Foundations of mathematics

Sylvain Poirier
http://settheory.net/

5. Galois connections

The notion of Galois connection was introduced in 2.11 (see http://settheory.net/set2.pdf) with its first properties. Let us develop and use them further.

For all $(\bot, \top) \in \mathrm{Gal}(E, F)$ and all $f \in E^G, g \in F^G$, we have $f \leq \top \circ g \Leftrightarrow g \leq \bot \circ f$.

Monotone Galois connections

The permutation $\complement_Y$, reversing the inclusion order in $F = \mathcal{P}(Y)$, adapts the fundamental example to monotone Galois connections: any $R \subset X \times Y$ defines an $(u, v) \in \mathrm{Gal}^+(\mathcal{P}(X), \mathcal{P}(Y))$ by

$$\forall A \subset X, u(A) = \{y \in Y | \exists x \in A, x\ R\ y\} = \bigcup_{x \in A} \overrightarrow{R}(x) = R_*(A) \qquad \overrightarrow{R}(x) = u(\{x\}) \qquad u(\emptyset) = \emptyset$$
$$\forall B \subset Y, v(B) = \{x \in X | \overrightarrow{R}(x) \subset B\} = \overrightarrow{R}^*(\mathcal{P}(B)) \qquad \overleftarrow{R}(y) = \complement_X v(\complement_Y \{y\}) \quad v(Y) = X$$

Indeed, $\forall A \subset X, \forall B \subset F, A \subset v(B) \Leftrightarrow (\forall x \in A, \overrightarrow{R}(x) \subset B) \Leftrightarrow u(A) \subset B$.

The case $R = \mathrm{Gr}\, f$ where $f \in Y^X$ gives $(f_*, f^*) \in \mathrm{Gal}^+(\mathcal{P}(X), \mathcal{P}(Y))$.

The case $R = {}^t\mathrm{Gr}\, g$ where $g \in X^Y$ gives $(g^*, \complement_X \circ g_* \circ \complement_Y) \in \mathrm{Gal}^+(\mathcal{P}(X), \mathcal{P}(Y))$.

Proposition. *Let E, F, G three ordered sets, $(u, v) \in \mathrm{Gal}^+(E, F)$, and $(u', v') \in \mathrm{Gal}(F, G)$ (resp. $\mathrm{Gal}^+(F, G)$). Then $(u' \circ u, v \circ v') \in \mathrm{Gal}(E, G)$ (resp. $\mathrm{Gal}^+(E, G)$)*

The monotone case is written $\forall x \in E, \forall y \in G, x \leq v(v'(y)) \Leftrightarrow u(x) \leq v'(y) \Leftrightarrow u'(u(x)) \leq y$. □

If $E = \mathcal{P}(X), F = \mathcal{P}(Y), G = \mathcal{P}(Z)$, if (u, v) is associated to $R \subset X \times Y$ and (u', v') to $R' \subset Y \times Z$, then $(u' \circ u, v \circ v')$ is associated to $R'' \subset X \times Z$ defined by:

— Antitone case: $xR''z \Leftrightarrow \overrightarrow{R}(x) \subset \overleftarrow{R'}(z)$, i.e. $\overrightarrow{R''}(x) = \bigcap_{y \in \vec{R}(x)} \overrightarrow{R'}(y)$.

— monotone case: $xR''z \Leftrightarrow \overrightarrow{R}(x) \cap \overleftarrow{R'}(z) \neq \emptyset$, i.e. $\overrightarrow{R''}(x) = \bigcup_{y \in \vec{R}(x)} \overrightarrow{R'}(y)$.

In both cases, if $R = \mathrm{Gr}\, f$ where $f \in Y^X$ then $\overrightarrow{R''} = \overrightarrow{R'} \circ f$.

In the monotone case, if $R' = \mathrm{Gr}\, g$ where $g \in Z^Y$ then $\overrightarrow{R''} = g_* \circ \overrightarrow{R}$.

Proposition. *Let E, F, G three ordered sets, $(u, v) \in \mathrm{Gal}^+(E, F)$, $f \in G^E$, $g \in G^F$.*
1) If f is monotone and $f \circ v \leq g$ then $f \leq g \circ u$.
2) If g is monotone and $f \leq g \circ u$ then $f \circ v \leq g$.

Proofs: 1) $f \leq f \circ v \circ u \leq g \circ u$; 2) $f \circ v \leq g \circ u \circ v \leq g$. □

(Note: both cases are symmetrical, though this symmetry is twisted).

Upper and lower bounds, infimum and supremum

In any ordered set E, the relation $\leq$ itself defines $(+_E, -_E) \in \mathrm{Gal}(\mathcal{P}(E), \mathcal{P}(E))$:

$$\forall A \subset E, +(A) = \{y \in E | \forall x \in A, x \leq y\} = \{y \in E | A \subset \overleftarrow{\leq}(y)\}$$
$$\forall A \subset E, -(A) = \{x \in E | \forall y \in A, x \leq y\} = \bigcap_{x \in A} \overleftarrow{\leq}(x).$$

The elements of $-(A)$ are the *lower bounds of* A, and those of $+(A)$ are the *upper bounds of* A in E.

$+ \circ \overleftarrow{\leq} = \overrightarrow{\leq}$ and $- \circ \overrightarrow{\leq} = \overleftarrow{\leq}$ as $\forall x, y \in E, y \in \overrightarrow{\leq}(x) \Leftrightarrow x \leq y \Leftrightarrow \overleftarrow{\leq}(x) \subset \overleftarrow{\leq}(y) \Leftrightarrow y \in +(\overleftarrow{\leq}(x))$.

In a subset $B \subset E$, $\forall A \subset B, -_B(A) = B \cap -(A) \wedge +_B(A) = B \cap +(A)$.

Any upper bound of A in A is called the *greatest element* (or maximum) of A. Similarly, a *least element* (or minimum) of A, is a lower bound of A in A:

$$x : \max A \Leftrightarrow x \in A \cap +(A) \Leftrightarrow (x \in A \wedge A \subset \overleftarrow{\leq}(x)) \Leftrightarrow x \in +_A(A)$$
$$x : \min A \Leftrightarrow x \in A \cap -(A) \Leftrightarrow (A \subset \overrightarrow{\leq}(x) \wedge x \in A)$$

In particular $x : \max \overleftarrow{\leq}(x)$. Such an element is unique ($\forall A \subset E, !x \in E, x : \max A$) because

$$(x : \max A \wedge y : \max A) \Rightarrow (x \in A \subset \overleftarrow{\leq}(y) \wedge y \in A \subset \overleftarrow{\leq}(x)) \Rightarrow x = y.$$

An *infimum* is the greatest lower bound; a *supremum* is the least upper bound, when they exist:

$$x : \inf A \Leftrightarrow x : \max -(A) \Leftrightarrow x \in -(A) \cap +(-(A))$$
$$x : \sup A \Leftrightarrow x : \min +(A) \Leftrightarrow x \in +(A) \cap -(+(A))$$

We have $x : \min A \Rightarrow x : \inf A$ as $A \subset +(-(A))$. Similarly $x : \max A \Rightarrow x : \sup A$.

If $E = \mathcal{P}(X)$,

$$\bigcup A : \sup A$$
$$\bigcap A : \inf A$$

Proposition. *For any monotone function $f \in F^E$, any $x \in E$ and any $A \subset E$, we have*

$$x : \max A \Rightarrow f(x) : \max f[A]$$
$$x : \min A \Rightarrow f(x) : \min f[A]$$

The proof is easy and left to the reader.

Proposition. $\forall A \subset E, \forall x \in E, x : \inf A \Leftrightarrow \overleftarrow{\leq}(x) = -(A) \Leftrightarrow (\forall y {\in} E, y \leq x \Leftrightarrow A \subset \overrightarrow{\leq}(y))$.

