Announcements

Midterm 2: Wed 3/26 7:00-8:30pm, Sidney Lu 1043

Topics: Everything through D&F §14.1 (i.e. pre-Spring break)

Practice problem sol'n sketches posted

HW7 posted (due Wed 4/2)

Office hour changes:

This week: Mon after class, Wed. before class

Next week and onwords: Mon. before class, Fri. before class

$\}$ CAB 69B

Will send email about these changes

Recall: K/F : field ext'n

$Aut(K/F) = \{$automs. of K fixing $F\}$

- $\sigma \in Aut(K/F)$ is det'd by its action on the set of generators of K/F (i.e. if $K = F(\alpha_1, \dots, \alpha_n)$ these are $\alpha_1, \dots, \alpha_n$)
- If $\alpha \in K$ is a root of $f(x) \in F[x]$, then $\sigma(\alpha)$ is also a root of f.
- If $K = Sp_f F$, $\alpha_1, \dots, \alpha_n$: roots of f in K then σ is det'd by the permutation $\bar{\sigma} = \sigma|_{\alpha_1, \dots, \alpha_n}$ i.e. $Aut(K/F) \subseteq S_n$

- If $K = Sp_f F$, f sep., then $\mathrm{Gal}(K/F) := \mathrm{Aut}(K/F)$ and K/F is <u>Galois</u>

- If $K = Sp_f F$, $|\mathrm{Aut}(K/F)| \leq [K:F]$, w/ equality iff K/F is Galois

- If $H \leq \mathrm{Aut}(K/F)$, $\mathrm{Fix}\, H = \{k \in K \mid \sigma(k) = k \ \forall h \in H\}$ is a subfield of K, and if $H \leq H' \leq \mathrm{Aut}(K)$
$F \subseteq L \subseteq K$

$$F \subseteq \mathrm{Fix}\, H' \subseteq \mathrm{Fix}\, H \subseteq K$$
$$1 = \mathrm{Aut}(K/K) \leq \mathrm{Aut}(K/L) \leq \mathrm{Aut}(K/F) \leq \mathrm{Aut}(K)$$

For the next couple of weeks, we'll focus our proofs on char 0 and/or finite fields

Def: K/F is separable if K/F is alg. and $m_{\alpha,F}(x)$ is sep. $\forall \alpha \in K$.

(If char $F = 0$ or F: finite, K/F finite $\Rightarrow$ K/F sep.)

Primitive Elt. Thm. (§13.4): Every finite, separable ext'n is simple.

E.g: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Pf in char 0: Since K/F is finite, $K = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n$. Inducting on n, suffices to consider $K = F(\alpha, \beta)$.

Let $f = m_{\alpha,F}(x)$, $g = m_{\beta,F}(x)$. Let E be a splitting field over K for fg, containing roots

$\alpha_1, \dots, \alpha_m$ of f and $\beta_1, \dots, \beta_n$ of g.

Choose $c \in F \setminus \{0\}$, and set $\gamma = \alpha + c\beta$, $L = F(\gamma)$.

$L \subseteq K$; if $K \neq L$, then $\alpha \notin L$, so $m_{\alpha,L}(x)$ has another root $\delta \neq \alpha$. Now, $m_{\alpha,L} \mid f = m_{\alpha,F}$

and also $m_{\alpha,L} \mid g\left(\frac{\gamma - x}{c}\right) =: h(x)$ since

$g(\beta) = 0$ and $\frac{\gamma - \alpha}{c} = \beta$, so $f(\delta) = h(\delta) = 0$.

The roots of h in E are

$$c = \frac{\beta - \beta_j}{\alpha_i - \alpha}$$

$$\delta_i = \gamma - c\beta_i = \alpha + c(\beta - \beta_i), \quad 1 \leq i \leq n$$

and we must have $\delta = \alpha_i = \delta_j$ for some i, j.

That is, $\alpha_i = \delta = \alpha + c(\beta - \beta_j)$. Since $\delta \neq \alpha$, this means that

$\beta \neq \beta_j$, so $c = \frac{\alpha_i - \alpha}{\beta - \beta_j}$. There are only finitely many such choices for c, and F is infinite, so there exists some $c \in K$ not of this form, and $K = F(\alpha + c\beta)$, so K/F is simple. $\square$