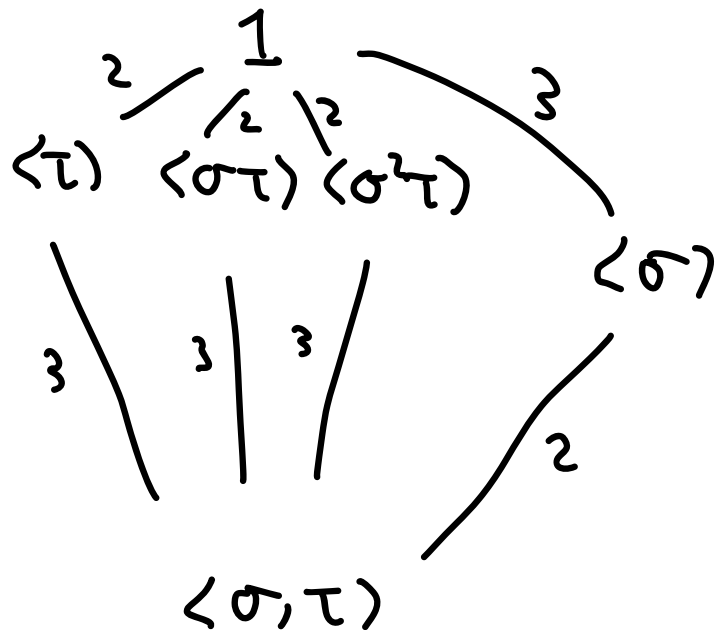
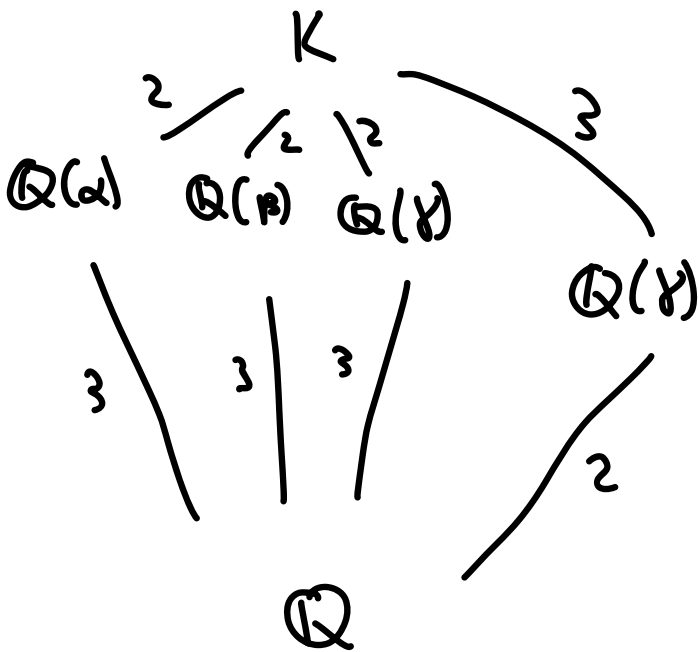
$$\begin{aligned} \tau: \alpha &\mapsto \alpha \\ \zeta &\mapsto \zeta^2 \end{aligned}$$

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

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

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

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



\* Note: You may worry whether  $K/F$  can be infinite. But by the previous line, every elt. of  $K$  is alg. over  $F$  of  $\text{deg} \leq n$ . So if  $[K:F] = \infty$ , we must have  $[F(\alpha_1, \dots, \alpha_k):F] > |G|$  for some elts.  $\alpha_1, \dots, \alpha_k \in K$ . But by the primitive elt. thm,  $F(\alpha_1, \dots, \alpha_k) = F(\gamma)$  for some  $\gamma \in K$ , contradicting  $[F(\gamma):F] \leq |G|$ .