Announcements

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

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 or website

Tues., Wed. after break: review

Conflicts: email me ASAP

HW7 (due Wed 4/2): will be posted over break
but all problems are from post-midterm 2 material

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 $\mathbb{Q}(\alpha, \beta)$

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

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

using D&F Thm. 13.27

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

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 σ 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

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

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

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

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

$= \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

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

Extra examples:

a) $f(x) = \Phi_8(x) \in \mathbb{Q}[x]$

$$= (x-\zeta_8)(x-\zeta_8^3)(x-\zeta_8^5)(x-\zeta_8^7) \in \mathbb{Q}(\zeta_8)[x]$$

$K := Sp_{\mathbb{Q}} \Phi_8 = Sp_{\mathbb{Q}}(x^8-1) = \mathbb{Q}(\zeta_8)$

$K/\mathbb{Q}$ is Galois since K is a splitting field over $\mathbb{Q}$.

So $|Gal(K/\mathbb{Q})| = [K:\mathbb{Q}] = \deg \Phi_8 = 4$

$\sigma \in Gal(K/\mathbb{Q})$ is determined by $\sigma(\zeta_8)$

$id = \sigma_1 : \zeta_8 \mapsto \zeta_8$

$\sigma_3 : \zeta_8 \mapsto \zeta_8^3$

$\sigma_5 : \zeta_8 \mapsto \zeta_8^5$

$\sigma_7 : \zeta_8 \mapsto \zeta_8^7$

for other basis vectors ζ_8^k,

$$\sigma_j(\zeta_8^k) = \zeta_8^{jk}$$

So $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Do compositions, and note

$\sigma_3^2 = \sigma_5^2 = \sigma_7^2 = 1$,

So

$$Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

We will do this in more detail in a couple of weeks

b) $f(x) = x^4 - 2 \in \mathbb{Q}[x]$

$$= (x^2+\sqrt{2})(x^2-\sqrt{2}) \in \overbrace{\mathbb{Q}(\sqrt{2})}^{L}[x]$$

$$= (x+\underbrace{\sqrt[4]{2}}_{\alpha})(x-\underbrace{\sqrt[4]{2}}_{\beta})(x+\underbrace{i\sqrt[4]{2}}_{\gamma})(x-\underbrace{i\sqrt[4]{2}}_{\delta}) \in \overbrace{\mathbb{Q}(i,\sqrt[4]{2})}^{K}[x]$$

$K/\mathbb{Q}$ is Galois since K is a splitting field over $\mathbb{Q}$.

$\sigma \in Gal(K/\mathbb{Q})$ is determined by

$\sigma(\sqrt[4]{2})$ and $\sigma(i\sqrt[4]{2})$

but notice that if $\sigma(\sqrt[4]{2}) = \sigma(i\sqrt[4]{2})$,

then $\sigma(i\sqrt[4]{2})$ cannot equal $\pm i\sqrt[4]{2}$

8 automs:

$\left.\begin{array}{l} \sqrt[4]{2} \mapsto \pm\sqrt[4]{2} \\ i\sqrt[4]{2} \mapsto \pm i\sqrt[4]{2} \end{array}\right\}$ 4 choices for the $\pm$

$\left.\begin{array}{l} \sqrt[4]{2} \mapsto \pm i\sqrt[4]{2} \\ i\sqrt[4]{2} \mapsto \pm \sqrt[4]{2} \end{array}\right\}$ 4 choices for the $\pm$

The first 4 automs. fix $\mathbb{Q}(\sqrt{2})$; the last 4 do not

Field ext'n diag.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[4]{2}, i) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}$$