

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

Course midterm feedback form (form still open)

- Lecture pace about right
 - Homework maybe a bit too long
 - Enjoy field ext's, compass and straightedge constructions
 - Not everyone can make office hours; email me to meet
-

Recall

Galois theory

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

$\text{Aut}(K) = \text{gp. of automs. of } K$

(under function composition)

If K/F field extn., let σ fixes F

$$\text{Aut}(K/F) = \left\{ \sigma \in \text{Aut}(K) \mid \underbrace{\sigma(a) = a \ \forall a \in F}_{\sigma \text{ fixes } a} \right\}$$

Remark:

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

b) $\text{Aut}\left(\frac{K}{\text{prime subfield}}\right) = \text{Aut}(K)$

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

E.g.: a)

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

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

where

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

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

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

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

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

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

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

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

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

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 $\sigma \in \text{Aut}(K/F)$.

If $\alpha \in K$ is a root of f , then so is $\sigma(\alpha)$.

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

Since σ is a field automorphism fixing F ,

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

□

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

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

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

Prop:

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

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

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

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

Pf: a) If $a, b \in \text{Fix } H$, 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 $\text{Fix } H_2$ satisfy all the conditions of elts. of $\text{Fix } H_1$

c) Similar

d) id fixes every elt.

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

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

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

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

$\text{Fix } 1 = K$

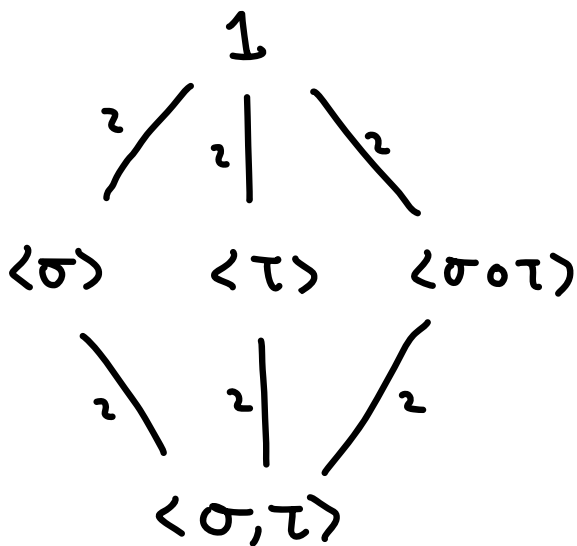
$\text{Fix } \langle \tau \rangle = \mathbb{Q}(\sqrt{2})$

$\text{Fix } \langle \sigma \rangle = \mathbb{Q}(i)$

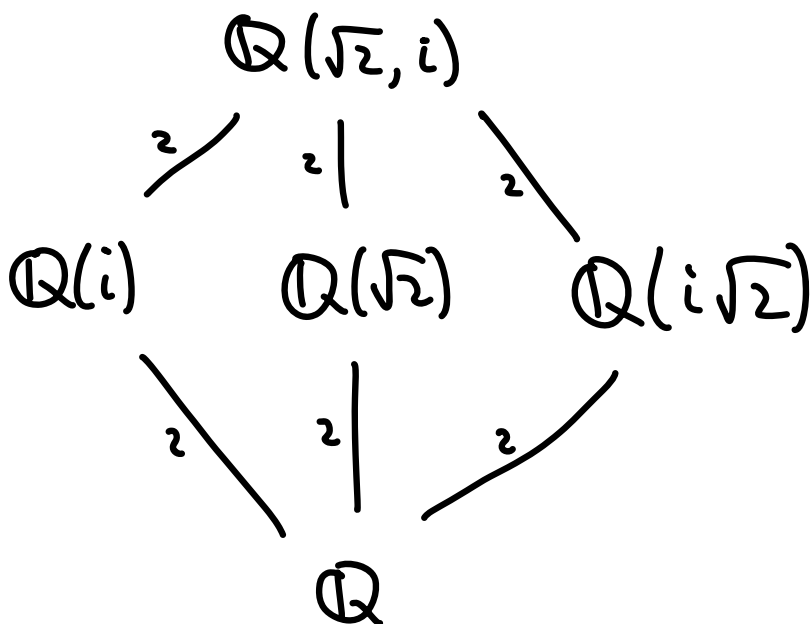
$\text{Fix } \langle \sigma \circ \tau \rangle = \mathbb{Q}(i\sqrt{2})$

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

Subgp. lattice
(upside down)



Lattice of int. fields



(turns out, this is all int. fields)

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

Subgp. lattice

1

Lattice of int. fields

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

3 |

\mathbb{Q}

We want the nice situation!

Thm: Let $f(x) \in F[x]$, $K = \text{Sp}_F f$. Then,

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

w/ equality iff f is separable.