Proof:

$$x \in +(-(A)) \Leftrightarrow -(A) \subset \overleftarrow{\leq}(x)$$
$$x \in -(A) \Leftrightarrow A \subset \overrightarrow{\leq}(x) = +(\overleftarrow{\leq}(x)) \Leftrightarrow \overleftarrow{\leq}(x) \subset -(A) \qquad \square$$

Proposition. $\forall (\perp, \top) \in \mathrm{Gal}(E, F)$,

$$\forall x \in E, \perp(x) : \max \top^*(\overrightarrow{\leq}(x))$$
$$\top^* \circ +_E = -_F \circ \perp_*$$
$$\forall A \subset E, \forall x \in E, x : \sup A \Rightarrow \perp(x) : \inf \perp[A].$$

Proofs:

$$(\perp(x) : \max \overleftarrow{\leq}(\perp(x))) \wedge (\overleftarrow{\leq}(\perp(x)) = \top^*(\overrightarrow{\leq}(x)))$$
$$\top^*(+(A)) = \bigcap_{y \in A} \top^*(\overrightarrow{\leq}(y)) = \bigcap_{y \in A} \overleftarrow{\leq}(\perp(y)) = -(\perp[A])$$
$$x : \sup A \Rightarrow \overleftarrow{\leq}(\perp(x)) = \top^*(\overrightarrow{\leq}(x)) = \top^*(+(A)) = -(\perp[A]) \qquad \square$$

Proposition. *For any closure f on E, denoting $K = \mathrm{Im}\, f$ we have $\forall x \in E$,*

$$f(x) : \min(K \cap \overrightarrow{\leq}(x))$$
$$\forall A \subset K, x : \inf A \Leftrightarrow x : \inf_K A$$

Proofs : $(f, \mathrm{Id}_K) \in \mathrm{Gal}^+(E, K) \Rightarrow (f(x) : \min \mathrm{Id}_K^*(\overrightarrow{\leq}(x)) \wedge (x : \inf_K A \Rightarrow \mathrm{Id}_K(x) : \inf \mathrm{Id}_K[A]))$.
$\forall y \in A, x \leq y \Leftrightarrow f(x) \leq y$ thus $x : \inf A \Rightarrow f(x) \in -(A) = \overleftarrow{\leq}(x)$, but $x \leq f(x)$ thus $x = f(x) \in K$. $\square$

Complete lattices

A *complete lattice* is an ordered set E where each $A \subset E$ has a supremum, denoted $\sup A$, and thus also an infimum $\inf A = \sup -(A)$ (as $-(+(-(A))) = -(A)$). Then E has a minimum $0 = \sup \emptyset = \inf E$, a maximum $1 = \inf \emptyset = \sup E$, $\inf \circ \overrightarrow{\leq} = \mathrm{Id}_E = \sup \circ \overleftarrow{\leq}$, $\overleftarrow{\leq} \circ \inf = -$, $\overrightarrow{\leq} \circ \sup = +$, $\overrightarrow{\leq} \circ \inf = + \circ -$, $\overleftarrow{\leq} \circ \sup = - \circ +$, $(\inf, \overrightarrow{\leq}) \in \mathrm{Gal}(\mathcal{P}(E), E)$, and $(\sup, \overleftarrow{\leq}) \in \mathrm{Gal}^+(\mathcal{P}(E), E)$.

The predicate $x : \sup A$ is rewritten $x = \sup A$. Suprema and infima apply to families:

$$\bigvee_{i \in I} x_i = \sup\{x_i | i \in I\} \qquad \bigwedge_{i \in I} x_i = \inf\{x_i | i \in I\}$$
$$\forall y \in E, \quad \bigvee_{i \in I} x_i \leq y \Leftrightarrow \forall i \in I, x_i \leq y \qquad y \leq \bigwedge_{i \in I} x_i \Leftrightarrow \forall i \in I, y \leq x_i$$

The case of tuples defines operations (the only ones in incomplete lattices):

$$\begin{array}{lcc} \forall x, y \in E, & x \vee y = \sup\{x, y\} & x \wedge y = \inf\{x, y\} \\ \forall z \in E, & x \vee y \leq z \Leftrightarrow ((x \leq z) \wedge (y \leq z)) & z \leq x \wedge y \Leftrightarrow ((z \leq x) \wedge (z \leq y)) \\ & x \vee y \vee z = (x \vee y) \vee z = \sup\{x, y, z\} & x \wedge y \wedge z = (x \wedge y) \wedge z = \inf\{x, y, z\} \end{array}$$

Any set $E = \mathcal{P}(X)$ is a complete lattice where $\sup = \bigcup$ and $\inf = \bigcap$. But $\vee$ and $\wedge$ are not always distributive like $\cup$ and $\cap$. For instance, in the lattice $\{0, 1, x, y, z\}$ where x, y, z are pairwise uncomparable, $x \wedge (y \vee z) = x \wedge 1 = x$ but $(x \wedge y) \vee (x \wedge z) = 0 \vee 0 = 0$.

Between two lattices E, F, $\forall (\perp, \top) \in \mathrm{Gal}(E, F), \forall x, y \in E, \perp(x \vee y) = \perp(x) \wedge \perp(y)$.

(With an monotone function $f \in F^E$, we only have $\sup f[A] \leq f(\sup A)$ and $f(\inf A) \leq \inf f[A]$.)

Theorem. *Let E a complete lattice, F an ordered set, and $f \in F^E$. Then*
— $(\forall A\subset E, f(\sup A) : \inf f[A]) \Leftrightarrow (\exists g\in E^F, (f,g) \in \mathrm{Gal}(E,F)) \Rightarrow (f(0) : \max F) \wedge ((f(1) : \min \mathrm{Im}\, f))$
— $(\forall A \subset E, f(\sup A) : \sup f[A]) \Leftrightarrow (\exists g \in E^F, (f,g) \in \mathrm{Gal}^+(E,F)) \Rightarrow f(0) : \min F$.
— $(\forall A \subset E, f(\inf A) : \inf f[A]) \Leftrightarrow (\exists g \in E^F, (g,f) \in \mathrm{Gal}^+(F,E)) \Rightarrow f(1) : \max F$.

Proof. $\forall y \in F$, let $A_y = \{x \in E | y \leq f(x)\}$, and $g(y) = \sup A_y = \sup \overleftarrow{\leq}(g(y))$. If $f(\sup A) : \inf f[A]$,

$$\begin{aligned}\forall A \subset E, A \subset A_y &\Leftrightarrow (\forall x \in A, y \leq f(x)) \Leftrightarrow y \leq f(\sup A)\\ A_y \subset A_y &\Rightarrow y \leq f(\sup A_y)\\ \overleftarrow{\leq}(g(y)) \subset A_y &\Leftarrow y \leq f(\sup \overleftarrow{\leq}(g(y)))\end{aligned}$$

Finally, $(\forall y \in F, A_y \subset \overleftarrow{\leq}(g(y)) \subset A_y) \Leftrightarrow (f,g) \in \mathrm{Gal}(E,F)$. □

Theorem. *Let X a set, E a complete lattice, $G = \mathrm{Gal}(\mathcal{P}(X), E)$, and $s = (X \ni x \mapsto \{x\})$. Then $G \cong E^X$ by the bijection $\phi = (G \ni (\bot, \top) \mapsto \bot \circ s)$, with inverse $\psi = (E^X \ni f \mapsto (\inf \circ f_*, f^* \circ \overrightarrow{\leq})$.*

Proof: first, $\forall f \in E^X, ((f_*, f^*) \in \mathrm{Gal}^+(\mathcal{P}(X), \mathcal{P}(E)) \wedge (\inf, \overrightarrow{\leq}) \in \mathrm{Gal}(\mathcal{P}(E), E)) \Rightarrow \psi(f) \in G$.
Then, $\forall f \in E^X, \phi(\psi(f)) = \inf \circ f_* \circ s = f$. Finally,
$\forall (\bot, \top) \in G, x\in X, y\in E, x \in \top(y) \Leftrightarrow y \leq \phi(\bot, \top)(x)$. But $(\bot, \top) \mapsto \top$ is injective thus ϕ too. □

Corollary. *For all sets X and Y, $\mathrm{Gal}(\mathcal{P}(X), \mathcal{P}(Y)) \cong \mathcal{P}(Y)^X \cong \mathcal{P}(X \times Y)$.*

A subset F of a complete lattice E is said *stable by infimum* iff $\forall A \subset F, \inf A \in F$. The *stability by supremum* is similarly defined. A set of subsets $F \subset \mathcal{P}(X)$ can similarly be called *stable by unions* (which implies $\emptyset \in F$); *stable by intersections* (including the case $\bigcap \emptyset = X \in F$, for a fixed X).

Proposition. *Let E a complete lattice, and $K \subset E$. The stability of K by infimum is equivalent to the existence of a closure* Cl *with image K, and implies that:*
1) K is a complete lattice where $\forall A \subset K, \inf_K A = \inf_E A$, and $1_K = 1_E (= \inf \emptyset)$.
2) $\forall A \subset K, \sup_K A = \mathrm{Cl}(\sup A)$.
3) $\forall A \subset E, \mathrm{Cl}(\sup A) = \mathrm{Cl}(\bigvee_{x\in A} \mathrm{Cl}(x))$

Proof: $(K$ stable by inf$) \Leftrightarrow (K$ complete lattice and $\forall A \subset K, \mathrm{Id}_K(\inf_K A) = \inf_E \mathrm{Id}_K[A])$
$\Leftrightarrow (\exists \mathrm{Cl} \in K^E, (\mathrm{Cl}, \mathrm{Id}_K) \in \mathrm{Gal}^+(E,K)) \Rightarrow K = \mathrm{Im}\,\mathrm{Cl}$

We easily deduce 1) and 2).

3) $\forall y \in K, \sup A \leq y \Leftrightarrow (\forall x \in A, \mathrm{Cl}(x) \leq y) \Leftrightarrow (\bigvee_{x\in A} \mathrm{Cl}(x)) \leq y$. □

The representation by $\overleftarrow{\leq}$ of any ordered set E as a set of subsets ordered by inclusion, imbeds it to the complete lattice $K = \mathrm{Im}\, -$, stable by intersections, where infimums are intersections. Both coincide if E already is a complete lattice ($\mathrm{Im} \overleftarrow{\leq} = K$), as the construction merely adds the missing infima/suprema (elements of $\mathrm{Im}\, - \setminus \mathrm{Im} \overleftarrow{\leq}$).

