

Announcements:

Midterm 2 graded

Median 49/75

Mean: 50.3/75

Std. dev: 10.6

Q1: 81%

Q2: 79%

Q3: 50%

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

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

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

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

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

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 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 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 . □

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

There exists a bijection

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

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

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

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

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

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

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

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

\hookleftarrow normal subgp.

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

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

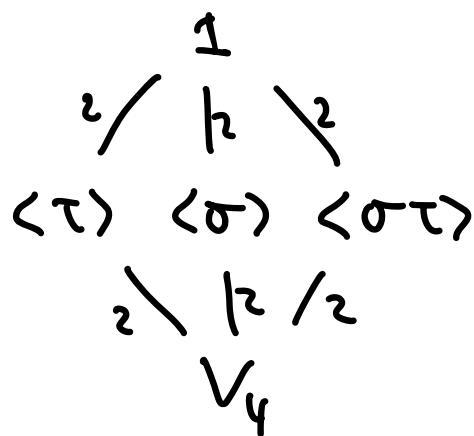
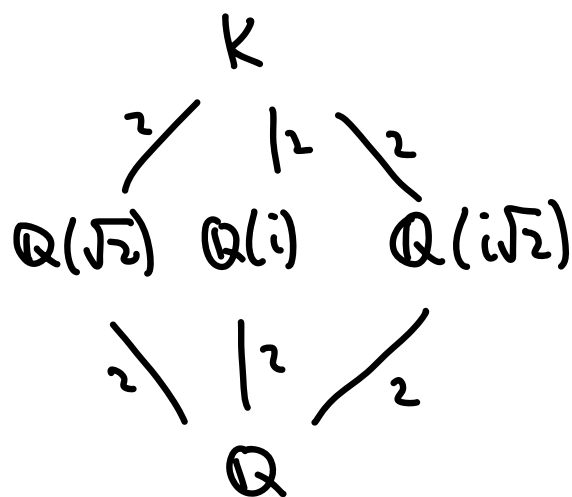
Examples:

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

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

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

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



Since V_4 is abelian, every subextn is Galois

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

$\text{Gal}(K/\mathbb{Q}) \cong S_3$ (all permutations of α, β, γ)

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

$1: \alpha \mapsto \alpha$
 $\beta \mapsto \beta$

$\tau: \alpha \mapsto \alpha$
 $\beta \mapsto \beta^2$

$\sigma: \alpha \mapsto \beta\alpha$
 $\beta \mapsto \beta$

$\sigma\tau = \tau\sigma^2: \alpha \mapsto \beta^2\alpha$
 $\beta \mapsto \beta^2$

$\sigma^2: \alpha \mapsto \beta^2\alpha$
 $\beta \mapsto \beta$

$\sigma^2\tau = \tau\sigma: \alpha \mapsto \beta\alpha$
 $\beta \mapsto \beta^2$

