Galois Theory

Suppose you have any kind of algebraic gadget - a set with some operations obeying some axioms. For example: monoids, groups, rings, fields. Then we can define a "subgadget" of a gadget K to be a subset $k \subseteq K$ which is closed under all the operations.

The gadgets F such that $k \subseteq F \subseteq K$ 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 $g: K \to K$ which preserve all the operations. For example, $g(x+y) = g(x) + g(y)$, $g(xy) = g(x)g(y)$, $g(0) = 0$, $g(1) = 1$ when K is a ring. We say an element $x \in K$ is fixed by $g \in \mathrm{Aut}(K)$ if $g(x) = x$. We say a subgadget $F \subseteq K$ is fixed by $g \in \mathrm{Aut}(K)$ if $g(x) = x$ for each $x \in F$. Notice 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 Galois group $G(K|k)$.

Let C be the poset of subgroups of $G(K|k)$ with the partial order $\subseteq$. 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 $R: D^{op} \to C$ is order-preserving (i.e. a functor), we need: $k \subseteq F \subseteq F' \subseteq K \Rightarrow RF \supseteq RF'$. This is true: it says 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: $LG = \{x \in K : G \text{ fixes } x\} := \{x \in K : \forall g \in G, g \text{ fixes } x\}$. To show $L: C \to D^{op}$ 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 $g \in G$.

Next, why is $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$ a Galois connection? That is, why is $LG \subseteq F \Leftrightarrow G \supseteq RF$? $LG \subseteq F$ means every element of K fixed by G is in F. $G \supseteq RF$ means every element of $\mathrm{Aut}(K)$ 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 $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$ is a Galois connection. Define $\bar{c} = RLc$ $\forall c \in C$ & $\bar{d} = LRd$ $\forall d \in D$. These are <u>closure operators</u>: $c \le \bar{c}$ & $\bar{c} = \bar{\bar{c}}$ and $d \le \bar{d}$ & $\bar{d} = \bar{\bar{d}}$. We say $c \in C$ is <u>closed</u> if $c = \bar{c}$ & similarly for $d \in D$. L & R give a 1-1 correspondence between closed elements of C & closed elements of D.

In our application, what's a "closed" subgadget $k \subseteq F \subseteq K$? It's one with $F = LRF = L\{g \in \mathrm{Aut}(G) : g \text{ fixes } F\} = \{x \in K : x \text{ is fixed by all } g \text{ that fix } F\}$. 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 $G \subseteq G(K|k)$? It's one with $G = RLG = R\{x \in K : G \text{ fixes } x\} = \{g \in \mathrm{Aut}(K) : g \text{ fixes all } x \in K \text{ fixed by } G\}$. So, a subgroup G is closed if it's the group of all $g \in \mathrm{Aut}(K)$ that fix all $x \in K$ fixed by G.

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 of subgroups of the Galois group

* Pf of Thm – We know: $c \le c' \Rightarrow Lc \ge Lc'$; $d \ge d' \Rightarrow Rd \le Rd'$; & $Lc \ge d \Leftrightarrow c \le Rd$.
(1) $Lc \ge Lc \Rightarrow c \le RLc = \bar{c}$; (2) $Rd \le Rd \Rightarrow \bar{d} = LRd \ge d$; (3) $\bar{c} \le \bar{\bar{c}}$ by (1) & $RLc \ge RLc \Rightarrow LRLc \ge Lc \Rightarrow RLRLc \le RLc \Rightarrow \bar{\bar{c}} \ge \bar{c} \Rightarrow \bar{c} = \bar{\bar{c}}$; (4) note $L\bar{c} = \overline{Lc}$ & so $c = \bar{c} \Rightarrow Lc = L\bar{c} = \overline{Lc}$. (Apply similar arguments to d.)
(5) $RL\bar{c} = \bar{c}$ & $LR\bar{d} = \bar{d}$ because $\bar{\bar{c}} = \bar{c}$ & $\bar{\bar{d}} = \bar{d}$, so L & R are inverses on closed elements.