As $+ \circ \overleftarrow{\leq} = \overrightarrow{\leq}$ and $\complement_E \circ +$ is a strictly monotone bijection from $\mathrm{Im}\, -$ onto $\mathrm{Im}(\complement_E \circ +)$, the construction is symtrical, giving another presentation of K as set of subsets stable by unions; but both types of stability are not present on the same representation.

But even a strictly monotone function f from E to a complete lattice F conserving infima, may not be extendable to a function from K to F with this property. Indeed there may exist $x, y, z \in E$ where $-\{x,y\} = -\{x,z\}$ but $f(x) \wedge f(y) \neq f(x) \wedge f(z)$.

For all complete lattice F and all set E, the set F^E is a complete lattice, with for any $A \subset F^E$, $\sup A = (x \mapsto \sup\{f(x) | f \in A\})$ and similarly for the infimum.

Proposition. *Let E an ordered set, F a complete lattice, and $\nearrow = (F^E \ni f \mapsto \sup_F \circ f_* \circ \overleftarrow{\leq}_E)$. Then $\nearrow$ is the closure with image the set C of monotone functions from E to F.*

Proof: $\forall f \in F^E, \nearrow f \in C$ as sup, f_* and $\overleftarrow{\leq}$ are all monotone.
Then, $f \leq \nearrow f$ as $\forall x \in E, x \in \overleftarrow{\leq}(x) \Rightarrow f(x) \leq \sup f[\overleftarrow{\leq}(x)] = \nearrow f(x)$.
Finally, $\forall g \in C, \forall x \in E, f \leq g \Rightarrow (\forall y \in \overleftarrow{\leq}(x), f(y) \leq g(y) \leq g(x)) \Rightarrow \sup f[\overleftarrow{\leq}(x)] \leq g(x)$. □

Tarski's Fixed Point Theorem

Let E be a complete lattice in all this section. Let $\forall F \subset E, \forall x \in E, \top_F(x) = F \cap \overrightarrow{\leq}(x)$ so that $(\inf_{|\mathcal{P}(F)}, \top_F) \in \mathrm{Gal}(\mathcal{P}(F), E) \cong E^F \ni \mathrm{Id}_F$. Its closure $\mathrm{Cl}_F = \inf \circ \top_F \in E^E$ is itself a component of $((F \mapsto \mathrm{Cl}_F), \top) \in \mathrm{Gal}(\mathcal{P}(E), E^E) \cong (E^E)^E \ni (y \mapsto (x \mapsto (x \leq y \to y | 1)))$, where

$$\forall f \in E^E, \top(f) = \{y \in E | \forall x \in E, x \leq y \Rightarrow f(x) \leq y\} = \{x \in E | \nearrow f(x) \leq x\} = \top(\nearrow f)$$

Its closure will be written $E^E \ni f \mapsto \lceil f \rceil = \mathrm{Cl}_{\top(f)}$. We have $\nearrow f \leq \lceil \nearrow f \rceil = \lceil f \rceil$.

Proposition. *For any closure $h \in E^E$ we have $\operatorname{Im} h = \top(h)$, and $h = \lceil h \rceil$.*

Proof: (h closure) $\Leftrightarrow$ $(\mathrm{Id} \le h \wedge \operatorname{Im} h \subset \top(h)) \Rightarrow (h, \mathrm{Id}_{\top(h)}) \in \mathrm{Gal}^+(E, \top(h)) \Rightarrow \operatorname{Im} h = \top(h)$.
Other method: $\forall x \in E, (x \le h(x) \wedge h = \nearrow h) \Rightarrow (x \in \operatorname{Fix} h \Leftrightarrow h(x) \le x \Leftrightarrow x \in \top(h))$.
Finally, $\forall x \in E, h(x) : \min(\operatorname{Im} h \cap \overrightarrow{\le}(x))$, thus $h = \mathrm{Cl}_{\operatorname{Im} h} = \lceil h \rceil$. $\square$

Proposition. *$\forall F \subset E, \top(\mathrm{Cl}_F) = \inf[\mathcal{P}(F)]$, and ($F$ is stable by infima) $\Leftrightarrow \top(\mathrm{Cl}_F) = F$.*

Proof. $\top(\mathrm{Cl}_F) = \operatorname{Im} \mathrm{Cl}_F = \operatorname{Im}(\inf_{|\mathcal{P}(F)})$. Then $\inf[\mathcal{P}(F)] \subset F \Leftrightarrow \top(\mathrm{Cl}_F) \subset F \Leftrightarrow (\top(\mathrm{Cl}_F) = F)$. $\square$

Any intersection of subsets of E stable by infima is itself stable by infima.

For all $F \subset E$, the stability of $\inf[\mathcal{P}(F)]$ by infima can also be directly seen in this way : $\forall B \subset \inf[\mathcal{P}(F)], \exists A \subset \mathcal{P}(F), B = \inf[A]$ (namely $A = \{X \subset F | \inf X \in B\}$).

But $(\inf, \overrightarrow{\le}) \in \mathrm{Gal}(\mathcal{P}(E), E)$ thus $\forall B \subset \inf[\mathcal{P}(F)], \inf B = \bigwedge_{X \in A} \inf X = \inf(\bigcup A) \in \inf[\mathcal{P}(F)]$.

Theorem. *Let $g = \nearrow f \in E^E$, $K = \top(f) = \top(g) = \{x \in E | g(x) \le x\}$, $h = \lceil f \rceil = \mathrm{Cl}_K$. Then*
1) $\forall x, y \in E, g(x) \le y \le x \Rightarrow y \in K$
2) $g[K] \subset K$
3) $\inf K : \min \operatorname{Fix} g$. In particular, $\operatorname{Fix} g \neq \emptyset$.
4) $\forall x, z \in E, z \in \top_K(x) \Leftrightarrow (x \vee g(z)) \le z$
5) $\forall x \in E, h(x) = (x \vee g(h(x))) \in \top_K(x)$
6) $h \circ f \le h \circ g \le g \circ h \le h$, that become all equal if f is extensive.

Proofs:
1) $g(x) \le y \le x \Rightarrow g(y) \le g(x) \le y \Rightarrow y \in K$
2) by 1) with $y = g(x)$
3) $\inf K = x \in K \Rightarrow ((g(x) \le x) \wedge (g(x) \in K \subset \overrightarrow{\le}(x))) \Rightarrow x \in \operatorname{Fix} g \subset K \subset \overrightarrow{\le}(x)$.
4) $z \in \top_K(x) \Leftrightarrow (z \in K \wedge (x \le z)) \Leftrightarrow ((g(z) \le z) \wedge (x \le z)) \Leftrightarrow x \vee g(z) \le z$
5) Let $y = x \vee g(h(x))$. Knowing that $(h(x) : \min \top_K(x))$ we have $g(h(x)) \le y \le h(x)$ thus $y \in K$. But $x \le y$ thus $y \in \top_K(x)$ thus $h(x) \le y$, thus $h(x) = y$.
6) $\forall x \in E, x \le h(x) \in K \Rightarrow g(x) \le g(h(x)) \in K \Rightarrow h(g(x)) \le g(h(x)) \le h(h(x)) = h(x)$. $\square$

Notes:
— 5) $\Rightarrow$ 3) by $\inf K = h(0)$; Conversely, 3) applied to $g' = (y \mapsto x \vee g(y))$ gives back 5). Moreover, $g' = \nearrow(y \mapsto (y = 0 \to x \vee f(0) | f(y)))$.
— $\forall f, g \in E^E, \top(g \vee f) = \top(f) \cap \top(g) \subset \top(g \circ f)$.
— If f and g are extensive and g is monotone then $\top(f) \cap \top(g) = \top(g \circ f)$.

