Lecture 25

Galois Theory: Symmetry groups of (some nice) field extensions.

defns.

① $\mathrm{Aut}(K) = \{$field automorphisms of $K\}$ is a group.

$\sigma \in \mathrm{Aut}(K)$ fixes $\alpha \in K$ if $\sigma\alpha = \alpha$.

② $\mathrm{Aut}(K/F) = \{$Automorphisms of K that fix $F\}$.

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

prop. Let K/F be an extension, and let $\alpha \in K$ be algebraic over F.

Then $\forall\, \sigma \in \mathrm{Aut}(K/F)$, $m_{\alpha,F}(\sigma\alpha) = 0$

↪ ie $\{\sigma\alpha\}$ are all roots of $m_{\alpha,F}(x)$!

pf. If $f(\alpha)=0$ then since coeffs of f are fixed by σ,

$0 = \sigma(f(\alpha)) = f(\sigma\alpha)$. //

defn. You can also consider $H \leq \mathrm{Aut}(K)$ and ask which subfield of K is fixed by H: this is the fixed field of H.

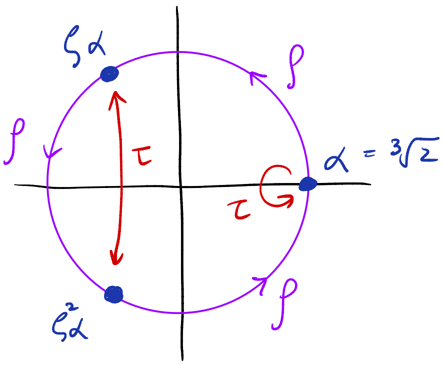
↪ note For any subset $X \subset \mathrm{Aut}(K)$, the fixed elements will form a field. (exercise)

prop.

$$\begin{array}{c} K \\ \cup\!\text{|} \\ F_2 \\ \cup\!\text{|} \\ F_1 \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} (\mathrm{Aut}(K/K)) = \{1\} \\ \wedge\!\text{|} \\ \mathrm{Aut}(K/F_2) \\ \wedge\!\text{|} \\ \mathrm{Aut}(K/F_1) \end{array}$$

pf. Think through the group action. (100-level exercise)

Eg. Consider $f(x) = x^3 - 2$.



Observe:

$$\begin{array}{ccc} \mathbb{Q}(\alpha) & & Aut(\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha)) = \{1\} \\ \Big| \ deg = 3 & \xleftrightarrow{\text{boo}} & \Big| \ index = 1 \\ \mathbb{Q} & & \underbrace{Aut(\mathbb{Q}(\alpha)/\mathbb{Q})}_{\text{too small}} \cong \{1\} \end{array}$$

Because $\sigma \in Aut(K/\mathbb{Q})$ must satisfy

$(\sigma\alpha)^3 - 2 = 0$

and the other options $\zeta\alpha, \zeta^2\alpha \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$

On the other hand:

$$\begin{array}{cccc} K = \mathbb{Q}(\zeta, \alpha) & & & Aut(K/K) = \{1\} \\ \Big| \ 2 & \xleftrightarrow{\text{yay}} & \text{index } 2 & \Big| \\ \mathbb{Q}(\alpha) & & & Aut(K/\mathbb{Q}(\alpha)) \cong \langle \tau \rangle \\ \Big| \ 3 & \xleftrightarrow{\text{yay}} & \text{index } 3 & \Big| \ \text{not a normal subgroup!} \\ F = \mathbb{Q} & & & Aut(K/\mathbb{Q}) \cong D_3 \cong S_3 \end{array}$$

prop. Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then $|Aut(E/F)| \leq [E:F]$, with equality if $f(x)$ is separable. (proof omitted.)

defn. Let K/F be a finite extension.

K is Galois over F (K/F is a Galois extension)

if $[Aut(K/F) : Aut(K/K)] = |Aut(K/F)| = [K:F]$

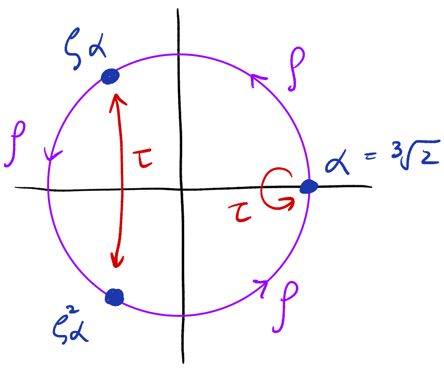
If K/F is Galois, then $Aut(K/F)$ is the Galois group of K/F, and is denoted $Gal(K/F)$.

prop. Let K/F be a finite extension. Then $|Aut(K/F)| \leq [K:F]$

with equality iff F is exactly the fixed field of $Aut(K/F)$.

