10/26/15

Galois Theory

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

E.g. monoids — unary operation

groups $\cdot$, $^{-1}$, 1 — 0-ary operations (constants)

rings $+$, $\cdot$, $0, 1$

fields — binary operations

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 $Aut(K)$ of "automorphisms", i.e. 1-1 & onto functions $g: K \to K$ that preserve all the operations,

e.g. (for rings)
$$g(x+y) = gx + gy$$
$$g(xy) = (gx)(gy)$$
$$g(0) = 0$$
$$g(1) = 1$$

We say an element $x \in K$ is <u>fixed</u> by $g \in Aut(K)$ if $gx = x$.
We say a subgadget $F \subseteq K$ is <u>fixed</u> by $g \in Aut(K)$ if $gx = x$ for each $x \in F$.
Notice: the subset $\{g \in Aut(K) : g \text{ fixes } F\}$ is a subgroup of $Aut(K)$.

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

$$\begin{tikzcd} C \arrow[r, bend left, "L"] & D^{op} \arrow[l, bend left, "R"] \end{tikzcd}$$

i.e. order-preserving maps obeying $LG \subseteq F \Leftrightarrow G \supseteq RF$.

What's R? It maps gadgets $k \subseteq F \subseteq K$ to subgroups of $G(K|k)$. It works as follows:

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

To show $R: D^{op} \to C$ is order-preserving (i.e. a functor) we need:

$$k \subseteq F \subseteq F' \subseteq K \implies R(F) \supseteq R(F')$$

This is true: it says that if g fixes F' and $F \subseteq F'$, then g fixes F.

What's L? It maps subgroups of $G(K|k)$ to gadgets $k \subseteq F \subseteq K$.
It works as follows: (Note: This is a subgadget of K!

$$LG = \{ x \in K : G \text{ fixes } x \} := \{ x \in K : \forall g \in G,\ g \text{ fixes } x \}.$$

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

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

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

Next: Why is $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$ a Galois correspondence?

I.e., why is $LG \subseteq F \Leftrightarrow G \supseteq RF$

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

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

These are 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 from last time... but let's throw in an "op" this time:

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

Define $\bar{c} = RLc \quad c \in C$
$\bar{d} = LRd \quad d \in D^{(op)}$.

These are <u>closure operators</u>: $c \le \bar{c}$ & $\bar{c} = \bar{\bar{c}}$
and $d \le \bar{d}$ & $\bar{d} = \bar{\bar{d}}$. (where $\le$ is ordering on D)

We say $c \in C$ is <u>closed</u> if $\bar{c} = c$, and similarly for $d \in D^{(op)}$.
L & R give a 1-1 correspondence between the closed elements of C and closed elements of D.

In our application, what's a "closed" subgadget $k \subseteq F \subseteq K$?
It's one with $F = LRF = L\{g \in \mathrm{Aut}(G) : g \text{ fixes } F\}$
$= \{x \in K : x \text{ is fixed by all } g \text{ fixing } F\}$

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

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

$$G = RLG$$
$$= R\{x \in K : x \text{ is fixed by } G\}$$
$$= \{g \in G(K|k) : g \text{ fixes } x \ \forall x \text{ fixed by } G\}$$

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 Gälois 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 — poset of subgroups of the Galois groups.