Proofs: $\forall y \in \top(f) \cap \top(g), \forall x \in E, x \le y \Rightarrow f(x) \le y \Rightarrow g(f(x)) \le y$ thus $y \in \top(g \circ f)$.
(Id $\le f, g$ monotone) $\Rightarrow (\forall y \in \top(g \circ f), \forall x \le y, g(x) \le g(f(x)) \le y) \Rightarrow \top(g \circ f) \subset \top(g)$.
$\mathrm{Id} \le g \Rightarrow (\forall y \in \top(g \circ f), \forall x \le y, f(x) \le g(f(x)) \le y) \Rightarrow \top(g \circ f) \subset \top(f)$. $\square$

Theorem. *If there are injections $f \in Y^X$ and $g \in X^Y$, then there is a bijection between X and Y.*

Proof: the function $\mathcal{P}(X) \ni A \mapsto \complement_X g[\complement_Y f[A]]$, made of 2 monotone and 2 antitone functions, is monotone thus has a fixed point F. Then g defines a bijection from $\complement_Y f[F]$ onto $\complement_X F$, whose inverse allows to complete $f_{|F}$ into a bijection $X \ni x \mapsto (x \in F \to f(x) | g^{-1}(x))$ from X to Y. $\square$

Transport of closure

Proposition. *Let E and F complete lattices, $(u, v) \in \mathrm{Gal}^+(E, F)$, $B \subset F, f \in E^E, g \in F^F$. Then*
1) $\top_{v[B]} = v_* \circ \top_B \circ u$
2) $\mathrm{Cl}_{v[B]} = v \circ \mathrm{Cl}_B \circ u$
3) $u \circ f \le \mathrm{Cl}_B \circ u \Leftrightarrow v[B] \subset \top(f) \Leftrightarrow u \circ \lceil f \rceil \le \mathrm{Cl}_B \circ u$
4) $\nearrow f \circ v \le v \circ g \Rightarrow u \circ f \le g \circ u \Rightarrow u \circ \nearrow f \le \nearrow(g) \circ u \Rightarrow f \circ v \le v \circ \nearrow g$.
5) $u \circ f \le g \circ u \Rightarrow v[\top(g)] \subset \top(f) \Leftrightarrow u \circ \lceil f \rceil \le \lceil g \rceil \circ u \Leftrightarrow \lceil f \rceil \circ v \le v \circ \lceil g \rceil \Rightarrow u(\lceil f \rceil(0)) \le \lceil g \rceil(0)$.

Proofs: 1) is easy; it implies 2) by $\inf \circ v_* = v \circ \inf$.
3) $u \circ f \le \mathrm{Cl}_B \circ u \Leftrightarrow f \le v \circ \mathrm{Cl}_B \circ u = \mathrm{Cl}_{v[B]} \Leftrightarrow v[B] \subset \top(f)$. Or more direcly:
$(\forall x \in E, \forall y \in B, u(x) \le y \Rightarrow u(f(x)) \le y) \Leftrightarrow (\forall y \in B, \forall x \in E, x \le v(y) \Rightarrow f(x) \le v(y))$.
The second equivalence is deduced by $\top(f) = \top(\lceil f \rceil)$.
4) $\mathrm{Id} \le v \circ u \Rightarrow f \le \nearrow f \circ v \circ u \le v \circ g \circ u$. Then, $f \le v \circ \nearrow(g) \circ u \Leftrightarrow \nearrow f \le v \circ \nearrow(g) \circ u$.
Hence 5). $\square$

Case of $E = \mathcal{P}(X)$

Then $E^E = \mathcal{P}(X)^E \cong \mathcal{P}(E \times X)$, so that the Galois connection $((F \mapsto \mathrm{Cl}_F), \top)$ comes from the relation between E and $E \times X$, defined by $(A, (B, x)) \mapsto (B \subset A \Rightarrow x \in A)$.

Proposition. *Let X, Y two sets, $f \in \mathcal{P}(X)^{\mathcal{P}(X)}, g \in \mathcal{P}(Y)^{\mathcal{P}(Y)}$ and $u \in Y^X$. Then*
(1) $\forall P \subset \mathcal{P}(Y), \forall A \subset X, \mathrm{Cl}_{u^*[P]}(A) = u^*(\mathrm{Cl}_P(u[A]))$
(2) $(\forall A \subset X, u[f(A)] \subset g(u[A])) \Rightarrow (\forall B \in \top(g), u^*(B) \in \top(f)) \Leftrightarrow \forall A \subset X, u[\lceil f\rceil(A)] \subset \lceil g\rceil(u[A])$
$\Leftrightarrow \forall B \subset Y, \lceil f\rceil(u^*(B)) \subset u^*(\lceil g\rceil(B))$
(3) $(\forall A \subset X, g(u[A]) \subset u[f(A)]) \Rightarrow (\forall A \in \top(f), u[A] \in \top(g)) \Leftrightarrow \forall A \subset X, \lceil g\rceil(u[A])) \subset u[\lceil f\rceil(A)]$
(4) $(\forall B \subset Y, u^*(g(B)) \subset f(u^*(B))) \Rightarrow \forall B \subset Y, u^*(\lceil g\rceil(B)) \subset \lceil f\rceil(u^*(B))$.

Proof: formulas (1), (2) and (4) are deduced from the above; we verify (3) by
$\forall A \in \top(f), \forall B \subset u[A], \quad g(B) = g(u[A \cap u^*(B)]) \subset u[f(A \cap u^*(B))] \subset u[A]$
$\forall A \subset X, \quad ((u[\lceil f\rceil(A)] \in \top(g)) \wedge (u[A] \subset u[\lceil f\rceil(A)])) \Rightarrow (\lceil g\rceil(u[A]) \subset u[\lceil f\rceil(A)])$. □

Proposition. *Let $E = \mathcal{P}(X)$, $f \in E^E$, $A \in E$ and $f_A = (\mathcal{P}(A) \ni B \mapsto f(B) \cap A)$. Then*

$$\forall B \in \top(f), A \cap B \in \top(f_A)$$
$$\forall B \subset A, \lceil f_A\rceil(B) \subset \lceil f\rceil(B)$$
$$\forall B \in E, \lceil f_A\rceil(A \cap B) \subset \lceil f\rceil(B).$$

If moreover $A \in \top(f)$ then $\top(f_A) = \top(f) \cap \mathcal{P}(A)$, and $\lceil f_A\rceil = \lceil f\rceil_{|\mathcal{P}(A)}$.

Preorder generated by a relation

For any sets E, F, any $f \in F^E$ and any relation R of preorder on F, the preimage of R by f, defined by $(x, y) \mapsto (f(x)\ R\ f(y))$, is a preorder on E. It is the only preorder on E for which f is strictly monotone from E to F.

Notations. *Let $E = \mathcal{P}(X)$ and $\mathcal{B}_X = \mathcal{P}(X \times X)$. Let $(\lambda, \rho) \in \mathrm{Gal}^+(\mathcal{B}_X, E^E)$ associated with the injection $X \times X \ni (x, y) \mapsto (\{x\}, y) \in E \times X$, namely*

$$\forall R \in \mathcal{B}_X, \forall x \in X, \lambda(R)(\{x\}) = \overrightarrow{R}(x)$$
$$\lambda(R)(A) = \emptyset \text{ if } A \text{ is not a singleton}$$
$$\forall f \in E^E, \forall x, y \in X, \rho(f)(x, y) \Leftrightarrow y \in f(\{x\}).$$

Then let $(\mathrm{Cut}, \mathrm{Pre}) \in \mathrm{Gal}(\mathcal{B}_X, \mathcal{P}(E))$ associated with the relation $\{((x, y), A) \in (X \times X) \times E | x \in A \Rightarrow y \in A\}$:

$$\mathrm{Cut}(R) = \top(\lambda(R)) = \{A \in E | \forall x, y \in X, (x\ R\ y \wedge x \in A) \Rightarrow y \in A\} = \{A \subset X | \bigcup_{x \in A} \overrightarrow{R}(x) \subset A\}.$$

$$\mathrm{Pre}(F) = \rho(\mathrm{Cl}_F) = \{(x, y) \in X^2 | \forall A \in F, x \in A \Rightarrow y \in A\}$$
$$\overrightarrow{\mathrm{Pre}(F)}(x) = \bigcap\{A \in F | x \in A\}.$$

These notions show a new symmetry: $\forall R \in \mathcal{B}_X, \mathrm{Cut}({}^tR) = \complement_X[\mathrm{Cut}(R)]$. Thus,

$$\overleftarrow{\mathrm{Pre}(F)}(x) = \bigcap\{B \in E | \complement_X B \in F \wedge x \in B\} = \complement_X \bigcup\{A \in F | x \notin A\}$$

Theorem. *The set $\mathrm{Im}\,\mathrm{Pre}$ of closed elements of $\mathcal{B}_X$ is the set of preorders on X.*

Proof: for all set Y, $\forall R \subset Y \times X, \forall x, y \in X$,

$$\mathrm{Pre}(\mathrm{Im}\,\overrightarrow{R})(x, y) \Leftrightarrow (\forall A \in \mathrm{Im}\,\overrightarrow{R}, x \in A \Rightarrow y \in A) \Leftrightarrow (\forall z \in Y, x \in \overrightarrow{R}(z) \Rightarrow y \in \overrightarrow{R}(z))$$
$$\Leftrightarrow (\forall z \in Y, z \in \overleftarrow{R}(x) \Rightarrow z \in \overleftarrow{R}(y)) \Leftrightarrow \overleftarrow{R}(x) \subset \overleftarrow{R}(y).$$

Thus $\forall F \subset \mathcal{P}(X)$, letting $Y = F$ and $\overrightarrow{R} = \mathrm{Id}_F$, (i.e. $R = {}^t\!\in$), we have $\mathrm{Pre}(F) = \mathrm{Pre}(\mathrm{Im}\,\overrightarrow{R})$, preorder given as preimage by $\overleftarrow{R}$ of inclusion.

