Announcements

Midterm 2: Wed. 3/26

7:00-8:30pm, Sidney Lu 1043

Policy email w/ practice problems coming soon

Course midterm feedback form still open

- Lecture style and pace about right
- Homework about right; a couple people want more theoretical (vs. computational) problems

---

Recall:

Def: A automorphism is a field isom. $\sigma : K \to K$

$\mathrm{Aut}(K)$ = gp. of automs. of K (under function composition)

If K/F field extn., let

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \overbrace{\underbrace{\sigma(a) = a}_{\text{"}\sigma\text{ fixes } a\text{"}} \ \forall a \in F}^{\text{"}\sigma\text{ fixes } F\text{"}}\}$$

Remark:

a) $\mathrm{Aut}(K/F) \leq \mathrm{Aut}(K)$

b) $\mathrm{Aut}\left(K/\begin{matrix}\text{prime}\\ \text{subfield}\end{matrix}\right) = \mathrm{Aut}(K)$

since every autom. fixes $\langle 1 \rangle$

E.g.: a)

$K = \mathbb{Q}(\sqrt{2}, i)$

$\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma \circ \tau\}$

where

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

$\sigma \circ \tau: \begin{matrix}\sqrt{2} \mapsto -\sqrt{2}\\ i \mapsto -i\end{matrix}$

$\underbrace{a + b\sqrt{2} + ci + di\sqrt{2}}_{[K:\mathbb{Q}]=4} \mapsto \quad \cdots$

$\mathrm{Aut}(K/\mathbb{Q}(\sqrt{2})) = \langle \tau \rangle = \{1, \tau\}$

$\mathrm{Aut}(K/\mathbb{Q}(i)) = \langle \sigma \rangle$

b) $K = \mathbb{Q}(\sqrt[3]{2})$

$\mathrm{Aut}(K/\mathbb{Q}) = \{id\}$

Pf: Let $\tau \in \mathrm{Aut}(K/\mathbb{Q})$

Then

$$0 = \tau(0) = \tau(\sqrt[3]{2}^3 - 2) = \tau(\sqrt[3]{2})^3 - 2,$$

so $\tau(\sqrt[3]{2})^3$ is a root of $x^3 - 2$

i.e. it equals $\sqrt[3]{2}$

only such root in K

Prop: Let $F \subseteq K$, $f(x) \in F[x]$. Let $\sigma \in \mathrm{Aut}(K/F)$. If $\alpha \in K$ is a root of f, then so is $\sigma(\alpha)$.

Pf: Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$.

Since σ is a field automorphism fixing F,

$$\begin{aligned} f(\sigma(\alpha)) &= a_n(\sigma(\alpha))^n + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(a_n)(\sigma(\alpha))^n + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) \\ &= \sigma(f(\alpha)) = \sigma(0) = 0 \end{aligned}$$

$\square$

Therefore, every elt. of $\mathrm{Aut}(K/F)$ permutes the roots of each $f(x) \in F[x]$.

Def: Let $H \leq \operatorname{Aut} K$. Define

$$\operatorname{Fix} H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$$

Prop:

a) $\operatorname{Fix} H$ is a field

b) If $H_1 \leq H_2$, then $\operatorname{Fix} H_2 \subseteq \operatorname{Fix} H_1$

c) If $F_1 \subseteq F_2 \subseteq K$, then $\operatorname{Aut}(K/F_2) \leq \operatorname{Aut}(K/F_1) \leq \operatorname{Aut}(K)$

d) $\operatorname{Fix} \{id\} = K$

Pf: a) If $a, b \in \operatorname{Fix} H$, then for all $\sigma \in H$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a+b$$

$$\sigma(ab) = \sigma(a)\sigma(b) = ab$$

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$$

b) If $H_1 \leq H_2$, elements of $\operatorname{Fix} H_2$ satisfy all the conditions of elts. of $\operatorname{Fix} H_1$

c) Similar

d) id fixes every elt.

Ex: a) $K = \mathbb{Q}(\sqrt{2}, i)$, $\mathrm{Aut}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma \circ \tau\}$

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

Subgps of $\mathrm{Aut}(K/\mathbb{Q})$: $\overset{=1}{\{id\}}$, $\langle \sigma \rangle$, $\langle \tau \rangle$, $\langle \sigma \circ \tau \rangle$, $\langle \sigma, \tau \rangle$

$\mathrm{Fix}\ 1 = K$ $\qquad$ $\mathrm{Fix}\ \langle \tau \rangle = \mathbb{Q}(\sqrt{2})$

$\mathrm{Fix}\ \langle \sigma \rangle = \mathbb{Q}(i)$ $\qquad$ $\mathrm{Fix}\ \langle \sigma \circ \tau \rangle = \mathbb{Q}(i\sqrt{2})$

$\mathrm{Fix}\ \langle \sigma, \tau \rangle = \mathbb{Q}$

Subgp. lattice
(upside down)

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
\langle \sigma \rangle \arrow[dr, dash, "2"'] & \langle \tau \rangle \arrow[d, dash, "2"'] & \langle \sigma \circ \tau \rangle \arrow[dl, dash, "2"] \\
 & \langle \sigma, \tau \rangle &
\end{tikzcd}$$

Lattice of int. fields

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

(turns out, this is all int. fields)

b) $K = \mathbb{Q}(\sqrt[3]{2})$, $\quad \mathrm{Aut}(K/\mathbb{Q}) = \{id\}$

Subgp. lattice	Lattice of int. fields
1	$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}) \\ 3 \Big\vert \\ \mathbb{Q} \end{array}$

We want the nice situation!

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

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

w/ equality iff f is separable.