Foundations of mathematics

Sylvain Poirier
settheory.net

2. Set theory (continued)

2.1. Tuples, families

A tuple (or n-tuple, for any integer n) is an interpretation of a list of n variables. It is thus a meta-function from a finite meta-set, to the universe. A 2-tuple is called an *oriented pair*, a 3-tuple is a *triple*, a 4-tuple is a *quadruple*... Tuples of a given kind (list of variables with their types) can be added to any theory as a new type of objects. Variables of this type play the role of abbreviations of packs of n variables with old types (copies of the given list) $x = (x_0, \cdots, x_{n-1})$. In practice, the domain of considered n-tuples will be the (meta-)set V_n of n digits from 0 to $n-1$. Set theory can represent its own n-tuples as functions, figuring V_n as a set of objects all named by constants.

The n-tuple definer is not a binder but an n-ary operator, placing its n arguments in a parenthesis and separated by commas: $(\ , \cdots , \ )$. The evaluator appears, curried by fixing the meta-argument, as a list of n functors called *projections*: for each $i \in V_n$, the i-th projection π_i gives the value $\pi_i(x) = x_i$ of each tuple $x = (x_0, \cdots, x_{n-1})$ at i (value of the i-th variable inside x). They are subject to the following axioms (where the first sums up the next ones) : for any $x_0, \cdots, x_{n-1}$ and any n-tuple x,

$$x = (x_0, \cdots, x_{n-1}) \Leftrightarrow (\pi_0(x) = x_0 \wedge \cdots \wedge \pi_{n-1}(x) = x_{n-1})$$
$$x_i = \pi_i((x_0, \cdots, x_{n-1})) \quad \text{for each } i \in V_n$$
$$x = (\pi_0(x), \cdots, \pi_{n-1}(x))$$

Oriented pairs suffice to build (copies of) n-tuples for each $n > 2$, in the sense that we can define operators to play the roles of definer and projections, satisfying the same axioms. For example, triples $t = (x, y, z)$ can be defined as $t = ((x, y), z))$ and evaluated by $x = \pi_0(\pi_0(t)), y = \pi_1(\pi_0(t)), z = \pi_1(t)$.

Conditional connective

The 3-ary connective "*If $\mathcal{A}$ then $\mathcal{B}$ else $\mathcal{C}$*", is written as follows (applying $(\mathcal{C}, \mathcal{B})$ to $\mathcal{A} \in V_2$) :

$$(\mathcal{A}?\mathcal{B} : \mathcal{C}) \Leftrightarrow (\neg\mathcal{C} \Rightarrow \mathcal{A} \Rightarrow \mathcal{B}) \Leftrightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\neg\mathcal{A} \Rightarrow \mathcal{C})) \Leftrightarrow (\neg\mathcal{A}?\mathcal{C} : \mathcal{B}) \Leftrightarrow (\mathcal{C}, \mathcal{B})(\mathcal{A})$$
$$\Leftrightarrow ((\mathcal{A} \wedge \mathcal{B}) \vee (\neg\mathcal{A} \wedge \mathcal{C})) \Leftrightarrow ((\mathcal{C} \Rightarrow \mathcal{A}) \Rightarrow (\mathcal{A} \wedge \mathcal{B})) \not\Leftrightarrow (\mathcal{A}?\neg\mathcal{B} : \neg\mathcal{C})$$

Any n+1-ary connective K amounts to two n-ary ones: $K(\mathcal{A}) \Leftrightarrow (\mathcal{A}?K(1) : K(0))$.
Thus, $\neg\mathcal{A} \Leftrightarrow (\mathcal{A}?0 : 1)$; $(\mathcal{A} \Rightarrow \mathcal{B}) \Leftrightarrow (\mathcal{A}?\mathcal{B} : 1)$; $(\mathcal{A} \vee \mathcal{B}) \Leftrightarrow (\mathcal{A}?1 : \mathcal{B})$; $(\mathcal{A} \Leftrightarrow \mathcal{B}) \Leftrightarrow (\mathcal{A}?\mathcal{B} : \neg\mathcal{B})$.

Families

A *family* is a function intuitively seen as a generalized tuple: its domain (a set) is seen as simple, fixed, outside the main studied system, as if it was a set of meta-objects. A "family of..." is a family whose image is a "set of...".