Conversely, with $Y = X$, any preorder R on X is $= \mathrm{Pre}(\mathrm{Im}\,\overrightarrow{R}) \in \mathrm{Im}\,\mathrm{Pre}$. □

Definition. *For any binary relation R on a set X, the* preorder generated by R*, denoted $\lceil R\rceil$, is the relation $\mathrm{Pre}(\mathrm{Cut}(R))$, which is the smallest of all preorders greater than R.*

Proposition. $\forall F \subset E, \forall A \in E, A \in \mathrm{Cut}(\mathrm{Pre}(F)) \Leftrightarrow \bigcup_{x \in A} \bigcap\{B \in F | x \in B\} = A$.

Proof:

$$A \in \mathrm{Cut}(\mathrm{Pre}(F)) \Leftrightarrow \bigcup_{x \in A} \overrightarrow{\mathrm{Pre}(F)}(x) \subset A$$
$$\Leftrightarrow \bigcup_{x \in A} \bigcap\{B \in F | x \in B\} \subset A$$

The other inclusion comes from $\forall x \in A, x \in \overrightarrow{\mathrm{Pre}(F)}(x)$. □

Theorem. *The set* $\operatorname{Im}\operatorname{Cut}$ *of closed elements of* $\mathcal{P}(E)$ *is the set of parts of* E *both stable by unions and by intersections.*

Proof: $\operatorname{Cut} = \top \circ \lambda \Rightarrow \operatorname{Im}\operatorname{Cut} \subset \operatorname{Im}\top$ thus any element of $\operatorname{Im}\operatorname{Cut}$ is stable by intersections. Symmetrically, it is also stable by unions.
Conversely, if F is stable by unions and intersections then $\operatorname{Cut}(\operatorname{Pre}(F)) \subset F$ by the above proposition, thus F is closed. $\square$

Let us further comment this result: starting from any $F \subset E = \mathcal{P}(X)$, we might consider the set of intersections of its parts, that would be stable by intersections. But we only take those of $\operatorname{Im}\overrightarrow{\operatorname{Pre}(F)}$. Then, we take a set $\operatorname{Cut}(\operatorname{Pre}(F))$ of elements each equal to the union of a part of $\operatorname{Im}\overrightarrow{\operatorname{Pre}(F)}$. And what is remarkable, is that this set $\operatorname{Cut}(\operatorname{Pre}(F))$ includes F and is both stable by unions and by intersections, thus is the smallest set stable by unions and by intersections that includes F. (It is thus also the set of all unions of intersections of parts of F.)

This property of any $\mathcal{P}(X)$, does not generalize to other complete lattices. In any complete lattice E, there is indeed for any $F \subset E$ a smallest set stable by suprema and suprema that includes F, just like any set $\top(f) \cap \top(g)$ of elements both closed for closures f and g is that $\top(g \circ f)$ of closed elements for a third closure $h = \lceil g \circ f \rceil$. But this $g \circ f$ that is here $F \mapsto \sup[\mathcal{P}(\inf[\mathcal{P}(F)])]$, needs not be a closure. Indeed a finite lattice can easily be found, with a part stable by infima but the set of its suprema is not stable by infima.

As a particular case of the previous remarks, any intersection of unions is also an union of intersections. Formally,

$$B = \bigcap_i \bigcup_{j \in J_i} A_{ij} \Rightarrow B = \bigcup_{x \in B} \bigcap_{(i,j) \in C_x} A_{ij} \text{ where } C_x = \{(i,j) \in \coprod_i J_i | x \in A_{ij}\}$$

This formula can be directly checked once translated from the formalism of sets to that of formulas:

$$(\forall y \exists z, A(x,y,z)) \Leftrightarrow (\exists x', (\forall y \exists z, A(x',y,z)) \wedge \forall y \forall z (A(x',y,z) \Rightarrow A(x,y,z))).$$

Let us see how the fixed point theorem applies here.

Let $R \in \mathcal{B}_X$, $f = \lambda(R) \in E^E$. The function $g = \nearrow f$ is now written

$$\forall A \in E, \qquad g(A) = \bigcup_{x \in A} \overrightarrow{R}(x)$$

$$\forall A \in E, \forall y \in X, \qquad y \in g(A) \Leftrightarrow (\exists x \in A, x \; R \; y) \Leftrightarrow A \cap \overleftarrow{R}(y) \neq \emptyset.$$

Then, let $h = \lceil f \rceil = \operatorname{Cl}_{\operatorname{Cut} R} \in (\operatorname{Cut} R)^E$. As $\operatorname{Cut} R$ is stable by unions,

$$\forall A \in E, \bigcup_{x \in A} h(\{x\}) \in \operatorname{Cut} R.$$

With $h(\{x\}) = \overrightarrow{\lceil R \rceil}(x)$, and applying to $A = \bigcup_{x \in A}\{x\}$ the formula $\operatorname{Cl}(\sup A) = \operatorname{Cl}(\bigvee_{x \in A} \operatorname{Cl}(x))$ we get

$$h(A) = \lceil R \rceil_* (A).$$

The fixed point theorem then says $\forall A \in E, h(A) = A \cup g(h(A))$. In particular,

$$\forall x, y \in X, x \lceil R \rceil y \Leftrightarrow (x = y \vee \exists z \in X, x \lceil R \rceil z \wedge z \; R \; y).$$

For any sets X, Y, $R \in \mathcal{B}_X, S \in \mathcal{B}_Y$, and $u \in Y^X$,

$$\begin{aligned}
\forall B \subset \mathcal{P}(Y), \forall x, y \in X, \operatorname*{Pre}_X(u^*[B])(x,y) &\Leftrightarrow \operatorname*{Pre}_Y(B)(u(x), u(y)) \\
(\forall x, y \in X, xRy \Rightarrow u(x) \lceil S \rceil u(y)) &\Rightarrow u^*[\operatorname{Cut}(S)] \subset \operatorname{Cut}(R) \\
&\Rightarrow \forall x, y \in X, x \lceil R \rceil y \Rightarrow u(x) \lceil S \rceil u(y) \\
(\forall x \in X, \overrightarrow{S}(u(x)) \subset u[\overrightarrow{R}(x)]) &\Rightarrow u_*[\operatorname{Cut}(R)] \subset \operatorname{Cut}(S) \\
&\Rightarrow (\forall x \in X, \overrightarrow{\lceil S \rceil}(u(x)) \subset u[\overrightarrow{\lceil R \rceil}(x)]) \\
(\forall x \in X, \overleftarrow{S}(u(x)) \subset u[\overleftarrow{R}(x)]) &\Rightarrow u_*[\operatorname{Cut}({}^tR)] \subset \operatorname{Cut}({}^tS) \\
&\Rightarrow (\forall x \in X, \overleftarrow{\lceil S \rceil}(u(x)) \subset u[\overleftarrow{\lceil R \rceil}(x)]).
\end{aligned}$$

The second formula can also be obtained this way:

$\lceil S \rceil$ is a preorder on Y thus $(x,y) \mapsto (u(x) \lceil S \rceil u(y))$ is a preorder on X, that must be greater than R by hypothesis. It is thus also greater than $\lceil R \rceil$ (the smallest preorder greater than R).

Finally, if $X \subset Y$ and R is the restriction of S to X, then $\forall x, y \in X, x \lceil R \rceil y \Rightarrow x \lceil S \rceil y$. If moreover $X \in \operatorname{Cut}(S)$ or $X \in \operatorname{Cut}({}^tS)$ then $\forall x, y \in X, x \lceil R \rceil y \Leftrightarrow x \lceil S \rceil y$.

Finite sets

Definition. *Let X a set, and $\mathcal{S}$ the binary relation on $\mathcal{P}(X)$ defined by*

$$\forall A, B \subset X, A\ \mathcal{S}\ B \Leftrightarrow (A \subset B \wedge \exists! x \in B, x \notin A) \Leftrightarrow \exists x \in X, x \notin A \wedge B = A \cup \{x\}.$$

A subset $A \subset X$ is called finite *iff $\emptyset\ \lceil\mathcal{S}\rceil\ A$; X is a* finite set *iff $\emptyset\ \lceil\mathcal{S}\rceil\ X$ (it is a finite subset of itself). A set that is not finite is called infinite.*

Proof of equivalence (the finiteness of A is independent of X):
$\mathcal{P}(A) \in \mathrm{Cut}({}^t\mathcal{S})$, thus the restriction of $\lceil\mathcal{S}\rceil$ to A is the $\lceil\mathcal{S}\rceil$ on A. □

Let us specify how this notion of finiteness is related to the intuitive one, called *meta-finiteness* (as it coincides with the application of this set theoretical notion of finiteness on the meta level, see 1.7).

Any meta-finite set X is finite: starting from $\emptyset$ then adding one by one each element of X until obtaining X, the finiteness of each of these sets is successively deduced from that of the former. In particular, $\emptyset$ is finite, then singletons and pairs are finite, etc.

