Announcements

Midterm 2: Thurs. 3/21 7:00-8:30pm, Loomis Lab. 144

See policy email (reference sheet allowed)

Topics: Everything through D&F §14.1
but focus is on post-Midterm 1 material (§13.2-onwards)

Practice problems: see email

Tues., Wed.: review

Recall: K/F : field ext'n

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

- $\sigma \in \mathrm{Aut}(K/F)$ 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 $K = \mathrm{Sp}_f F$, $\alpha_1, \dots, \alpha_n$: roots of f in K
then σ is det'd by the permutation $\overline{\sigma} = \sigma|_{\alpha_1, \dots, \alpha_n}$
i.e. $\mathrm{Aut}(K/F) \subseteq S_n$

- 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 $m_{\alpha,L} \mid g(\gamma - cx) =: h(x)$ since $g = m_{\beta,L}$ and $\gamma - c\alpha = \beta$, so $f(\delta) = h(\delta) = 0$.

The roots of h in E are

$$\delta_i = \frac{\gamma - \beta_i}{c} = \frac{c\alpha + \beta - \beta_i}{c} = \alpha + \frac{\beta - \beta_i}{c} \qquad 1 \leq i \leq n$$

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

Since $\delta \neq \alpha$, $c = \dfrac{\beta - \beta_j}{\alpha_i - \alpha}$. There are only finitely many such choices for c, and F is infinite, so

K/F is simple. $\square$

Cor: If K/F: finite, then $|\mathrm{Aut}(K/F)| \leq [K:F]$.

Pf in char 0: Let $K = F(\gamma)$, $f = m_{\gamma,F}(x)$.

Then f has $n := \deg f = [K:F]$ roots $\gamma = \gamma_1, \ldots, \gamma_n$, and $\sigma \in \mathrm{Aut}(K/F)$ is det'd by the image $\sigma(\gamma) = \gamma_i$. $\square$

Thm: Let $\underset{\substack{\uparrow \\ \text{finite gp.}}}{H} \leq \mathrm{Aut}(\underset{\substack{\uparrow \\ \text{any field}}}{K})$, $F = \mathrm{Fix}\, H$

Then K/F is Galois!

More precisely,

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

First, given $\alpha \in K$, let's construct $m_{\alpha,F} \in F[x]$.

Let

$$H\alpha := \{\sigma(\alpha) \mid \sigma \in H\} =: \{\underbrace{\alpha = \alpha_1, \ldots, \alpha_n}_{\text{distinct}}\}$$

We know that $\alpha_1, \dots, \alpha_n$ are roots of $m_{\alpha,F}$,

so set

not nec. $F[x]$

$$f(x) = \prod_{1 \le i \le n} (x - \alpha_i) \in K[x]$$

If $f(x) \in F[x]$, then $f = m_{\alpha,F}$.

Claim: This is indeed the case.

Pf: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

If $\tau \in H$, then $\tau(\alpha_i) = \tau(\sigma(\alpha)) = (\tau\sigma)(\alpha) = \alpha_j$,

so τ permutes the α_j.

Then,

$$\tau(a_n)x^n + \cdots + \tau(a_1)x + \tau(a_0)$$

$$= \tau(f(x)) = \tau\left(\prod (x - \alpha_i)\right) = \prod (x - \tau(a_i))$$

$$= \prod (x - a_i) = f(x) = a_n x^n + \cdots + a_0,$$

so $a_i \in \text{Fix } H = F$, so $f = m_{\alpha,F}$. $\square$

Ex: $K = \mathbb{Q}(\sqrt{2}, i)$, $\mathrm{Aut}(K/\mathbb{Q})$

$G := \mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ $\quad \sigma: \sqrt{2} \mapsto -\sqrt{2}$
$\quad \tau: i \mapsto -i$

Let $\alpha = i + \sqrt{2}$

$$G\alpha = \{\underbrace{\sqrt{2}+i}_{\alpha_1}, \underbrace{-\sqrt{2}+i}_{\alpha_2}, \underbrace{\sqrt{2}-i}_{\alpha_3}, \underbrace{-\sqrt{2}-i}_{\alpha_4}\}$$

and

$$m_{\alpha,\mathbb{Q}}(x) = \prod (x - \alpha_i) = x^4 - 2x^2 + 9$$