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 $-\varepsilon$

C+/C/C-: 15 to 32 $-\varepsilon$

D+/D/D-: 4 to 15 $-\varepsilon$

Sol'ns posted to website

"Where do I stand" spreadsheet updated

Remarks:

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

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

Thm A: Let $G \leq Aut(K)$, $F = Fix\ G$
finite gp. — any field

Then K/F is Galois!

More precisely,

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

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/ $F = Fix\ G$, then

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

Pf of thm when 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 α is a prim. elt. for K/F i.e. $K = F(\alpha)$,* then we have

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

Therefore, these are all equalities and so

(a) K/F is Galois

(b) $[K:F] = G$

(c) $\mathrm{Gal}(K/F) = G$ $\square$

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

Pf: By Thm A, $G_i = \mathrm{Aut}(K/\mathrm{Fix}\, G_i)$. $\square$

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

Thm B: K/F finite ext'n. The following are equivalent.

a) K/F is Galois

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

c) $\mathrm{Fix}(\underbrace{\mathrm{Aut}(K/F)}_{G}) = F$

Pf: b) $\Rightarrow$ a) "Proved" (by example) in Lecture 22

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

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

$$m_{\alpha,F}(x) = m_{\alpha, \mathrm{Fix}\, G}(x) = \prod_{\beta \in G\alpha} (x - \beta).$$ 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 $G = \mathrm{Gal}(K/F)$. Then $\mathrm{Fix}\, G = F$, so

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

and since $\alpha \in K$, $G \leq \mathrm{Aut}(K)$, each of the other roots β of f is in K, so f splits completely over K.

$\square$

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

There exists a bijection

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

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

$$\mathrm{Fix}\, H \longleftarrow H$$

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

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

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

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

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

normal subgp.

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

5) $E_1 \cap E_2 \leftrightarrow \underbrace{\langle H_1, H_2 \rangle}_{\substack{\text{subgp. of } G \\ \text{gen'd by } H_1, H_2}}$ 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, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau, \sigma \rangle \cong V_4$ $\begin{pmatrix} \text{Klein 4-gp.} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \end{pmatrix}$

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

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

$$\begin{tikzcd}
& K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(i) \arrow[d, dash, "2"] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle \tau \rangle \arrow[dr, dash, "2"'] & \langle \sigma \rangle \arrow[d, dash, "2"] & \langle \sigma\tau \rangle \arrow[dl, dash, "2"] \\
& V_4 &
\end{tikzcd}$$

Since V_4 is abelian, every subext'n is Galois

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

$\beta = \zeta\alpha, \quad \gamma = \zeta^2\alpha$

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

$\quad = \langle \sigma, \tau \rangle$ where

$1: \alpha \mapsto \alpha$, $\zeta \mapsto \zeta$

$\tau: \alpha \mapsto \alpha$, $\zeta \mapsto \zeta^2$

$\sigma: \alpha \mapsto \zeta\alpha$, $\zeta \mapsto \zeta$

$\sigma\tau = \tau\sigma^2: \alpha \mapsto \zeta^2\alpha$, $\zeta \mapsto \zeta^2$

$\sigma^2: \alpha \mapsto \zeta^2\alpha$, $\zeta \mapsto \zeta$

$\sigma^2\tau = \tau\sigma: \alpha \mapsto \zeta\alpha$, $\zeta \mapsto \zeta^2$

$$\begin{tikzcd}
 & & K \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\alpha) \arrow[drr, dash, "3"'] & \mathbb{Q}(\beta) \arrow[dr, dash, "3"] & \mathbb{Q}(\gamma) \arrow[d, dash, "3"] & \mathbb{Q}(\gamma) \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & 1 \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\langle \tau \rangle \arrow[drr, dash, "3"'] & \langle \sigma\tau \rangle \arrow[dr, dash, "3"] & \langle \sigma^2\tau \rangle \arrow[d, dash, "3"] & \langle \sigma \rangle \arrow[dl, dash, "2"] \\
 & & \langle \sigma, \tau \rangle &
\end{tikzcd}$$

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