

Galois Theory

Suppose you have any kind of algebraic gadget — a set with some operations obeying some axioms.

e.g. monoids, groups, rings, fields

Then we can define a "subgadget" of a gadget K to be a subset $k \subseteq K$ closed under all the operations.

The gadgets F with

$$k \subseteq F \subseteq K$$

form a poset with \subseteq as the partial ordering. Let's call this poset D .

Galois theory uses groups to study D .

Any gadget K has a group $\text{Aut}(K)$ of "automorphisms", i.e. 1-1 & onto functions $g: K \rightarrow K$ that preserve all the operations,

$$\text{e.g. } g(x+y) = gx+gy$$

$$g(xy) = (gx)(gy)$$

$$g(0) = 0$$

$$g(1) = 1$$

We say an element $x \in k$ is fixed by $g \in \text{Aut}(K)$ if $gx = x$.

We say a subgadget $F \subseteq k$ is fixed by $g \in \text{Aut}(K)$ if $gx = x$ for each $x \in F$.

Note the subset $\{g \in \text{Aut}(K) : g \text{ fixes } F\}$ is a subgroup of $\text{Aut}(K)$.

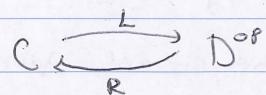
The subgroup of $\text{Aut}(K)$ fixing the subgadget $k \subseteq K$ is called the Galois group $G(K|k)$.

Let C be the poset of subgroups of $G(K|k)$, where the partial ordering is \subseteq . The idea is to use C to study D .

We'll do this by constructing a Galois correspondence

i.e. order-preserving maps obeying

$$L_G \subseteq F \iff G \supseteq RF$$



What's R ?

It maps gadgets $k \subseteq F \subseteq K$ to subgroups of the Galois group $G(K|k)$

It works as follows:

$$RF = \{g \in \text{Aut}(K) : g \text{ fixes } F\}$$

To show $R: D^{\text{op}} \rightarrow C$ is order preserving (i.e. a functor) we need:
 $k \subseteq F \subseteq F' \subseteq K \Rightarrow R(F) \supseteq R(F')$

This is true: that if g fixes F' & $F \subseteq F'$ then g fixes F .

What's L ?

L maps subgroups $G \subseteq G(K|k)$ to gadgets between k & K .

L works as follows

$$\begin{aligned} LG &= \{x \in K : G \text{ fixes } x\} \\ &= \{x \in K : \forall g \in G \text{ } g \text{ fixes } x\} \end{aligned} \quad \text{Note: this is a subgadget of } K!$$

To show $L: C \rightarrow D^{\text{op}}$ is order-preserving we need:

$$G \subseteq G' \subseteq G(K|k) \Rightarrow LG \supseteq LG'$$

This is true: it says that if $x \in F$ is fixed by all $g \in G'$ then it's fixed by all $g \in G$ (some $G \subseteq G'$)

Next: why is $L: C \rightleftarrows D^{\text{op}}: R$ a Galois connection?

i.e., why is $LG \subseteq F \iff G \supseteq RF$

$LG \subseteq F$ means every element of F is fixed by G .

$G \supseteq RF$ means everything fixing F is in G .

These are just two ways of saying the same thing.

Now we can relate nice subgadgets $K \subseteq F \subseteq K$ & nice subgroups $G \subseteq G(K|k)$
 using the theorem we saw last time...

but now let's stick in an "op":

Thm Suppose $L: C \rightleftarrows D^{\text{op}}: R$ is a Galois connection. Define

$$\bar{c} = RLc \quad c \in C$$

$$\bar{d} = LRd \quad d \in D^{\text{op}}$$

These are closure operators: $c \leq \bar{c}$ & $\bar{\bar{c}} = \bar{c}$
 $d \leq \bar{d}$ & $\bar{\bar{d}} = \bar{d}$ (when \leq is ordering on D)

We say $c \in C$ is closed if $c = \bar{c}$, and similarly for $d \in D$. L & R give a 1-1 correspondence between closed elements of C & closed elements of D .

[If we would have done C^{op} instead, we would get open operators.]

In our application, what's a "closed" subgadget $k \subseteq F \subseteq K$?

It's one with $F = LRF$

$$= L \{ g \in \text{Aut}(G) : g \text{ fixes } F \}$$

$$= \{ x \in K : x \text{ is fixed by all } g \text{ that fixes } F \}$$

So a subgadget F is closed if it contains all $x \in K$ that are fixed by all $g \in G(K|k)$ that fix F .

What's a "closed" subgroup $G \subseteq G(K|k)$?

$$G = RLG$$

$$= R \{ x \in K : x \text{ is fixed by } G \}$$

$$= \{ g \in G(K|k) : gx = x \text{ for all } x \text{ fixed by } G \}$$

So: a subgroup G is closed if it's the group of all $g \in G(K|k)$ that fix all x fixed by G .

So: the hard part of Galois theory includes:

1) finding a more concrete characterization of the "closed" subfields
 $k \subseteq F \subseteq K$

2) Similarly for the closed subgroups

3) Understanding the poset \mathcal{C} — the poset of the Galois groups.