Families use the formalism of functions disguised in the style of tuples (whose tools cannot apply due to the finiteness of symbols). The evaluator (evaluating u at i), instead of $u(i)$ or $\pi_i(u)$, is written u_i (looking like a meta-variable symbol of variable). A family defined by a term t, is written $(t(i))_{i \in I}$ instead of $(I \ni i \mapsto t(i))$ or $(t(0), \cdots, t(n-1))$. The argument i is called *index*, and the family is said *indexed by* its domain I.

Structures and binding symbols

Each n-ary structure can be seen as a unary structure with domain a class of n-tuples (like a binder can be seen as a unary structure on a class of functions or subsets of a given set): binders are the generalization of structures when replacing tuples by families. In particular, quantifiers $\forall$, $\exists$ respectively generalize the chains of conjunctions and disjunctions: $(\mathcal{B}_0 \wedge \cdots \wedge \mathcal{B}_{n-1}) \Leftrightarrow (\forall i \in V_n, \mathcal{B}_i)$. The equality condition between ordered pairs, $(x, y) = (z, t) \Leftrightarrow (x = z \wedge y = t)$, is similar to the one for functions.

Let $\mathcal{R}$ a unary predicate definite on E, and $\mathcal{C}$ a boolean. We have distributivities

$$(\mathcal{C} \wedge \exists x \in E, \mathcal{R}(x)) \;\Leftrightarrow\; (\exists x \in E, \mathcal{C} \wedge \mathcal{R}(x))$$
$$(\mathcal{C} \vee \forall x \in E, \mathcal{R}(x)) \;\Leftrightarrow\; (\forall x \in E, \mathcal{C} \vee \mathcal{R}(x))$$
$$(\mathcal{C} \Rightarrow \forall x \in E, \mathcal{R}(x)) \;\Leftrightarrow\; (\forall x \in E, \mathcal{C} \Rightarrow \mathcal{R}(x))$$
$$((\exists x \in E, \mathcal{R}(x)) \Rightarrow \mathcal{C}) \;\Leftrightarrow\; (\forall x \in E, \mathcal{R}(x) \Rightarrow \mathcal{C})$$
$$(\exists x \in E, \mathcal{C}) \Leftrightarrow (\mathcal{C} \wedge E \neq \emptyset) \Rightarrow \mathcal{C} \Rightarrow (\mathcal{C} \vee E = \emptyset) \Leftrightarrow (\forall x \in E, \mathcal{C})$$

Extensional definitions of sets

The functor Im defines the binder $\{T(x)|x \in E\} = \{T(x)\}_{x\in E} = \mathrm{Im}(E \ni x \mapsto T(x))$. As this notation looks similar to the set builder, we can combine both :

$$\{T(x)|x \in E \wedge \mathcal{R}(x)\} = \{T(x)|x \in \{y \in E|\mathcal{R}(y)\}\}$$

Applying Im to tuples, defines the operator symbols of *exensional definition* of sets (listing their elements): $\mathrm{Im}(a, b, \cdots) = \{a, b, \cdots\}$. Those of arity 0,1,2 were presented in 1.10: the empty set $\emptyset$, the singleton $\{a\}$ and the pairing $\{a, b\}$. We defined V_n as $\{0, \cdots, n-1\}$. Images of tuples are finite sets.

2.2. Boolean operators on families of sets

Union of a family of sets

For any family of unary predicates $\mathcal{A}_i$ with index $i \in I$, all definite in (at least) a common class $\mathcal{C}$, their application to the same variable x with range $\mathcal{C}$ reduces this to a family of Boolean variables depending on x (their parameter, see 1.5). This way, any operation Q on these variables (a quantifier with range I, which becomes a connective when I is finite) defines a meta-operation between unary predicates, with result a unary predicate $\mathcal{R}$, defined for x in $\mathcal{C}$ as $Qi, \mathcal{A}_i(x)$. When $\mathcal{C}$ is a set E, this operates between subsets of E (through $\in$ and the set builder).

For example, the existential quantifier ($Q = \exists$) defines the union of a family of sets:

$$x \in \bigcup_{i\in I} F_i \Leftrightarrow \exists i \in I, x \in F_i$$

This class is a set independent of E, as it can also be defined from the union of a set of sets (1.11):

$$\bigcup_{i\in I} F_i = \bigcup\{F_i|i \in I\} \qquad (\forall x \in \bigcup_{i\in I} F_i, \mathcal{B}(x)) \Leftrightarrow \forall i \in I, \forall x \in F_i, \mathcal{B}(x)$$

$$x \in A \cup B \Leftrightarrow (x \in A \vee x \in B) \qquad A \subset A \cup B = B \cup A$$

All extensional definition operators (except $\emptyset$) are definable from pairing and binary union.

