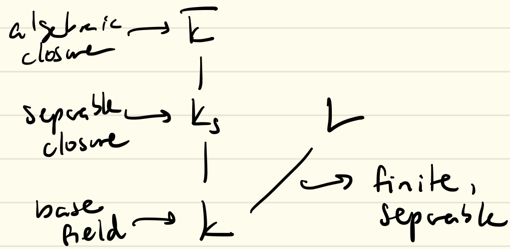
2/24

Action of Galois Group

Setup:



k_s = splitting field of all separable polys over k $\Rightarrow$ k_s/k Galois
So we can consider the group $Gal(k_s/k) =: Gal(k)$

L/k finite, separable $\Rightarrow$ by Primitive Elt. Thm $L = k(\alpha)$, $\alpha \in L$ is the root of some irred. poly. f over k, f deg n. Consider set of ring homs $Hom(L, \bar{k})$. Any $\phi \in Hom(L, \bar{k})$ is def. by where it sends α, and it must send α to a root of f; so $\exists$ n choices, hence n distinct ϕ's $\in Hom_k(L, \bar{k})$, so $Hom_k(L, \bar{k})$ is a finite set. Since L is separable, the image $\phi(L)$ will be separable, hence $\subseteq k_s$, so we can consider $Hom_k(L, \bar{k}) = Hom_k(L, k_s)$.

So we have a group $Gal(k)$ and a finite set $Hom_k(L, k_s)$. Want to consider the action $Gal(k) \circlearrowright Hom_k(L, k_s)$ & see what it can tell us about Galois exts.

☆ We are going to build an equivalence b/t finite, separable field extensions and $Gal(k)$-sets of a certain type!

First, some review + new defs:

I. Review - Gp Actions

① A group action by a group G on a set X is a map
$m: G \times X \longrightarrow X$, $m(g, x) = g \cdot x$, where $g \cdot x$ satisfies:

1) Identity: $\forall x \in X$, $1 \cdot x = x$, where $1 \in G$ is the identity.
2) Composition: $\forall g_1, g_2 \in G$, $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

$\rightsquigarrow$ (if Cadell does cts grps, say cts gr action here)

② $\forall x \in X$, the orbit of x is the set $Orb_x = \{g \cdot x \mid g \in G\} \subseteq X$
The stabilizer of x is the subgp $Stab_x = \{g \in G \mid g \cdot x = x\} \leq G$

Orb_x + $Stab_x$ are related by $|Orb_x| = [G : Stab_x]$

③ An action is transitive if $Orb_x = X$ $\forall x \in X$.

④ Two G-sets X, Y are isomorphic if $\exists$ bijection $f: X \longrightarrow Y$
s.t. $\forall x \in X, g \in G$, $f(g \cdot x) = g \cdot f(x)$.

⑤ Facts: 1) The reln. on X, $x \sim y \Leftrightarrow y = g \cdot x$ for some $g \in G$,
defines an equivalence reln. on X where the equivalence classes are the orbits, which partition X.

2) $\forall x \in X$, $\exists$ isomorphism $Orb_x \xrightarrow{\sim} Stab_x \backslash G$ $\rightarrow$ left cosets
$g \cdot x \longmapsto g\, Stab_x$ left coset

II. When can we say a gp action is cts?

① A topological group G is a group which is also a top. space satisfying T1 (finite point sets are closed) s.t. the group operation maps $G \times G \rightarrow G$, $(g, h) \mapsto gh$ and inversion maps $G \rightarrow G$, $g \mapsto g^{-1}$ are cts.

② Action is cts if $G \times X \longrightarrow X$, $(g, x) \mapsto g \cdot x$ is cts.

② Examples: $\mathrm{Gal}(E/F)$ w/ profinite topology
$\mathbb{Z}$ with discrete topology $\rightsquigarrow$ (any gp w/ discrete top).

③ <u>Lemma</u>: If X is a discrete top space, and G is a topological group, then $G \circlearrowright X$ is cts $\iff$ $\forall x \in X$, $\mathrm{Stab}_x = \{g \in G \mid g \cdot x = x\}$ is open in G.

