## Announcements

Friday class cancelled (start Spring break early)

Email me if you want office hours

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

See policy email (reference sheet allowed)

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

Practice problems: see email

Tues., Wed. after break: review

Conflicts: email me ASAP

HW7 (due Wed 3/27): will be posted after break

---

Recall: $K/F$ field ext'n.

$\mathrm{Aut}(K/F) = \{$automs. of $K$ which fix $F\} \leq \mathrm{Aut}(K)$

$H \leq \mathrm{Aut}(K)$

$\mathrm{Fix}\, H$ = subfield of $K$ fixed by every elt. of $H$

Thm: Let $f(x) \in F[x]$, $K = Sp_F f$. Then,

$$|\mathrm{Aut}(K/F)| \leq [K:F],$$

w/ equality if $f$ is separable.

Pf by example: (see D&F for full argument)

$f(x) = x^3 - 2 \in \mathbb{Q}[x]$

Splits as $(x - \underbrace{\sqrt[3]{2}}_{\alpha})(x - \underbrace{\zeta_3 \sqrt[3]{2}}_{\beta})(x - \underbrace{\zeta_3^2 \sqrt[3]{2}}_{\gamma})$ over $\mathbb{Q}(\alpha, \beta)$

$$\begin{array}{cc}
K = \mathbb{Q}(\alpha, \beta) & (x-\alpha)(x-\beta)(x-\gamma) \\
| & \\
L = \mathbb{Q}(\alpha) & (x-\alpha)(x^2 + \alpha x + \alpha^2) \\
| & \\
\mathbb{Q} & x^3 - 2
\end{array}$$

Build $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ in two steps

$$
\begin{tikzcd}
\mathbb{Q}(\alpha,\beta) \arrow[r, "\sim"', "\beta \mapsto \gamma"] \arrow[d, dash] & \mathbb{Q}(\beta,\gamma) = K \arrow[d, dash] \\
\mathbb{Q}(\alpha) \arrow[r, "\sim"', "\alpha \mapsto \beta"] \arrow[d, dash] & \mathbb{Q}(\beta) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "id"] & \mathbb{Q}
\end{tikzcd}
$$

adjoin root of $g(x) = x^2 + \alpha x + \alpha^2 \in \mathbb{Q}(\alpha)[x]$

adjoin root of $\sigma(g(x)) = x^2 + \beta x + \beta^2 \in \mathbb{Q}(\beta)[x]$

(Note that $x^3 - 2 = (x-\beta)\,\sigma(g(x))$

adjoin root of $f(x)$

How many such $\sigma$ can we construct?

(# choices in step 1)(# choices in step 2)

$= 3 \cdot 2 =$ (# roots of $f$)(# roots of $g$)

$= (\deg f)(\deg g) = [\mathbb{Q}(\alpha):\mathbb{Q}]\,[K:\mathbb{Q}(\alpha)]$

$f$ sep.

$= [K:\mathbb{Q}]$

$\square$

Remark: If $f(x) \in F[x]$ has roots $\alpha_1, \dots, \alpha_n$ and $K = Sp_F f$, $\sigma \in Aut(K/F)$ then the restriction

$\sigma|_{\{a_1,\dots,a_n\}}$ yields a permutation $\begin{array}{c} \alpha_1 \mapsto \alpha_{\bar{\sigma}(1)} \\ \vdots \\ \alpha_n \mapsto \alpha_{\bar{\sigma}(n)} \end{array}$

The homom. $Aut(K/F) \longrightarrow S_n$ (symmetric gp. on n letters)

$$\sigma \longmapsto \bar{\sigma}$$

is inj. (every autom. gives a different perm.)
but not necessarily surj.

Def: A finite extension $K/F$ is <u>Galois</u> if $|Aut(K/F)| = [K:F]$. In this case, we set $Gal(K/F) := Aut(K/F)$ and call it the <u>Galois group</u> of $K/F$.

Cor: If $f \in F[x]$ is sep., $K = Sp_F f$, then $K/F$ is Galois
(Turns out <u>all</u> Galois ext'ns are of this form)

Examples:

a) $\underbrace{\mathbb{Q}(\sqrt{2},i)}_{K}/\mathbb{Q}$ is Galois since

$|\mathrm{Aut}(K/\mathbb{Q})| = 4 = [K:\mathbb{Q}]$

$K = Sp_{\mathbb{Q}} f$ where $f(x) = (x^2-2)(x^2+1)$

roots: $\pm\sqrt{2}$, $\pm i$

$$\mathrm{id}: \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \\ -i \mapsto -i \end{array} \qquad \sigma: \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ i \mapsto i \\ -i \mapsto -i \end{array}$$

$$\tau: \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \\ -i \mapsto i \end{array} \qquad \sigma\tau: \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \\ -i \mapsto i \end{array}$$

Note: this is a proper subgp. of $S_4$

b) $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ $\quad L = \mathbb{Q}(\sqrt[3]{2})$ $\quad K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3 \sqrt[3]{2})$

$|\mathrm{Aut}(K/\mathbb{Q})| = 6 = [K:\mathbb{Q}]$ Galois!

$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$

$|\mathrm{Aut}(L/\mathbb{Q})| = 1 \neq 3 = [L:\mathbb{Q}]$ Not Galois

$|\mathrm{Aut}(K/L)| = 2 = [K:L]$ Galois!

$\mathrm{Gal}(K/L) \cong S_2$

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

Then $K/F$ is Galois!

More precisely,

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

Enjoy the break!