Intersection

Now any fixed family of sets $(F_i)_{i\in I}$ can be seen as a family of subsets of some common set, such as their union $U = \bigcup_{i\in I} F_i$, or any other set E such that $U \subset E$. Then for any operation Q between Booleans indexed by I, the predicate $\mathcal{R}(x)$ defined as $(Qi, x \in F_i)$ takes value $(Qi, 0)$ for all $x \notin U$. Thus Q needs to satisfy $\neg(Qi, 0)$ (to be false when all entries are false) for the class $\mathcal{R}$ to be a set $\{x \in E|\mathcal{R}(x)\} = \{x \in U|\mathcal{R}(x)\}$. This was always the case for $Q = \exists$, including on the empty family ($\bigcup \emptyset = \emptyset$), but for $\forall$ (that defines the intersection) it requires a non-empty family of sets ($I \neq \emptyset$):

$$\forall j \in I, \quad \bigcap_{i\in I} F_i = \{x \in F_j|\forall i \in I, x \in F_i\} \qquad x \in \textstyle\bigcap_{i\in I} F_i \Leftrightarrow \forall i \in I, x \in F_i$$

$$x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B)$$

$$A = A \cup B \Leftrightarrow B \subset A \Leftrightarrow \ B = A \cap B \qquad A \cap B = B \cap A = \{x \in A|x \in B\} \subset A$$

Two sets A and B are called *disjoint* when $A \cap B = \emptyset$, which is equivalent to $\forall x \in A, x \notin B$.

Union and intersection have the same associativity and distributivity properties as $\wedge$ and $\vee$:

$$A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C) = \bigcup\{A, B, C\}$$

$$(\bigcup_{i\in I} A_i) \cap C = \bigcup_{i\in I}(A_i \cap C) \qquad (\bigcap_{i\in I} A_i) \cup C = \bigcap_{i\in I}(A_i \cup C)$$

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \qquad (A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Other operators

The *difference* is defined by $A\backslash B = \{x \in A|x \notin B\}$ so that $x \in A\backslash B \Leftrightarrow x \in A \wedge x \notin B$.

Finally the connective $\not\Leftrightarrow$ gives the symmetric difference: $A\Delta B = (A \cup B)\backslash(A \cap B)$.

When $(Qi, 0)$ is true, we must choose a set E to define operations between subsets of E :

- Negation defines $\complement_E F = E\backslash F$, called the *complement of* F *in* E : $\forall x \in E, x \in F \not\Leftrightarrow x \in \complement_E F$.
- The intersection of the empty family gives E: for a family of subsets F_i of E,

$$\bigcap_{i\in I} F_i = \bigcap\{F_i|i\in I\} = \{x \in E|\forall i \in I, x\in F_i\} = \complement_E \bigcup_{i\in I} \complement_E F_i$$

2.3. Products, graphs and composition

Finite product

For two sets E and F, the *product* $E \times F$ is the set of (x, y) where $x \in E$ and $y \in F$. Similarly, the product of n sets $E_0 \times \cdots \times E_{n-1}$ is the set of n-tuples $(x_0, \cdots, x_{n-1})$ where $\forall i \in V_n, x_i \in E_i$.

An n-ary operation is a function with domain a product of n sets. A relation (for example between E and F) can be expressed as a set of tuples ($G \subset E \times F$). The domains E and F can be specified by taking the triple (E, F, G). A set of oriented pairs (such as G) is called a *graph*.

For any binder Q and any graph G, the formula $Qx \in G, S(x_0, x_1)$ that binds $x = (x_0, x_1)$ on a binary structure A with domain G, can be seen as binding 2 variables x_0, x_1 on $A(x_0, x_1)$, and thus be denoted with an oriented pair of variables: $Q(y, z) \in G, A(y, z)$.

