
Abstract Algebra III

— This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat. —

Galois correspondence / Fundamental Theorem of Galois theory

Let K/F be a Galois extension. There is a one-to-one correspondence (a bijection) between the fields $F \subseteq E \subseteq K$ and the subgps of $\text{Gal}(K/F)$.

• for every field E $F \subseteq E \subseteq K$ there is

a subgroup of $\text{Gal}(K/F)$:

$\text{Gal}(K/E)$

• K/E is Galois !

big \Downarrow

if σ fixes E then
fixes $F \subseteq E$

• $\text{Gal}(K/E) = \text{Aut}(K/E) < \text{Aut}(K/F)$

• for every subgroup $H < \text{Gal}(K/F)$ there
is a field $F \subseteq E \subseteq K$:

K^H

$$K^H := \left\{ \alpha \in K : \sigma(\alpha) = \alpha \quad \forall \sigma \in H \right\}$$

(defined)

the elements of K fixed by every element of H

"the fixed field of H in K "

Further! If $E = K^H$ then $H = \text{Gal}(K/E)$

If $F \subseteq E \subseteq K$ then $E = K^{\text{Gal}(K/E)}$

These processes (field \rightarrow gp ; gp \rightarrow field) are inverses

So what about F ?

F is an intermediate field: $F \subseteq F \subseteq K$

What is the subgroup? It is $\text{Gal}(K/F)$

So going $\text{gp} \rightarrow \text{field}$

$$F = K^{\text{Aut}(K/F)}$$

Last definition
of K/F is
Galois.

Notice that $F \subseteq K^{\text{Aut}(K/F)}$

Example: $K = \mathbb{Q}(\sqrt[3]{2})$ $\sigma \in \text{Aut}(K/\mathbb{Q})$

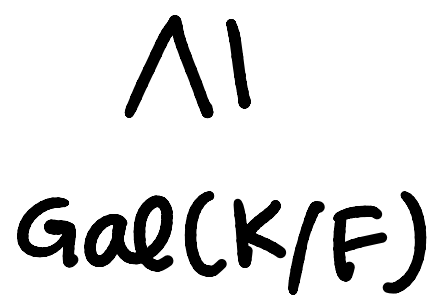
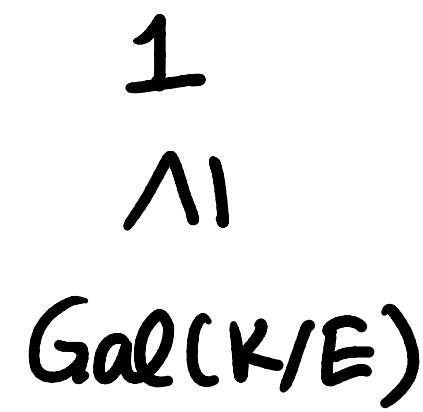
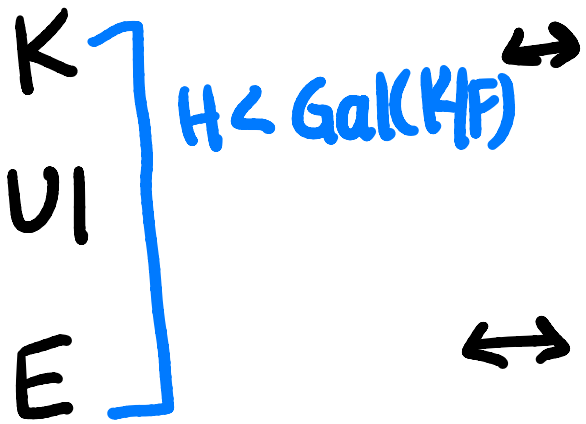
$$F = \mathbb{Q}$$

must send $\sqrt[3]{2} \mapsto$ root of $x^3 - 2$

but K contains only one
root of $x^3 - 2$

so if $\sigma \in \text{Aut}(K/\mathbb{Q}) \Rightarrow \sigma = \text{id}$

$$\Rightarrow K^{\text{Aut}(K/\mathbb{Q})} = K \supseteq \mathbb{Q}$$



\uparrow fewer elements fix more things

\downarrow more elements fix fewer things

K is Galois over E
 E might not be Galois over F

Furthermore!

