Additional notes #8.

Galois Connections.

Definition. Let S and T be classes of objects, and let $R \subseteq S \times T$ be a binary relation from S to T. The *Galois connection determined by* R is the pair of mappings (both denoted $\perp$) defined by

$$\perp : \mathcal{P}(S) \to \mathcal{P}(T) : U \mapsto U^{\perp} = \{t \in T \mid \forall u \in U((u,t) \in R)\}$$

and

$$\perp : \mathcal{P}(T) \to \mathcal{P}(S) : V \mapsto V^{\perp} = \{s \in S \mid \forall v \in V((s,v) \in R)\}.$$

Theorem. Assume that $U \subseteq V \subseteq S$ and $X \subseteq Y \subseteq T$.
(i) $\perp$ reverses inclusions: $U^{\perp} \supseteq V^{\perp}$ and $X^{\perp} \supseteq Y^{\perp}$.
(ii) $\perp\perp$ is increasing: $U \subseteq U^{\perp\perp}$ and $X \subseteq X^{\perp\perp}$.
(iii) $\perp\perp\perp=\perp$: $U^{\perp} = U^{\perp\perp\perp}$ and $X^{\perp} = X^{\perp\perp\perp}$.
(iv) The operations

$$\mathsf{cl} : \mathcal{P}(S) \to \mathcal{P}(S) : U \mapsto U^{\perp\perp}$$

and

$$\mathsf{cl} : \mathcal{P}(T) \to \mathcal{P}(T) : U \mapsto U^{\perp\perp}$$

are closure operators.
(v) A set is closed if and only if it is in the image of $\perp$.
(vi) If $\mathcal{L}_S$ is the lattice of closed subsets of S and $\mathcal{L}_T$ is the lattice of closed subsets if T, then $\perp : \mathcal{L}_S \to \mathcal{L}_T$ is an order-reversing bijection.

Proof. (i) and (ii) are easy. We show how to derive (iii)–(vi) from (i) and (ii).

For (iii), apply $\perp$ to the inclusion in (ii) and use part(i) to get $U^{\perp} \supseteq U^{\perp\perp\perp}$. But by part (ii) we have $U^{\perp} \subseteq (U^{\perp})^{\perp\perp}$. Hence $U^{\perp} = U^{\perp\perp\perp}$.

For (iv), we have that $\perp\perp$ is extensive from (ii). To prove that $\perp\perp$ is isotone we use (i) twice:

$$U \subseteq V \Longrightarrow U^{\perp} \supseteq V^{\perp} \Longrightarrow U^{\perp\perp} \subseteq V^{\perp\perp}.$$

For idempotence we $\perp$ the equation from (iii) to get

$$U^{\perp\perp} = U^{\perp\perp\perp\perp} = (U^{\perp\perp})^{\perp\perp}.$$

For (v), note that any closed set is in the image of $\perp$, since $U = U^{\perp\perp}$ implies that U is the result of applying $\perp$ to $U^{\perp}$. Conversely, if $U = W^{\perp}$, then

$$U^{\perp\perp} = W^{\perp\perp\perp} = W^{\perp} = U,$$

so U is closed.

(vi) follows from (v), (iii), and (i). $\square$

Examples.

(1) Let $\mathcal{S}$ be the class of all algebras defined with operations $\cdot, {}^{-1}, 1$. Let $\mathcal{T}$ be the collection of all equations involving only these operation symbols. Let R denote the relation of satisfaction. (This means that $(\mathbf{A}, \varepsilon)$ is in R if and only if $\mathbf{A} \models \varepsilon$, which is a way of writing that the algebra $\mathbf{A}$ satisfies the equation ε.)

In this example, $\{x \cdot (y \cdot z) = (x \cdot y) \cdot z, x \cdot 1 = x, x \cdot x^{-1} = 1\}^{\perp}$ is the class of all groups. More generally, if $\Sigma \subseteq \mathcal{T}$, then $\Sigma^{\perp}$ is the variety of all algebras satisfying the equations in Σ.

If $\mathcal{K} \subseteq \mathcal{S}$, then $\mathcal{K}^{\perp}$ is the set of all equations that hold in all members of $\mathcal{K}$. This set of equations is called *the equational theory of* $\mathcal{K}$.

The lattice of closed subclasses of $\mathcal{S}$ is the lattice of all varieties of algebras defined with operations $\cdot, {}^{-1}, 1$. The lattice of closed subsets of $\mathcal{T}$ is the lattice of equational theories in this language. These lattices are dual to each other.

(2) Let S be a set and let G be a group of permutations of S. The relation $R = \{(s, g) \mid g(s) = s\}$ determines a Galois connection between S and G.

If $s \in S$, then $\{s\}^{\perp}$ is the stabilizer subgroup of s. If $g \in G$, then $\{g\}^{\perp}$ is the set of fixed points of g.

The Galois Connection of Galois Theory

Let $\mathbb{F} < \mathbb{E}$ be a finite extension. Let $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ be the group of all $\mathbb{F}$-linear automorphisms of $\mathbb{E}$. Let $R \subseteq \mathbb{E} \times G$ be the relation $R = \{(e, g) \mid g(e) = e\}$. This relation determines a Galois connection between $\mathbb{E}$ and G.

Exercises.

(1) Show that a field automorphism $\sigma : \mathbb{E} \to \mathbb{E}$ is $\mathbb{F}$-linear (i.e., satisfies $\sigma(f \cdot e) = f \cdot \sigma(e)$ for $f \in \mathbb{F}$ and $e \in \mathbb{E}$) if and only if $\sigma(f) = f$ for all $f \in \mathbb{F}$.

(2) Show that any closed subset of $\mathbb{E}$ is a subfield of $\mathbb{E}$ containing $\mathbb{F}$.

(3) Show that any closed subset of G is a subgroup.

Fundamental Theorem of Galois Theory. If $\mathbb{F} < \mathbb{E}$ is a finite, normal, separable extension, then every subgroup of $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is closed, and every intermediate subfield $\mathbb{F} < \mathbb{K} < \mathbb{E}$ is closed.