The existence of the product (in all arity) is justified by the set generation principle:

$$(\exists (x, y) \in E \times F, A(x, y)) \Leftrightarrow (\exists x \in E, \exists y \in F, A(x, y)) \Leftrightarrow (\exists y \in F, \exists x \in E, A(x, y))$$
$$(\forall (x, y) \in E \times F, A(x, y)) \Leftrightarrow (\forall x \in E, \forall y \in F, A(x, y)) \Leftrightarrow (\forall y \in F, \forall x \in E, A(x, y))$$

The quantifier $\forall (x, y) \in E \times E$ will be abbreviated as $\forall x, y \in E$, and the same for $\exists$. When $F = V_2$,

$$\begin{aligned}(\exists x \in E, A(x) \vee B(x)) &\Leftrightarrow ((\exists x \in E, A(x)) \vee (\exists x \in E, B(x))\\ (\forall x \in E, A(x) \wedge B(x)) &\Leftrightarrow ((\forall x \in E, A(x)) \wedge (\forall x \in E, B(x))\end{aligned}$$
$$(\exists x \in E, C \vee A(x)) \Leftrightarrow ((C \wedge (E \neq \emptyset)) \vee \exists x \in E, A(x))$$
$$(\forall x \in E, C \wedge A(x)) \Leftrightarrow ((C \vee (E = \emptyset)) \wedge \forall x \in E, A(x))$$

Sum or disjoint union

The *transpose* of an ordered pair is ${}^t(x, y) = (y, x)$; that of a graph R is ${}^tR = \{(y, x) | (x, y) \in R\}$.

Graphs can be expressed in curried forms $\overrightarrow{R}$ and $\overleftarrow{R}$: $y \in \overrightarrow{R}(x) \Leftrightarrow (x, y) \in R \Leftrightarrow x \in \overleftarrow{R}(y) = \overrightarrow{{}^tR}(y)$, justified by defining the functor $\overrightarrow{R}$ as $\overrightarrow{R}(x) = \{y | (z, y) \in R \wedge z = x\}$.

Inversely, any family of sets $(E_i)_{I \in I}$ defines a graph called their *sum* (or *disjoint union*) $\coprod_{i \in I} E_i$:

$$(i \in I \wedge x \in E_i) \Leftrightarrow (i, x) \in \coprod_{i \in I} E_i = \bigcup_{i \in I} \{i\} \times E_i = \bigcup_{i \in I} \{(i, x) | x \in E_i\} \subset I \times \bigcup_{i \in I} E_i$$
$$(\forall x \in \textstyle\coprod_{i \in I} E_i, \mathcal{A}(x)) \Leftrightarrow (\forall i \in I, \forall y \in E_i, \mathcal{A}(i, y))$$
$$E_0 \sqcup \cdots \sqcup E_{n-1} = \textstyle\coprod_{i \in V_n} E_i$$
$$E \times F = \textstyle\coprod_{x \in E} F \qquad E \times \emptyset = \emptyset = \emptyset \times E$$
$$(E \subset E' \wedge F \subset F') \Rightarrow E \times F \subset E' \times F'$$
$$(\forall i \in I, E_i \subset E'_i) \Leftrightarrow \coprod_{i \in I} E_i \subset \coprod_{i \in I} E'_i$$

Composition, restriction, graph of a function

For any set E, the function *identity* on E is defined by $\mathrm{Id}_E = (E \ni x \mapsto x)$.

For any functions f, g with $\operatorname{Im} f \subset \operatorname{Dom} g$ (namely, $f : E \to F$ and $g : F \to G$), their *composite* is

$$g \circ f = ((\operatorname{Dom} f) \ni x \mapsto g(f(x))) : E \to G$$

The same with $h : G \to H$, $h \circ g \circ f = (h \circ g) \circ f = h \circ (g \circ f) = (E \ni x \mapsto h(g(f(x))))$ and so on.

The *restriction* of f to $A \subset \operatorname{Dom} f$ is $f_{|A} = (A \ni x \mapsto f(x)) = f \circ \mathrm{Id}_A$.

The *graph of a function* f is defined by

$$\operatorname{Gr} f = \{(x, f(x)) | x \in \operatorname{Dom} f\} = \textstyle\coprod_{x \in \operatorname{Dom} f} \{f(x)\}$$
$$(x, y) \in \operatorname{Gr} f \Leftrightarrow (x \in \operatorname{Dom} f \wedge y = f(x))$$