<u>$\Rightarrow$</u>: Let $x \in X$, consider $\mathrm{Stab}_x = \{g \in G \mid g \cdot x = x\}$.
Consider the composite map
$$G \xrightarrow{i_x} G \times X \xrightarrow{m} X$$
$$g \longmapsto (g, x) \longmapsto g \cdot x$$
The map i_x is clearly cts $\Rightarrow$ $m \circ i_x$ is cts, and $(m \circ i_x)^{-1}(x) = \{g \in G \mid g \cdot x = x\} = \mathrm{Stab}_x \Rightarrow \mathrm{Stab}_x$ is open, since $\{x\}$ is open in X.

<u>$\Leftarrow$</u>: Let $m: G \times X \to X$ be the group action, let $x \in X$ and consider the open set $\{x\} \subseteq X$. WTS $m^{-1}(\{x\}) = m^{-1}(x)$ is open in $G \times X$ (where we give $G \times X$ product top)

$$m^{-1}(x) = \{(g, y) \in G \times X \mid g \cdot y = x\}$$
$$= \coprod_{y \in X} \{(g, y) \in G \times \{y\} \mid g \cdot y = x\} =: \coprod_{y \in Y} A_y$$
WTS open $\forall y$.

If $\nexists g \in G$ s.t. $g \cdot y = x$, then $A_y \neq \emptyset$, open.
If $A_y \neq \emptyset$, then A_y is homeomorphic to Stab_x:
Fix $h \in G$ s.t. $h \cdot y = x$ ($\exists$ since $A_y \neq \emptyset$).
Define
$$\mathrm{Stab}_x \to A_y \qquad A_y \to \mathrm{Stab}_x$$
$$g \mapsto (gh, y) \qquad (g, y) \mapsto gh^{-1}$$
$$\left\{ \begin{array}{l} (g,y) \mapsto gh^{-1} \mapsto (g,y) \\ g \mapsto (gh, y) \mapsto g \end{array} \right\}$$
$h^{-1} \cdot x = y$
$gh^{-1} \cdot x = g \cdot y = x$
cts since gp multiplication is cts.

So Stab_x open $\Rightarrow A_y$ open $\forall y \Rightarrow m^{-1}(x)$ open $\Rightarrow m$ is cts.

separable closure k_s $\;\;$ L finite, separable
k

Back to fields: Consider $\mathrm{Gal}(k)$, $\mathrm{Hom}(L, k_s)$
There is a natural gp action $\mathrm{Gal}(k) \circlearrowright \mathrm{Hom}(L, k_s)$:
for $g \in \mathrm{Gal}(k)$, $\phi \in \mathrm{Hom}_k(L, k_s)$, define
$$g \cdot \phi = g \circ \phi \in \mathrm{Hom}_k(L, k_s).$$
Exr: this is a gp action

Lemma: This action is cts and transitive.
Cts: By previous, WTS for $\phi \in \mathrm{Hom}_k(L, k_s)$, $\mathrm{Stab}\,\phi$ is open.

$$\begin{aligned}\mathrm{Stab}\,\phi &= \{g \in \mathrm{Gal}(k) \mid g \circ \phi = \phi\} \\ &= \{g \in \mathrm{Gal}(k) \mid g(\phi(L)) = \phi(L)\} \\ &= \text{elts. fixing } \phi(L) \\ &= \mathrm{Gal}(k_s/\phi(L)) \leq \mathrm{Gal}(k_s/k)\end{aligned}$$

Since $\mathrm{Orb}\,\phi \subseteq \mathrm{Hom}(L, k_s)$ is finite set, by orbit-stabilizer thm $\mathrm{Gal}(k_s | \phi(L))$ is a subgp of finite index.
By main theorem of Galois theory $\mathrm{Gal}(k_s | \phi(L))$ is closed. which comes since L is normal.
Since open subgps = closed subgps of finite index, $\mathrm{Gal}(k_s | \phi(L))$ is open, so the action is cts.