E/F is Galois iff $\text{Gal}(K/E) \trianglelefteq \text{Gal}(K/F)$

and in that case $\text{Gal}(E/F) \cong \text{Gal}(K/F) / \text{Gal}(K/E)$

$$\text{Gal}(K/F) \left[\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right] \begin{array}{l} \text{Gal}(K/E) \\ \text{Gal}(E/F) \cong \text{Gal}(K/F) / \text{Gal}(K/E) \end{array}$$

field side

gp side

$E_1 \rightsquigarrow H_1$
 $E_2 \rightsquigarrow H_2$

composite \rightarrow

$E_1 E_2$

smallest field containing E_1 and E_2

E_1

E_2

$H_1 \cap H_2$

largest subgp contained in H_1 and H_2

H_1

H_2

intersection \rightarrow

$E_1 \cap E_2$

largest field contained in E_1 and E_2

\leftarrow

subgp generated by H_1 and H_2

$\langle H_1, H_2 \rangle$

smallest subgp containing H_1 and H_2

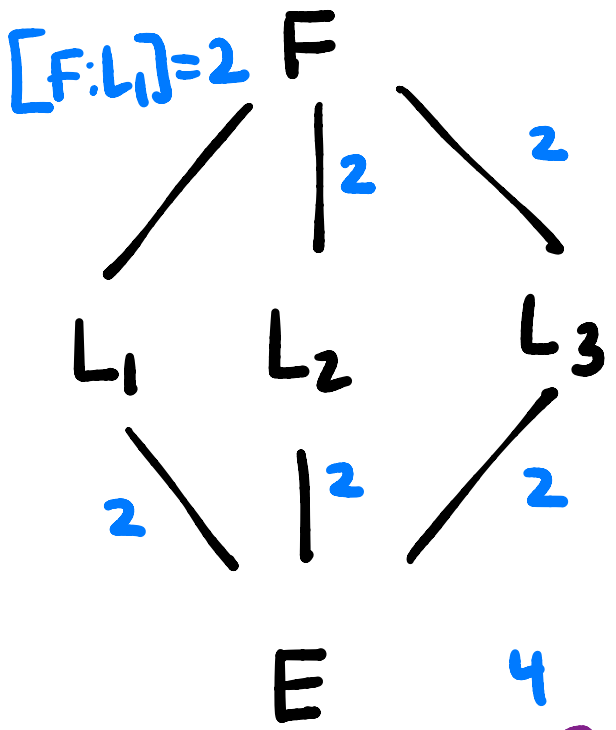
$$K^{H_1 \cap H_2} = K^{H_1} K^{H_2} \quad \text{composite}$$

$$K^{\langle H_1, H_2 \rangle} = K^{H_1} \cap K^{H_2}$$

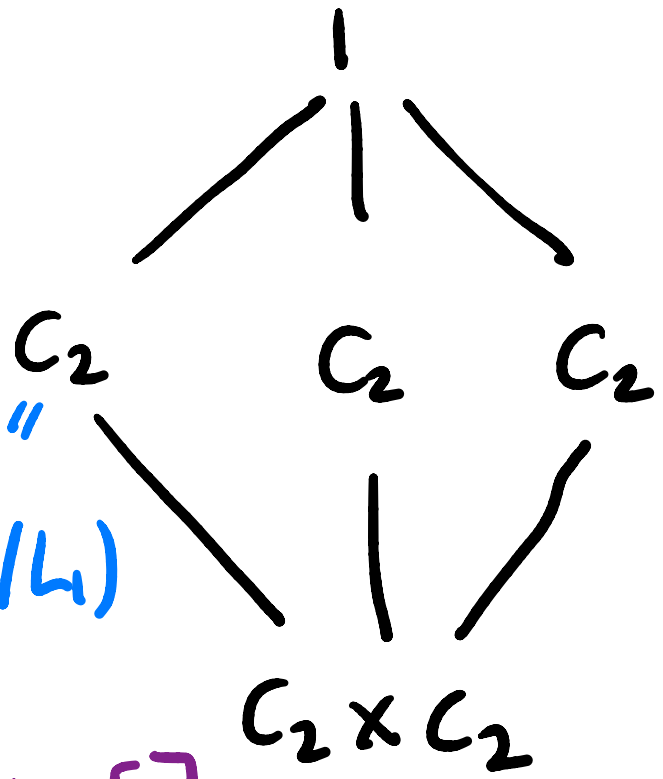
$$\text{Gal}(K/E_1 \cap E_2) = \langle \text{Gal}(K/E_1), \text{Gal}(K/E_2) \rangle$$

$$\text{Gal}(K/E_1 E_2) = \text{Gal}(K/E_1) \cap \text{Gal}(K/E_2)$$

#4 F/E is Galois with $\text{Gal}(F/E) \cong C_2 \times C_2$



$\text{Gal}(F/L_1)$



$4 = 2 \cdot 2$
 $[F:E] = [F:L_1][L_1:E]$

Lemma: If $[L:E]=2$ and E is not of char 2
then $\exists x \in E \ x \notin E^2$ with
 $L = E(\sqrt{x})$