We can define domains, images and restrictions for graphs, letting those for functions be particular cases (i.e. $\operatorname{Dom} f = \operatorname{Dom}(\operatorname{Gr} f)$, $\operatorname{Im} f = \operatorname{Im}(\operatorname{Gr} f)$ and $\operatorname{Gr}(f_{|A}) = (\operatorname{Gr} f)_{|A}$):

$$\operatorname{Dom} R = \{x | (x, y) \in R\} = \operatorname{Im} {}^tR \qquad \forall x, \quad x \in \operatorname{Dom} R \Leftrightarrow \overrightarrow{R}(x) \neq \emptyset$$
$$R \subset E \times F \Leftrightarrow (\operatorname{Dom} R \subset E \wedge \operatorname{Im} R \subset F)$$
$$R_{|A} = R \cap (A \times \operatorname{Im} R) = \{(x, y) \in R | x \in A\} = \textstyle\coprod_{x \in A} \overrightarrow{R}(x)$$

Then we have $R = \coprod_{i\in I} E_i \Leftrightarrow (\mathrm{Dom}\, R \subset I \wedge \forall i \in I, \overrightarrow{R}(i) = E_i) \Rightarrow \mathrm{Im}\, R = \bigcup_{i\in I} E_i$.
For any functions f, g, any graph R, and $E = \mathrm{Dom}\, f$,

$$\begin{aligned}
\mathrm{Gr}\, f \subset R &\Leftrightarrow \forall x \in E, f(x) \in \overrightarrow{R}(x)\\
R \subset \mathrm{Gr}\, f &\Leftrightarrow (\forall (x,y) \in R, x \in E \wedge y = f(x)) \Leftrightarrow (\mathrm{Dom}\, R \subset E \wedge \forall (x,y) \in R, y = f(x))\\
\mathrm{Gr}\, f \subset \mathrm{Gr}\, g &\Leftrightarrow ((E \subset \mathrm{Dom}\, g) \wedge f = g_{|E})
\end{aligned}$$

Direct image, inverse image

The direct image of a set A by a graph R is $R_*(A) = \mathrm{Im}\, R_{|A} = \bigcup_{x\in A} \overrightarrow{R}(x)$.

$$\mathrm{Dom}\, R \subset A \Leftrightarrow R_{|A} = R \Rightarrow R_*(A) = \mathrm{Im}\, R$$
$$R_*(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} R_*(A_i) \qquad R_*(\bigcap_{i\in I} A_i) \subset \bigcap_{i\in I} R_*(A_i)$$
$$A \subset B \Rightarrow R_*(A) \subset R_*(B)$$

The *direct image* of $A \subset \mathrm{Dom}\, f$ by a function f is

$$f[A] = f_*(A) = (\mathrm{Gr}\, f)_*(A) = \mathrm{Im}(f_{|A}) = \{f(x) | x \in A\} \subset \mathrm{Im}\, f$$

For any $f : E \to F$ and $B \subset F$, the *inverse image* of B by f, written $f^*(B)$, is defined by

$$\begin{aligned}
f^*(B) &= ({}^t\mathrm{Gr}\, f)_*(B) = \{x \in E | f(x) \in B\} = \bigcup_{y\in B} f^\bullet(y)\\
f^\bullet(y) &= (\overleftarrow{\mathrm{Gr}} f)(y) = f^*(\{y\}) = \{x \in E | f(x) = y\}\\
f^*(\complement_F B) &= \complement_E f^*(B)
\end{aligned}$$

For any family $(B_i)_{i\in I}$ of subsets of F, $f^*(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^*(B_i)$ where intersections are respectively interpreted as subsets of F and E.

2.4. Uniqueness quantifiers, functional graphs

For all sets $F \subset E$, all unary predicate $\mathcal{A}$ definite on E, and all $x \in E$,

$$\begin{aligned}
x \in F &\Leftrightarrow \{x\} \subset F \Leftrightarrow (\exists y \in E, x = y \wedge y \in F) \Leftrightarrow (\forall y \in E, x = y \Rightarrow y \in F)\\
x \in F &\Rightarrow ((\forall y \in F, \mathcal{A}(y)) \Rightarrow \mathcal{A}(x) \Rightarrow \exists y \in F, \mathcal{A}(y))\\
F \subset \{x\} &\Leftrightarrow (\forall y \in F, x = y) \Rightarrow ((\exists y \in F, \mathcal{A}(y)) \Rightarrow \mathcal{A}(x) \Rightarrow (\forall y \in F, \mathcal{A}(y)))\\
F = \{x\} &\Leftrightarrow (x \in F \wedge \forall y \in F, x = y) \Leftrightarrow (\forall y \in E, y \in F \Leftrightarrow x = y)
\end{aligned}$$