ie K/F is Galois iff

eg. Revisit $f(x) = x^3 - 2$



$\zeta = \zeta_3$ root of $\Phi_3(x) = x^2 + x + 1$

$$\begin{tikzcd}
 & \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle \rho \rangle \arrow[dr, dash] & \langle \tau \rangle \arrow[d, dash] & \langle \rho\tau \rangle \arrow[dl, dash] & \langle \rho^2\tau \rangle \arrow[dll, dash] \\
 & D_3 \cong S_3 & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta, \alpha) \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "2"] & & \\
\mathbb{Q}(\zeta) \arrow[dr, dash, "2"'] & \mathbb{Q}(\alpha) \arrow[d, dash, "3"] & \mathbb{Q}(\zeta\alpha) \arrow[dl, dash, "3"] & \mathbb{Q}(\zeta^2\alpha) \arrow[dll, dash, "3"] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

How to compute these Galois groups / fixed fields

- Constraints: $\sigma \in \mathrm{Aut}(K/F)$ must be injective.
  $\hookrightarrow$ $\mathrm{Aut}(\text{splitting field of } x^3-2 / \mathbb{Q}) \leq S_3$ = perms of the roots.
  Check that these are actually field automorphisms.
- fixed fields: just compute.

—//—

Fact ~~Thm.~~ K/F is Galois iff K is the splitting field of some separable polynomials over F.

↳ Note that in this case, every irreducible $f(x) \in F[x]$ with a root in K has all roots in K (and is separable).

b/c $f(x) =$ product of some minimal polynomials.

defn. Let K/F be a Galois extension.

If $\alpha \in K$, then the elements $\{\sigma\alpha\}_{\sigma \in Gal(K/F)}$ are called Galois conjugates of α.

↳ These are precisely the set of roots of $m_{\alpha,F}(x)$.

Characterizations of Galois Extensions

1. splitting fields of separable polynomials over F
2. K/F where the fixed field of $Aut(K/F)$ is F
3. K/F where $[K:F] = |Aut(K/F)|$
4. finite, normal, separable extensions.

↳ normal extension: splitting field of some set of polynomials ($\Rightarrow$ algebraic) thm (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$.

There is a bijection

$$\left\{ \begin{array}{l} \text{subfields } E \text{ of} \\ K \text{ containing } F \end{array} \quad \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{subgroups } H \\ \text{of } G \end{array} \quad \begin{array}{c} \{1\} \\ | \\ H \\ | \\ G \end{array} \right\}$$

$$E \longmapsto \mathrm{Aut}(K/E)$$

notation: $K_H :=$ fixed field of $H \longleftarrow H$

Under this correspondence: $E_i \longleftrightarrow H_i$

① (Inclusion reversing) $E_1 \leq E_2 \rightsquigarrow H_1 \geq H_2$

②
$$\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\end{array}}\right\} |H| \\ \\ \left.\vphantom{\begin{array}{c}1\\1\end{array}}\right\} [G:H] \end{array}$$

③ K/E is Galois, with $\mathrm{Gal}(K/E) = H$.

④ E/F is Galois iff $H \trianglelefteq G$.

Then $\mathrm{Gal}(E/F) \cong G/H$.

⑤ $E_1 \cap E_2 \rightsquigarrow \langle H_1, H_2 \rangle$

$E_1 E_2 \leftrightsquigarrow H_1 \cap H_2$

$\boxed{\text{Proof of part (4)}}$

Consider

$$\begin{array}{l} K \\ | \ \text{degree} = H \\ E \\ | \ \text{degree} = [G:H] \\ F \end{array} \qquad\qquad \begin{array}{l} \{1\} \\ | \\ H = \mathrm{Aut}(K/E) \\ | \\ G = \mathrm{Aut}(K/F) \ni \sigma, \sigma' \end{array}$$

Let $\sigma, \sigma' \in G \rightsquigarrow \sigma, \sigma' : K \longrightarrow K$.

where $\sigma|_F, \sigma'|_F = id_F$.

Now consider $\sigma|_E, \sigma'|_E : E \longrightarrow K \quad \in \mathrm{Emb}(E/F)$

= embeddings of E into K which fix F

Then $\sigma|_E = \sigma'|_E$ iff $\sigma^{-1}\sigma'$ fixes E, ie $\sigma^{-1}\sigma' \in \mathrm{Aut}(K/E) = H$

$\Longrightarrow \mathrm{Aut}(E/F) \subseteq \mathrm{Emb}(E/F) \xleftrightarrow{1:1} G/H$ (cosets)

$\Longrightarrow |\mathrm{Aut}(F/E)| \leq |\mathrm{Emb}(E/F)| = [G:H] = [E:F]$.

E/F is Galois $\Longleftrightarrow |\mathrm{Aut}(E/F)| = [E:F]$.

ie. every embedding of E is an automorphism of E

Observe: $\sigma(E) = K_{\sigma H \sigma^{-1}}$

$(\sigma h \sigma^{-1})(\underset{\substack{\uparrow \\ \sigma(E)}}{\sigma\alpha}) = \sigma h \alpha = \sigma\alpha \quad \forall\, h \in H = \mathrm{Aut}(K/E) \quad \Longrightarrow \sigma H \sigma^{-1} \in \mathrm{Aut}(K/\sigma(E))$

h fix E

Then use $|\sigma H \sigma^{-1}| = [K:\sigma(E)] = |K:E|$.

Now $\sigma(E) = E$ iff $\sigma H \sigma^{-1} = H \quad \forall\, \sigma \in G$.

ie. E/F is Galois iff $H \trianglelefteq G$.

//