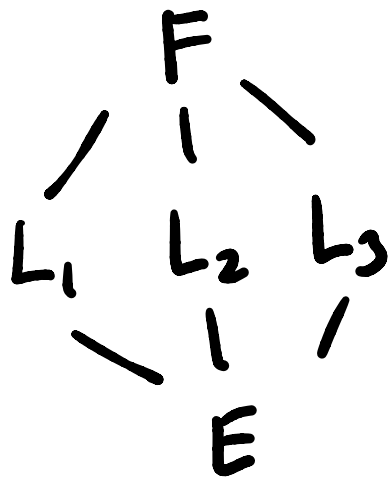
proof: L/E is finite, and it's also separable
since $\gcd([L:E], \text{char } E) = 1$, by the
Primitive Element Theorem, $L = E(\alpha)$, $\deg m_{\alpha, E} = 2$

Since $\deg m_{\alpha, E} = 2$ and $\text{char } E \neq 2$
can use the quadratic formula to
give the roots of $m_{\alpha, E}$ to be

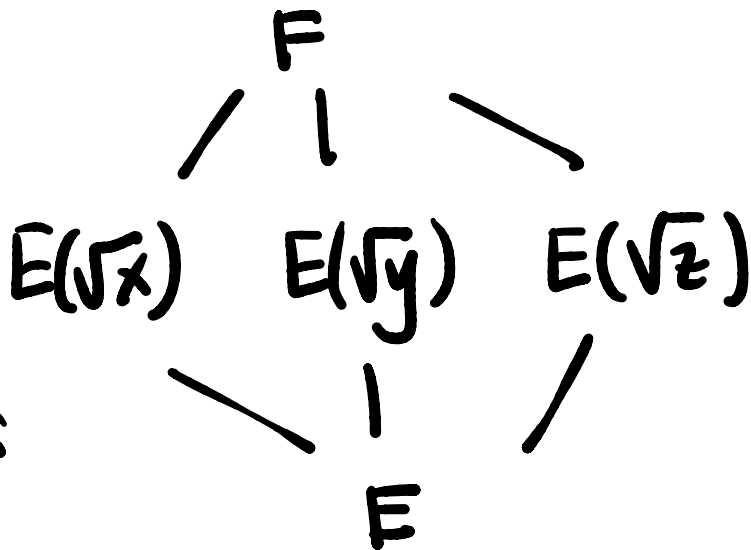
$$\beta, \alpha = \frac{a \pm \sqrt{x}}{b} \quad a, b, x \in E$$

$$E(\alpha) = E(\sqrt{x}), \quad x^2 \notin E \text{ because if} \\ \text{so } E(\sqrt{x}) = E$$

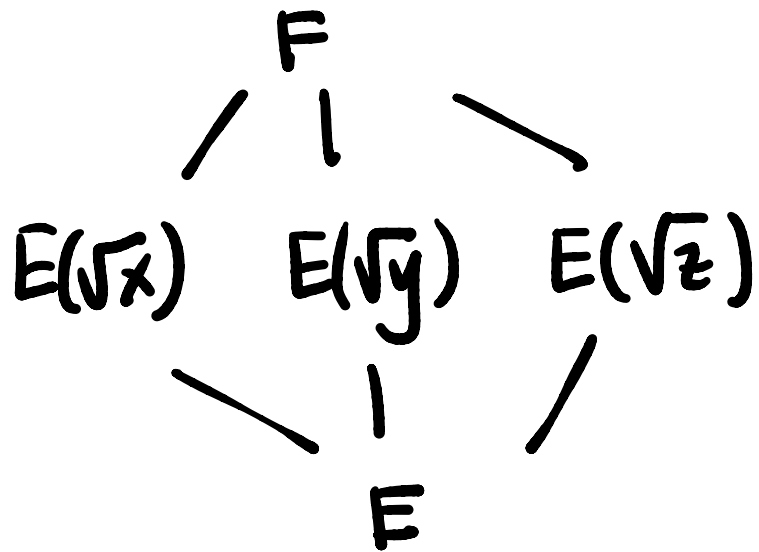
So my



is really



x, y, z are
all nonsquares
in E



Since $E(\sqrt{x}) \neq E(\sqrt{y})$,
 $\sqrt{y} \notin E(\sqrt{x})$

$$\Rightarrow [E(\sqrt{x})(\sqrt{y}) : E(\sqrt{x})] = 2$$

since $t^2 - y$ is still irreducible
 over $E(\sqrt{x})[t]$

Since $E(\sqrt{x}, \sqrt{y}) = E(\sqrt{x})(\sqrt{y})$

$$[E(\sqrt{x}, \sqrt{y}) : E] = 4 \quad \text{and} \quad E(\sqrt{x}, \sqrt{y}) \subseteq F$$

But $[F:E]=4$ also so $F = E(\sqrt{x}, \sqrt{y})$

Consider $E(\sqrt{xy}) \subseteq F$ because $\sqrt{xy} = \sqrt{x}\sqrt{y}$

\rightsquigarrow on Friday we'll get that xy not square, this is the last quadratic extension

That's all for today!

Friday

- finish this

- quiz 8