Here are 3 new quantifiers: $\exists 2$ (plurality), $!$ (uniqueness), and $\exists!$ (existence and uniqueness), whose results when applied to A in E only depend on $F = \{x \in E, A(x)\}$ (like $\exists$ and unlike $\forall$) :

$$\begin{aligned}
(\exists x \in E, A(x)) &\Leftrightarrow (F \neq \emptyset) \Leftrightarrow (\exists x \in F, 1) \Leftrightarrow (\exists x \in E, \{x\} \subset F)\\
(\exists 2 x \in E, A(x)) &\Leftrightarrow (\exists 2 : F) \Leftrightarrow (\exists x, y \in F, x \neq y) \Leftrightarrow (\exists x, y \in E, A(x) \wedge A(y) \wedge x \neq y)\\
(!x \in E, A(x)) &\Leftrightarrow (!: F) \Leftrightarrow \neg(\exists 2 : F) \Leftrightarrow (\forall x, y \in F, x = y) \Leftrightarrow \forall x \in F, F \subset \{x\}\\
(\exists! x \in E, A(x)) &\Leftrightarrow (\exists! : F) \Leftrightarrow (\exists x \in F, F \subset \{x\}) \Leftrightarrow (\exists x \in E, F = \{x\})\\
F \subset \{x\} &\Rightarrow \forall y \in F, F \subset \{y\} \Leftrightarrow (!: F)\\
(\exists! : F) &\Leftrightarrow (F \neq \emptyset \wedge !: F)\\
F \neq \emptyset &\Rightarrow ((\forall y \in F, B(y)) \Rightarrow (\exists y \in F, B(y)))\\
(!: F) &\Rightarrow ((\exists y \in F, B(y)) \Rightarrow (\forall y \in F, B(y)))\\
F = \{x\} &\Rightarrow ((\exists y \in F, B(y)) \Leftrightarrow B(x) \Leftrightarrow \forall y \in F, B(y))
\end{aligned}$$

A function f is said *constant* when $!: \mathrm{Im}\, f$. The constancy of a tuple is the chain of equalities:

$$x = y = z \Leftrightarrow !: \{x, y, z\} \Leftrightarrow ((x = y) \wedge (y = z)) \Rightarrow x = z$$

Translating operators into predicates

In a generic theory, any functor symbol T can be replaced by a binary predicate symbol R (where $x\ R\ y \Leftrightarrow (y = T(x))$) with the axiom $\forall x, \exists! y, x\ R\ y$, replacing any formula $\mathcal{A}(T(x))$ (where x is a term) by $(\exists y, x\ R\ y \wedge \mathcal{A}(y))$, or by $(\forall y, x\ R\ y \Rightarrow \mathcal{A}(y))$ (while terms cannot be translated). This way, any predicate R such that $\forall x, \exists! y, x\ R\ y$ implicitly defines an operator symbol T. We can extend this to other arities by replacing x by a tuple.

But the use of open quantifiers in this construction makes it unacceptable in our set theory. Instead, let us introduce a new operator ϵ on the class $(\mathrm{Set}(E) \wedge \exists! : E)$ of singletons, giving their element according to the axiom $(\forall x)\epsilon\{x\} = x$, or equivalently $(\mathrm{Set}\, E \wedge \exists! : E) \Rightarrow \epsilon E \in E$. Then for every unary predicate $\mathcal{A}$ and every singleton E, $\mathcal{A}(\epsilon E) \Leftrightarrow (\exists x \in E, \mathcal{A}(x)) \Leftrightarrow (\forall x \in E, \mathcal{A}(x))$.

Conditional operator

Like the conditional connective, it chooses between two objects x, y depending on the boolean $\mathcal{B}$:

$$(\mathcal{B}?x : y) = (y, x)_{\mathcal{B}} = \epsilon\{z \in \{x, y\} | \mathcal{B}?z = x : z = y\}$$

so that for any predicate $\mathcal{A}$ we have $\mathcal{A}(\mathcal{B}?x : y) \Leftrightarrow (\mathcal{B}?\mathcal{A}(x) : \mathcal{A}(y))$. All para-operators other than connectives but with at least a Boolean argument, are naturally expressed as composed of the conditional operator with operators, or the conditional connective with predicates, which is why they did not need an explicit presence in the language of a theory.