$\mathrm{Gal}(L|k)$ acts transitively; the fact that it extends to trans. of $\mathrm{Gal}(k) \circlearrowright \{\text{roots}\}$ follows from surj. $\mathrm{Gal}(k) \twoheadrightarrow \mathrm{Gal}(L|k)$

Transitive: Again letting $L = k(\alpha)$, where α is the root of some irred. poly f over k, $\mathrm{Gal}(k)$ acts transitively on the set of roots of f.
These roots are in bijection w/ elts of $\mathrm{Hom}(L, k_s)$, since each elt. $\phi_i \in \mathrm{Hom}_k(L, k_s)$ is uniquely det. by which root it sends α to; so the transitivity of $\mathrm{Gal}(k) \circlearrowright \{\text{roots of } f\}$ extends to transitivity of $\mathrm{Gal}(k) \circlearrowright \mathrm{Hom}_k(L, k_s)$.

$\alpha_1, \ldots, \alpha_n$ roots of f

$\mathrm{Gal}(k)\,\alpha = \{\alpha_1, \ldots, \alpha_n\}$, $\alpha = \alpha_1$

exist g_i $\;\;$ say $\phi_1 : \alpha \mapsto \alpha$

$\rightarrow \alpha_i = g_i \cdot \alpha_1 \;\; \forall i$

$\phi_i(\alpha) = g_i \cdot \phi_1(\alpha)$

$\phi_i = g_i \cdot \phi_1$

By Fact 2, we have an isomorphism of G-sets

$$\mathrm{Orb}_\phi \xrightarrow{\sim} \mathrm{Stab}_\phi \backslash \mathrm{Gal}(k)$$ $\to$ set of left cosets of $\mathrm{Gal}(k)$ by Stab_ϕ (this is a G set)

(transitivity) $\|$

$$\mathrm{Hom}_k(L, k_s) \xrightarrow{\sim} \mathcal{U} \backslash \mathrm{Gal}(k),$$ some open subset $\mathcal{U}$.

If $L|k$ is Galois, then $L \cong \phi(L)$, since L is the splitting field of some f over k $\Rightarrow$ $\phi(L)$ is also the splitting field of f, since ϕ just permutes the roots of f, and any 2 splitting fields of the same poly are isomorphic.

So $L|k$ Galois $\Rightarrow \phi(L)|k$ Galois $\Rightarrow \mathrm{Stab}_\phi = \mathrm{Gal}(k_s|\phi(L))$ is a normal subgroup of $\mathrm{Gal}(k) \Rightarrow \mathrm{Stab}_\phi \backslash \mathrm{Gal}(k) = \mathrm{Gal}(k)/\mathrm{Stab}_\phi$ quotient group. So $L|k$ Galois $\Rightarrow \mathrm{Hom}_k(L, k_s) \cong \mathrm{Gal}(k)/\mathcal{U}$, $\mathcal{U} \trianglelefteq \mathrm{Gal}(k)$ open.

From category perspective:

If M is another finite sep. ext of k, each k-hom. $\phi: L \to M$ (respects $+$, $\cdot$, scalar product) induces a map

$$\mathrm{Hom}_k(M, k_s) \xrightarrow{F} \mathrm{Hom}_k(L, k_s)$$
$$\gamma \mapsto \gamma \circ \phi$$

F respects action by $\mathrm{Gal}(k)$: $g \in \mathrm{Gal}(k)$, $\gamma \in \mathrm{Hom}_k(M, k_s)$, $\phi: L \to M$

$$F(g \cdot \gamma) = (g \cdot \gamma) \circ \phi = g \circ \gamma \circ \phi = g \cdot (\gamma \circ \phi) = g \cdot F(\gamma)$$

So F is a well-defined contravariant functor from

$$\left\{ \begin{matrix} \text{category of} \\ \text{finite separable} \\ \text{exts. of } k \end{matrix} \right\} \xrightarrow{F} \left\{ \begin{matrix} \text{category of} \\ \text{finite sets w/} \\ \text{cts transitive left } \mathrm{Gal}(k) \text{ action} \end{matrix} \right\}$$

Galois $\longrightarrow$ quotients of $\mathrm{Gal}(k)$ by open normals.

Thm 1.5.2: these categories are (anti) equivalent.