Conversely, assume there is a set F exactly containing the meta-finite subsets of X. Then $\emptyset \in F$ and $F \in \mathrm{Cut}(\mathcal{S})$. But the set $\overrightarrow{\lceil\mathcal{S}\rceil}(\emptyset)$ of finite subsets of X is the smallest set with this property, thus must be included in F, so they are equal. But, nothing can ensure F to exist in the universe, by lack of a formal definition of meta-finiteness.

But if X is not meta-finite then neither is $\mathcal{P}(X)$, so that $\mathcal{P}(\mathcal{P}(X))$ might not contain truly all subsets of $\mathcal{P}(X)$, among which the set F of meta-finite elements of $\mathcal{P}(X)$, that has no first-order definition. Thus X might satisfy the formal definition of finiteness "by mistake". This fact of indefinability of finiteness in first-order logic was already seen with the incompleteness of arithmetic and the existence of non-standard models in section 3.

Proposition. *The direct image of a finite set by any function is finite.*

Proof: Let f with domain X fini, and $Y = \operatorname{Im} f$. Then

$$\forall A, B \subset X, A\ \mathcal{S}\ B \Rightarrow (f[A] = f[B] \vee f[A]\ \mathcal{S}\ f[B]) \Rightarrow f[A]\ \lceil\mathcal{S}\rceil\ f[B]$$
$$\emptyset\ \lceil\mathcal{S}\rceil\ X \Rightarrow f[\emptyset]\ \lceil\mathcal{S}\rceil\ f[X] \Rightarrow \emptyset\ \lceil\mathcal{S}\rceil\ Y.$$

Terminology. *A "finite family" is a family indexed by a finite set. Also, a finite operation is an operation on a finite family: for example, a finite product is the product of a finite family of sets (even if these sets may be infinite).*

Theorem. *Let $(E_x, R_x)_{x\in X}$ a finite family where R_x is a binary relation on E_x. On $P = \prod_{x\in X} E_x$, consider the binary relation T, called tensor product of the R_x, defined by*

$$\forall u, v \in P, uTv \Leftrightarrow \exists x \in X, u_x R_x v_x \wedge \forall y \in X, y \neq x \Rightarrow u_y = v_y.$$

Then, $\forall u, v \in P, u\ \lceil T\rceil\ v \Leftrightarrow \forall x \in X, u_x \lceil R_x\rceil v_x$.

Proof. For the direct implication, let $\forall x \in X, \pi_x = (u \mapsto u_x) \in E_x^P$ the canonical surjection.

$$\forall u, v \in P, uTv \Rightarrow (u_x = v_x \vee u_x R_x v_x) \Rightarrow \pi_x(u) \lceil R_x\rceil \pi_x(v)$$
$$\forall u, v \in P, u\ \lceil T\rceil\ v \Rightarrow \pi_x(u)\lceil R_x\rceil \pi_x(v)$$

For the converse, $\forall x \in X, a \in P$, let j_x^a the function from E_x to P defined by

$$\forall b \in E_x, \forall y \in X, j_x^a(b)_y = (b, a_y)(y = x).$$

Then, $\forall w \in P, \forall x \in X, \forall a, b \in E_x, aR_x b \Rightarrow j_x^w(a) T j_x^w(b)$ thus $a\ \lceil R_x\rceil\ b \Rightarrow j_x^w(a)\ \lceil T\rceil\ j_x^w(b)$.

Then, $\forall u, v \in P$, let $\phi \in P^{\mathcal{P}(X)}$ defined by $\phi(A)_x = (v_x, u_x)(x \in A)$. Let $A, B \subset X$ such that $A\ \mathcal{S}\ B$, and $x \in \complement_B A$. Letting $w = \phi(A)$, we get $j_x^w(u_x) = \phi(A)$, $j_x^w(v_x) = \phi(B)$, so that the hypothesis implies $\phi(A)\ \lceil T\rceil\ \phi(B)$. Thus ϕ is monotone from $(\mathcal{P}(X), \lceil\mathcal{S}\rceil)$ to $(P, \lceil T\rceil)$.

We conclude $\phi(\emptyset)\ \lceil T\rceil\ \phi(X)$, where $\phi(\emptyset) = u$ and $\phi(X) = v$. □

Proposition. *In the powerset of a finite set X, $\lceil\mathcal{S}\rceil$ is the inclusion relation.*

This is the application of the theorem to $E_x = \mathcal{P}(\{x\}) \simeq \mathcal{V}$ and $aR_xb \Leftrightarrow (a = \emptyset \wedge b = \{x\})$. Indeed, $P \simeq \mathcal{P}(X)$ which maps T to $\mathcal{S}$, and translates $(\forall x \in X, u_x\lceil R_x\rceil v_x)$ into $A \subset B$. $\square$

Corollary. *If $X \subset Y$ (or if there is an injection from X to Y) and if Y is finite then X is finite.*

Proposition. *For any finite union $U = \bigcup_{x\in X} A_x$, U is finite iff all A_i are finite.*

Proof: first when the A_x are a partition of U, the result expresses the theorem applied to the family of $E_x = \mathcal{P}(A_x)$ with $\mathcal{S}$, where $\mathcal{P}(U) \simeq \prod_{x\in X} \mathcal{P}(E_x)$.

In the general case, if all A_i are finite, then U is finite as an image of the canonical surjection from $\coprod_{x\in X} A_x$ to U. Conversely, if U is finite then $A_x \subset U$ is finite too. $\square$

Corollary. *If X and Y are finite sets then $X \times Y$ is finite.*

Lemma. *Let X a set and $K \subset \mathcal{P}(X)$ such that $\emptyset \in K$, $(\forall x \in X, \{x\} \in K)$ and $(\forall A, B \in K, A \cap B = \emptyset \Rightarrow A \cup B \in K)$. Then K contains all finite subsets of X.*

Proof: Let $A, B \subset X$ such that $A\ \mathcal{S}\ B$. $\exists x \in X, A \cap \{x\} = \emptyset \wedge B = A \cup \{x\} \wedge \{x\} \in K$, so that $(A \in K \Rightarrow B \in K)$. Thus $K \in \mathrm{Cut}(\mathcal{S})$, and $\emptyset \in K$ gives the conclusion. $\square$

Finite Choice Theorem. *For any finite set X, AC_X.*

Proposition. *Any finite product of finite sets is finite.*

Let us deduce in parallel both results from the lemma.
So let $(E_x)_{x\in X}$ a finite family of sets (nonempty, resp. finite).
Let $\forall A \subset X, P_A = \prod_{x\in A} E_x$, and let $K = \{A \subset X | P_A \text{ is finite , resp. } \neq \emptyset\}$.
From $P_\emptyset = \{0\}$ we get $\emptyset \in K$. Then, $\forall x \in X, P_{\{x\}} \simeq E_x$ thus $\{x\} \in K$.
Finally, $\forall A, B \subset X, A \cap B = \emptyset \Rightarrow P_{A\cup B} \simeq P_A \times P_B$ donc $(A \in K \wedge B \in K) \Rightarrow A \cup B \in K$.
But X is finite, thus $X \in K$. $\square$

Theorem. *Let X a set, $E = \mathcal{P}(X)$ and $\mathcal{F} \subset E$ the set of finite subsets of X. Let $f \in E^E$ such that $\forall A \in E, A \in \mathcal{F} \vee f(A) = \emptyset$. Still denoting $\forall A \subset E, f_A = (\mathcal{P}(A) \ni B \mapsto f(B) \cap A)$,*

$$\forall x \in X, x \in \lceil f\rceil(\emptyset) \Leftrightarrow (\exists A \in \mathcal{F}, x \in A \wedge \lceil f_A\rceil(\emptyset) = A)$$
$$\forall B \subset X, \forall x \in X, x \in \lceil f\rceil(B) \Leftrightarrow (\exists A \in \mathcal{F}, x \in A \wedge \lceil f_A\rceil(A \cap B) = A)$$

The latter formula is deduced from the former by replacing $f(\emptyset)$ by $f(\emptyset) \cup B$. As the converse is clear, let us prove the direct implication. Let

$$K = \{x \in X | \exists A \in \mathcal{F}, x \in A \wedge \lceil f_A\rceil(\emptyset) = A\}.$$

For all $B \subset K$ and all $y \in f(B)$, here B is finite. By the finite choice theorem,

$$\exists A \in \mathcal{F}^B, \forall x \in B, x \in A_x \wedge \lceil f_{A_x}\rceil(\emptyset) = A_x.$$

Let $C = \{y\} \cup \bigcup_{x\in B} A_x$. It is finite, as a finite union of finite sets.
$\forall x \in B, \lceil f_{A_x}\rceil(\emptyset) = A_x \subset C$ thus $A_x \subset \lceil f_C\rceil(\emptyset)$.
But $\forall x \in B, x \in A_x$ thus $B \subset C$, and $B \subset \lceil f_C\rceil(\emptyset)$.
But $y \in f_C(B)$ thus $y \in \lceil f_C\rceil(\emptyset)$. Finally $\lceil f_C\rceil(\emptyset) = C$, thus $y \in K$.
We conclude: $\forall B \subset K, f(B) \subset K$, thus $\lceil f\rceil(\emptyset) \subset K$. $\square$

Example: $\forall R \in \mathcal{B}_X, \forall x, y \in X, x\ \lceil R\rceil\ y \Leftrightarrow \exists A \text{ finite} \subset X, x \in A \wedge y \in A \wedge x\ \lceil R_{|A}\rceil\ y$.
On the other hand, we can note that $\forall B \subset A, \nearrow(f_A)(B) = \nearrow f(B) \cap A$.