Functional graphs

A graph R is said *functional* if $\forall x \in \mathrm{Dom}\, R, ! : \overrightarrow{R}(x)$, or equivalently $\forall x, y \in R, x_0 = y_0 \Rightarrow x_1 = y_1$. This is the condition for it to be the graph of a function. Namely, $R = \mathrm{Gr}(\epsilon\overrightarrow{R})$ where

$$\epsilon\overrightarrow{R} = ((\mathrm{Dom}\, R) \ni x \mapsto \epsilon(\overrightarrow{R}(x)))$$

2.5. The powerset axiom

Let us extend set theory by 3 new symbols (powerset, exponentiation, product) with axioms, that will declare given classes $\mathcal{C}$ to be sets K. These extensions are similar to those provided by the set generation principle (1.11), but no more satisfy its requirement.

In the traditional ZF formalization of set theory only accepting $\in$ as primitive stucture, such a declaration is done purely by the axiom (or theorem) $(\forall$ parameters$), \exists K, \forall x, x \in K \Leftrightarrow \mathcal{C}(x)$. Then, the operator symbol K taking the parameters of $\mathcal{C}$ as its arguments, represents the following abbreviations: $\forall x \in K$ means $\forall x, \mathcal{C}(x) \Rightarrow$; the equality $X = K$ means $(\forall x, x \in X \Leftrightarrow \mathcal{C}(x))$, and any other $\mathcal{A}(K)$ means $\exists X, (X = K) \wedge \mathcal{A}(X)$. But these formulas use open quantifiers, forbidden in our framework.

For what the set generation principle justified, $\forall_{\mathcal{C}}$ could be replaced by formulas, while the above $\exists X$ could be treated by existential elimination (1.9). But otherwise without open quantifiers, even a given set K identical to a class $\mathcal{C}$, would not be recognizable as such, so that the very claim that $\mathcal{C}$ coincides with a set remains practically meaningless. Thus, our set theoretical framework requires the operator symbol K to be regarded as primitive in the language (instead of a defined abbreviation), with argument the tuple y of parameters of $\mathcal{C}$, and the axiom

$$(\forall y \cdots), \mathrm{Set}(K(y)) \wedge (\forall x, x \in K(y) \Leftrightarrow \mathcal{C}_y(x))$$

Powerset. $\forall_{\mathrm{Set}} E, \mathrm{Set}(\mathcal{P}(E)) \wedge (\forall F, F \in \mathcal{P}(E) \Leftrightarrow (\mathrm{Set}(F) \wedge F \subset E))$.

We shall also shorten $\in\mathcal{P}$ into $\subset$ in binding symbols: $(\forall A \subset E, \cdots) \Leftrightarrow (\forall A \in \mathcal{P}(E), \cdots)$.

Exponentiation. $\forall_{\mathrm{Set}} E, F,\ \mathrm{Set}(F^E) \wedge (\forall f, f \in F^E \Leftrightarrow f : E \to F)$.

Product of a family of sets. *This binder generalizes the finite product operators (2.3):*

$$\forall x, x \in \prod_{i \in I} E_i \Leftrightarrow (\mathrm{Fnc}(x) \wedge \mathrm{Dom}\, x = I \wedge \forall i \in I, x_i \in E_i).$$

For all $i \in I$, the *i-th projection* is the function π_i from $\prod_{j \in I} E_j$ to E_i evaluating every family x at $i : \pi_i(x) = x_i$. This is the function evaluator curried in the unnatural order.

These operators are "equivalent" in the sense that they are definable from each other:

$$\mathcal{P}(E) = \{\{x \in E | f(x) = 1\} | f \in {V_2}^E\}$$

$$F^E = \prod\nolimits_{x \in E} F = (\{(\epsilon\overrightarrow{R}(x))_{x \in E} | R \subset E \times F \wedge \forall x \in E, \exists! : \overrightarrow{R}(x)\}$$

$$\prod_{i \in I} E_i = \{x \in (\bigcup_{i \in I} E_i)^I | \forall i \in I, x_i \in E_i\} = \{(\epsilon\overrightarrow{R}(i))_{i \in I} | R \subset \coprod_{i \in I} E_i \wedge \forall x \in E, \exists! : \overrightarrow{R}(x)\}$$

