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 $Gal(K/F)$.

- for every field E $\quad F \subseteq E \subseteq K$ there is a subgp of $Gal(K/F)$: $\boxed{Gal(K/E)}$

    - $\boxed{K/E \text{ is Galois !}}$ big $\Downarrow$ if σ fixes E then fixes $F \subseteq E$
    - $Gal(K/E) = Aut(K/E) < Aut(K/F)$

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

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

defined

the elements of K fixed by every element of H

"the fixed field of H in K"

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

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

These processes (field $\to$ gp ; gp $\to$ field) are inverses

So what about F?

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

What is the subgp? It is $\mathrm{Gal}(K/F)$

So going gp $\to$ field

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

Last definition of K/F is Galois.

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

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

$F = \mathbb{Q}$ $\quad$ must send $\sqrt[3]{2} \mapsto$ Root of $x^3 - 2$

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

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

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

$$\begin{array}{ccc} K & \leftrightarrow & 1 \\ \cup\!| & & \wedge\!| \\ E & \leftrightarrow & \mathrm{Gal}(K/E) \\ \cup\!| & & \wedge\!| \\ F & \leftrightarrow & \mathrm{Gal}(K/F) \end{array}$$

$H < \mathrm{Gal}(K/F)$

↑ fewer elements fix more things

↓ more elements fix fewer things

K is Galois over E

E might not be Galois over F

Furthermore!

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

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

$$\begin{array}{ccc} & K & \\ & | & \mathrm{Gal}(K/E) \\ \mathrm{Gal}(K/F) & E & \\ & | & \mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \\ & F & \end{array}$$

field side

gp side

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

$$
\begin{tikzcd}
 & E_1E_2 \arrow[dl, no head] \arrow[dr, no head] & \\
E_1 \arrow[dr, no head] & & E_2 \arrow[dl, no head] \\
 & E_1 \cap E_2 &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & H_1 \cap H_2 \arrow[dl, no head] \arrow[dr, no head] & \\
H_1 \arrow[dr, no head] & & H_2 \arrow[dl, no head] \\
 & \langle H_1, H_2 \rangle &
\end{tikzcd}
$$

composite → E_1E_2

smallest field containing E_1 and E_2 ⟷ $H_1 \cap H_2$ largest subgp contained in H_1 and H_2

intersection → $E_1 \cap E_2$

largest field contained in E_1 and E_2 ⟷ subgp generated by H_1 and H_2 $\langle H_1, H_2 \rangle$

smallest subgp containing H_1 and H_2

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

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

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

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

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

$[F:L_1]=2$

$$
\begin{tikzcd}
 & F \arrow[dl, dash] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
L_1 \arrow[dr, dash, "2"'] & L_2 \arrow[d, dash, "2"] & L_3 \arrow[dl, dash, "2"] \\
 & E &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
C_2 \arrow[dr, dash] & C_2 \arrow[d, dash] & C_2 \arrow[dl, dash] \\
 & C_2 \times C_2 &
\end{tikzcd}
$$

$C_2 = \mathrm{Gal}(F/L_1)$

$$4 = 2 \cdot 2$$

$$[F:E] = [F:L_1][L_1:E]$$

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 $\gcd([L:E], \operatorname{char} E) = 1$, by the Primitive Element Theorem, $L = E(\alpha)$, $\deg m_{\alpha,E} = 2$

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

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

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

So my

$$\begin{tikzcd}[column sep=small]
& F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & L_2 \arrow[d, dash] & L_3 \arrow[dl, dash] \\
& E &
\end{tikzcd}$$

is really

$$\begin{tikzcd}[column sep=small]
& F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
E(\sqrt{x}) \arrow[dr, dash] & E(\sqrt{y}) \arrow[d, dash] & E(\sqrt{z}) \arrow[dl, dash] \\
& E &
\end{tikzcd}$$

x, y, z are all nonsquares in E

$$\begin{tikzcd}
 & F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
E(\sqrt{x}) \arrow[dr, dash] & E(\sqrt{y}) \arrow[d, dash] & E(\sqrt{z}) \arrow[dl, dash] \\
 & E &
\end{tikzcd}$$

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

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

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