Corollary. *For any closure h on E, $(\exists f \in E^E, h = \lceil f\rceil \wedge \forall A \in E, A \in \mathcal{F} \vee f(A) = \emptyset) \Leftrightarrow (\forall B \in E, \forall x \in h(B), \exists A \text{ finite} \subset B, x \in h(A))$. Such a closure will be called* finitary.

3.9. Generated equivalence relation, and more

Let $(f_i)_{i\in I}$ a family of functions with domain X, and $f = \prod_{i\in I} f_i \in (\prod_{i\in I} \mathrm{Im}\, f_i)^X$. Then

$$\forall x, y \in X, (f(x) = f(y)) \Leftrightarrow (\forall i \in I, f_i(x) = f_i(y)) \quad \text{i.e.} \underset{f}{\sim} = \inf\{\underset{f_i}{\sim} | i \in I\}.$$

This expresses the fact that the set of equivalence relations on X is stable by infima.

Other method: the set of preorders is stable by infima; similarly for the set of symmetric relations. Thus the infimum of a set of equivalence relations is a symmetric preorder, thus an equivalence relation.

For any binary relation R, we call *equivalence relation generated* by R, the smallest equivalence relation greater than R. It is the preorder generated by $(x, y) \mapsto (xRy \vee yRx)$, (since the preorder generated by a symmetric relation is symmetric).

In the canonical bijection between preorders R on X and sets F of subsets of X stable by unions and intersections, the equivalence relations correspond to the sets F also stable by complementarity ($\complement_X[F] \subset F$, which can also be written $\complement_X[F] = F$).

The notions of generated preorder and generated equivalence relation, are examples of a general notion of a binary relation of a given kind generated by a binary relation R on X, for any kind of binary relation defined by a system of axioms, all of the form : (a conjunction of formulas $R(t, t')$ where t, t' are terms independent of R) implies (another formula $R(t, t')$ for other t, t').

Indeed, such an axioms system corresponds to a function f from $\mathcal{P}(X \times X)$ into itself (or a subset of $\mathcal{P}(X \times X) \times (X \times X)$), and the conformity of a relation to these axiomes means it belongs to $\top(f)$. Moreover, each axiom only using a finite list of conditions, the last theorem says that, denoting R' the relation thus generated by R, any formula $R'(x, x')$ with given x and x', is true iff it has a finite proof where each step consists in deducing, from the truth of premises of some axiom, that of its conclusion.

Later, we shall still generalize this process by replacing the binary relation by a system of relations with any arities between diverse sets.

Proposition. *Let $R \in \mathcal{B}_X$. The smallest transitive relation T greater than R, called the* transitive closure *of R, satisfies*

$$\forall x, y \in X, xTy \Leftrightarrow (\exists z \in X, x\ R\ z \wedge z\ \lceil R \rceil\ y) \Leftrightarrow (\exists z \in X, x\ \lceil R \rceil\ z \wedge z\ R\ y)$$
$$\forall x, y \in X, x\ \lceil R \rceil\ y \Leftrightarrow (xTy \vee x = y).$$

Proof: Let $T' = \{(x, y) | \exists z \in X, x\ R\ z \wedge z\ \lceil R \rceil\ y\}$. Then $\overrightarrow{T'} = \lceil R \rceil_* \circ \overrightarrow{R}$. By definition of $\lceil R \rceil_*$, T' is the smallest relation greater than R such that $g \circ \overrightarrow{T'} < \overrightarrow{T'}$, i.e. that

$$\forall x, y, z \in X, xT'y \wedge yRz \Rightarrow xT'z.$$

But T satisfies both conditions thus $T' \subset T$. The other inequality $T \subset T'$ comes from the transitivity of T': $\forall x, y, z \in X, xT'y \wedge yT'z \Rightarrow xT'y \wedge y\ \lceil R \rceil\ z \Rightarrow xT'z$.

The other equivalence follows by symmtry. The second formula can be directly checked easily (seeing that $(xTy \vee x = y)$ is a preorder), or from the fixed point theorem. □

Well-founded relations

Consider a set X with a binary relation R, $E = \mathcal{P}(X)$, and $\overleftarrow{R}^\bullet \in E^E$:

$$\forall A \subset X, \forall y \in X, y \in \overleftarrow{R}^\bullet(A) \Leftrightarrow \overleftarrow{R}(y) = A.$$

Denote $\mathcal{D}_R = \nearrow(\overleftarrow{R}^\bullet)$, i.e.

$$\forall A \subset X, \forall y \in X, y \in \mathcal{D}_R(A) \Leftrightarrow \overleftarrow{R}(y) \subset A$$
$$\forall A \subset X, A \subset \mathcal{D}_R(A) \Leftrightarrow A \in \mathrm{Cut}({}^tR).$$

It is related to the g defined for generated preorders, by $\mathcal{D}_R = \complement_X \circ g \circ \complement_X$.

Denote $\mathcal{F}_R = \lceil \overleftarrow{R}^\bullet \rceil \in E^E$ the corresponding closure. The relation $x \in \mathcal{F}_R(B)$ between $B \in E$ and $x \in X$ will be read *x is founded on B by R*, and is equivalently expressible by:

$$\forall A \subset X, (B \subset A \wedge \forall y \in X, \overleftarrow{R}(y) \subset A \Rightarrow y \in A) \Rightarrow x \in A$$
$$\forall A \subset \complement_X B, (\forall y \in A, A \cap \overleftarrow{R}(y) \neq \emptyset) \Rightarrow x \notin A$$
$$\forall A \subset \complement_X B, A \subset R_*(A) \Rightarrow x \notin A$$
$$\forall A \subset X, x \in A \wedge A \subset R_*(A) \Rightarrow A \cap B \neq \emptyset$$
$$\forall A \subset \complement_X B, x \in A \Rightarrow (\exists y \in A, A \cap \overleftarrow{R}(y) = \emptyset)$$

The set X with R is called well-founded (or: the relation R is well-founded) when $\mathcal{F}_R(\emptyset) = X$, which is equivalenly expressible as

$$\forall A \subset X, (\forall x \in X, \overleftarrow{R}(x) \subset A \Rightarrow x \in A) \Rightarrow A = X$$
$$\forall A \subset X, (\forall x \in A\ \exists y \in A, yRx) \Rightarrow A = \emptyset$$
$$\forall A \subset X, A \subset R_*(A) \Rightarrow A = \emptyset$$
$$\forall A \subset X, A \neq \emptyset \Rightarrow (\exists x \in A, A \cap \overleftarrow{R}(x) = \emptyset)$$

Given a set X with a well-founded relation R, and a formula P with variable $x \in X$, a *proof by induction* of $(\forall x \in X, P(x))$, is a proof that for all $x \in X$, deduces $P(x)$ from the hypothesis $\forall y \in \overleftarrow{R}(x), P(y)$. Indeed the set $A = \{x \in X | P(x)\}$ then satisfying $\forall x \in X, \overleftarrow{R}(x) \subset A \Rightarrow x \in A$, this implies $A = X$.

Proposition. *Let X and Y two sets, $R \in \mathcal{B}_X, S \in \mathcal{B}_Y, u \in Y^X$. Then*
1) If $\forall x \in X, \overleftarrow{S}(u(x)) \subset u[\overleftarrow{R}(x)]$, then $u_* \circ \mathcal{F}_R \leq \mathcal{F}_S \circ u_*$ et $\mathcal{F}_R \circ u^* < u^* \circ \mathcal{F}_S$.
2) If $\forall x \in X, u[\overleftarrow{R}(x)] \subset \overleftarrow{S}(u(x))$, then $u^* \circ \mathcal{F}_S < \mathcal{F}_R \circ u^*$ and if S is well-founded then R too.

