10/26/15

Galois Theory

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

e.g. monoids, $\overset{+,-,0}{\text{groups}}$, $\overset{+,\times,0,1}{\text{rings}}$, 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 $\mathrm{Aut}(K)$ of "automorphisms", i.e. 1-1 & onto functions $g: K \to K$ that preserve all the operations,

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 <u>fixed</u> by $g \in \mathrm{Aut}(K)$ if $gx = x$.

We say a subgadget $F \subseteq K$ is <u>fixed</u> by $g \in \mathrm{Aut}(K)$ if $gx = x$ for each $x \in F$.

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

The subgroup of $\mathrm{Aut}(K)$ fixing the subgadget $k \subseteq K$ is called the <u>Galois group</u> $G(K|k)$.

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 $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$

i.e. order-preserving maps obeying

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

What's R?

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

It works as follows:

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

To show $R: D^{op} \longrightarrow C$ 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?

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

It works as follows

$LG = \{x \in K : G \text{ fixes } x\}$

$= \{x \in K : \forall g \in G \;\; g \text{ fixes } x\}$ ← Note: this is a subgadget of K!

To show $L: C \longrightarrow D^{op}$ 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 $L: C \rightleftarrows D^{op}: R$ a Galois connection?

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

$LG \subseteq F$ means everything (every element of K) fixed by G is in F

$G \supseteq RF$ 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".

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

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

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

These are <u>closure</u> <u>operators</u>: $c \le \bar{c}$ & $\bar{c} = \bar{\bar{c}}$

$d \le \bar{d}$ & $\bar{d} = \bar{\bar{d}}$ (when $\le$ 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 $F = LRF$

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

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

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 C — the poset of the Galois groups.