It comes from the formulas of transport of closure, translating the hypotheses as follows:

$$\begin{aligned}(\forall x \in X, \overleftarrow{S}(u(x)) \subset u[\overleftarrow{R}(x)]) &\Leftrightarrow \forall x \in X, \forall A \subset X, \overleftarrow{R}(x) = A \Rightarrow \overleftarrow{S}(u(x)) \subset u[A]\\ &\Leftrightarrow \forall A \subset X, \forall x \in X, x \in \overleftarrow{R}^\bullet(A) \Rightarrow u(x) \in \mathcal{D}_S(u[A])\\ &\Leftrightarrow \forall A \subset X, u[\overleftarrow{R}^\bullet(A)] \subset \mathcal{D}_S(u[A]))\end{aligned}$$

$$\begin{aligned}(\forall x \in X, u[\overleftarrow{R}(x)] \subset \overleftarrow{S}(u(x))) &\Leftrightarrow \forall x \in X, \forall B \subset Y, \overleftarrow{S}(u(x)) = B \Rightarrow \overleftarrow{R}(x) \subset u^*(B)\\ &\Leftrightarrow \forall B \subset Y, \forall x \in X, u(x) \in \overleftarrow{S}^\bullet(B) \Rightarrow x \in \mathcal{D}_R(u^*(B))\\ &\Leftrightarrow \forall B \subset Y, u^*(\overleftarrow{S}^\bullet(B)) \subset \mathcal{D}_R(u^*(B))\end{aligned}$$ ☐

Corollary. *Let R and R' two binary relations on the same set. If $R \leq R'$ and R' is well-founded then R is well-founded.*

Proposition. *Let R a binary relation on a set X, $K \subset X$ such that $K \in \mathrm{Cut}({}^tR)$, and let R' the restriction of R to K. Then $\forall B \subset X, \mathcal{F}_{R'}(K \cap B) = K \cap \mathcal{F}_R(B)$. If moreover $K \in \mathrm{Im}\,\mathcal{F}_R$ then $\forall B \subset K, \mathcal{F}_{R'}(B) = \mathcal{F}_R(B)$.*

This comes from the previous proposition, with $u = \mathrm{Id}_K$ from K to X; the last point comes as a particular case of the properties of f_A. ☐

Proposition. *Let R a binary relation on a set X, and $z \in X$. There is equivalence between :*
1) $z \in \mathcal{F}_R(\emptyset)$
2) $\overleftarrow{R}(z) \subset \mathcal{F}_R(\emptyset)$
3) $\overleftarrow{\lceil R \rceil}(z) \subset \mathcal{F}_R(\emptyset)$
4) the restriction of R to $\overleftarrow{\lceil R \rceil}(z)$ is well-founded.

From $\mathcal{F}_R(\emptyset) \in \mathrm{Fix}\,\mathcal{D}_R$ comes 1) $\Leftrightarrow$ 2), and $\mathcal{F}_R(\emptyset) \in \mathrm{Cut}({}^tR)$ thus 1) $\Leftrightarrow$ 3).
Finally, 3) $\Leftrightarrow$ 4) comes from the last proposition with $\overleftarrow{\lceil R \rceil}(z) \in \mathrm{Cut}({}^tR)$. ☐

Proposition. *The transitive closure T of a well-founded relation R is well-founded.*

Proof: $\forall A \subset X, ((A \subset T_*A) \wedge (B = A \cup T_*A = \lceil R \rceil_* A)) \Rightarrow A \subset B = T_*A = R_*B = \emptyset$. ☐

Proposition. *Any well-founded relation is antireflexive and antisymmetric.*

Proof: $\forall x \in X, \exists y \in \{x\}, \{x\} \cap \overleftarrow{R}(y) = \emptyset$ thus R is antireflexive. For antisymmetry, we can either use $A = \{x, y\}$, or note that T being antireflexive is also antisymmetric. ☐

Proposition. *The preorder generated by a well-founded relation is an order.*

It comes from $x \lceil R \rceil y \Leftrightarrow (xTy \vee x = y)$ and the antisymmetry of T. ☐

Proposition. *Let R a well-founded relation on a set X such that $\forall x \in X, \overleftarrow{R}(x)$ is finite. Then $\forall x \in X, \overleftarrow{\lceil R \rceil}(x)$ is finite.*

Proof 1 by induction: let $y \in X$ such that $\forall x \in \overleftarrow{R}(y), \overleftarrow{\lceil R \rceil}(x)$ is finite. Then

$$\overleftarrow{\lceil R \rceil}(y) = \{y\} \cup \bigcup_{x \in \overleftarrow{R}(y)} \overleftarrow{\lceil R \rceil}(x)$$

being a finite union of finite sets is finite.
Proof 2: $\forall x \in X, \exists A$ finite $\subset X, x \in A \wedge \lceil (\overleftarrow{R}^{\bullet})_A \rceil(\emptyset) = A$. By the fixed point theorem, $A \subset \mathcal{D}_R(A)$ thus $A \in \mathrm{Cut}({}^tR)$ thus $\overleftarrow{\lceil R \rceil}(x) \subset A$. □

Theorem (generalized recursion principle). *Let (X, R) a well-founded set, $(E_x)_{x\in X}$ a family of sets, and*

$$P = \prod_{y \in X} E_y$$
$$\forall x \in X, P_x = \prod_{y \in \overleftarrow{R}(x)} E_y$$
$$\forall x \in X, \forall f \in P, r_x(f) = f_{|\overleftarrow{R}(x)} \in P_x$$

Let $\phi \in \prod_{x\in X} E_x^{P_x}$ a family of functions $\phi_x : P_x \to E_x$. Then, $\exists! \psi \in P, \forall x \in X, \psi(x) = \phi_x(r_x(\psi))$.

Proof. Let $F = \coprod_{x \in X} E_x$, and $K = \{h \in P | \forall x \in X, h(x) = \phi_x(r_x(h))\}$.

Let $g = \nearrow(\overrightarrow{S}) \in \mathcal{P}(F)^{\mathcal{P}(F)}$ where $\mathrm{Gr}(S) = \{(\mathrm{Gr}(u), (x, \phi_x(u))) | x \in X, u \in P_x\}$, i.e.

$$\forall G \subset F, g(G) = \{(x, \phi_x(u)) | x \in X, u \in P_x \wedge \mathrm{Gr}(u) \subset G\}.$$

$\forall G \subset F$, let $A = \{x \in X | \exists! y \in E_x, (x, y) \in G\}$, and $h \in \prod_{x \in A} E_x$ defined by $\mathrm{Gr}\, h \subset G$.

$$\forall x \in X, \overleftarrow{R}(x) \subset A \Rightarrow (\forall y \in E_x, (x, y) \in g(G) \Leftrightarrow y = \phi_x(h_{|\overleftarrow{R}(x)})) \Rightarrow \exists! y \in E_x, (x, y) \in g(G)$$
$$G \in \mathrm{Fix}\, g \Rightarrow (\forall x \in X, \overleftarrow{R}(x) \subset A \Rightarrow (\exists! y \in E_x, (x, y) \in G) \Rightarrow x \in A) \Rightarrow A = X \Rightarrow (h \in P \wedge G = \mathrm{Gr}\, h)$$
$$\forall h \in P, \mathrm{Gr}\, h \in \mathrm{Fix}\, g \Leftrightarrow (\forall (x, y) \in F, (x, y) \in \mathrm{Gr}\, h \Leftrightarrow y = \phi_x(r_x(h))) \Leftrightarrow h \in K$$
$$\exists \psi \in K, \mathrm{Gr}\, \psi : \min \mathrm{Fix}\, g \wedge \forall h \in P, (h \in K \Rightarrow \mathrm{Gr}(h) \in \mathrm{Fix}\, g \Rightarrow \mathrm{Gr}(\psi) \subset \mathrm{Gr}(h) \Rightarrow \psi = h).$$ □

Proposition. *With the same notations, if $\phi, \phi' \in \prod_{x\in X} E_x^{P_x}$, $\psi, \psi' \in P$ defined by induction respectively by ϕ and ϕ', if $A \in \mathrm{Cut}({}^tR)$ and $\phi_{|A} = \phi'_{|A}$, then $\psi_{|A} = \psi'_{|A}$. In particular for any fixed $y \in X$, with $A = \overleftarrow{\lceil R \rceil}(y)$, if $\phi_{|A} = \phi'_{|A}$, then $\psi(y) = \psi'(y)$.*

We just need to apply the uniqueness result to the set A with $\phi_{|A} \in \prod_{x\in A} E_x^{P_x}$ while the restriction R' of R to A is well-founded and from $A \in \mathrm{Cut}({}^tR)$ comes $\forall x \in A, \overleftarrow{R}(x) = \overleftarrow{R'}(x)$, so that the definitions of P_x in X and A coincide. □

Example 1. *The induction principle is the particular case of the induction on $\mathbb{N}$ with the well-founded relation $(x, y) \mapsto (y = x + 1)$. However the same formula on $\mathbb{Z}$ does not give a well-founded relation.*

Example 2. *If R and S are binary relations on E, where R is well-founded and $\forall x, y \in E, (xSy) \Leftrightarrow (x = y \vee \exists z \in E, (xSz \wedge zRy))$, then $S = \lceil R \rceil$.*

Indeed this formula can be written

$$\forall y \in E, \overleftarrow{S}(y) = \{y\} \cup \bigcup_{z \in \overleftarrow{R}(y)} \overleftarrow{S}(z)$$

which defines $\overleftarrow{S}$ by induction. But $\overleftarrow{\lceil R \rceil}$ satisfies the same formula, thus $S = \lceil R \rceil$.

This can also be seen as for all x a definition of $(y \mapsto (xSy))$ by induction.