Even some cases are expressible from previous tools:

$$F^{\{a\}} = \{\{a\} \ni x \mapsto y | y \in F\} \qquad F^{\emptyset} = \{\emptyset\} \qquad \mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$$

$$\prod_{i\in I\cup J} E_i = \left\{(i \in I?x_i : y_i)_{i\in I\cup J} \middle| (x,y) \in \prod_{i\in I} E_i \times \prod_{i\in J} E_i\right\}$$

$$(\exists i \in I, E_i = \emptyset) \Rightarrow \prod_{i\in I} E_i = \emptyset \qquad (\forall i \in I, \exists! : E_i) \Rightarrow \prod_{i\in I} E_i = \{(\epsilon E_i)_{i\in I}\}$$

If $F \subset F'$ then $\mathcal{P}(F) \subset \mathcal{P}(F')$, $F^E \subset {F'}^E$, and $(\forall i \in I, E_i \subset E'_i) \Rightarrow \prod_{i\in I} E_i \subset \prod_{i\in I} E'_i$.

Cantor Theorem. $\forall_{\text{Set}} E, \forall_{\text{Fnc}} f, \operatorname{Dom} f = E \Rightarrow \mathcal{P}(E) \not\subset \operatorname{Im} f$.

Proof: $F = \{x \in E | x \notin f(x)\} \Rightarrow (\forall x \in E, x \in F \not\Leftrightarrow x \in f(x)) \Rightarrow (\forall x \in E, F \neq f(x)) \Rightarrow F \notin \operatorname{Im} f$. □
(The Russell paradox may be seen as a particular case)

2.6. Injectivity and inversion

A function $f : E \to F$ is *injective* (or : an *injection*) if ${}^t\mathrm{Gr}\, f$ is a functional graph:

$$\begin{aligned} \operatorname{Inj} f &\Leftrightarrow (\forall y \in F, !\!: f^\bullet(y)) \\ &\Leftrightarrow (\forall x, x' \in E, f(x) = f(x') \Rightarrow x = x') \\ &\Leftrightarrow (\forall x, x' \in E, x \neq x' \Rightarrow f(x) \neq f(x')) \end{aligned}$$

Then its *inverse* is defined by $f^{-1} = (\operatorname{Im} f \ni y \mapsto \epsilon f^\bullet(y))$ so that $\mathrm{Gr}(f^{-1}) = {}^t\mathrm{Gr}\, f$.

A function $f : E \to F$ is said *bijective* (or a *bijection*) from E onto F, and we write $f : E \leftrightarrow F$, if it is injective and surjective: $\forall y \in F, \exists! : f^\bullet(y)$, in which case $f^{-1} : F \leftrightarrow E$.

A *permutation* (or *transformation*) of a set E is a bijection $f : E \leftrightarrow E$.

Proposition. Let $f : E \to F$ and $g : F \to G$.
1. $(\operatorname{Inj} f \wedge \operatorname{Inj} g) \Rightarrow \operatorname{Inj}(g \circ f)$
2. $\operatorname{Inj}(g \circ f) \Rightarrow \operatorname{Inj} f$
3. $\operatorname{Im}(g \circ f) = g[\operatorname{Im} f] \subset \operatorname{Im} g$.
4. $\operatorname{Im}(g \circ f) = G \Rightarrow \operatorname{Im} g = G$.
5. $\operatorname{Im} f = F \Rightarrow \operatorname{Im}(g \circ f) = \operatorname{Im} g$, so that $((f : E \twoheadrightarrow F) \wedge (g : F \twoheadrightarrow G)) \Rightarrow (g \circ f : E \twoheadrightarrow G)$

Proofs:
1. $(\operatorname{Inj} f \wedge \operatorname{Inj} g) \Rightarrow \forall x, y \in E, g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y) \Rightarrow x = y$.
2. $\forall x, y \in E, f(x) = f(y) \Rightarrow g(f(x)) = (g(f(y)) \Rightarrow x = y$.
3. $\forall z \in G, z \in \operatorname{Im}(g \circ f) \Leftrightarrow (\exists x \in E, g(f(x)) = z) \Leftrightarrow (\exists y \in \operatorname{Im} f, g(y) = z) \Leftrightarrow z \in g[\operatorname{Im} f]$.

3. ⇒ 4. and 3. ⇒ 5. are obvious. □

Proposition. *For any sets E, F, G and any $f \in F^E$,*

$$\operatorname{Im} f = F \Rightarrow \operatorname{Inj}(G^F \ni g \mapsto g \circ f) \Rightarrow (\operatorname{Im} f = F \vee !\!: G)$$
$$(\operatorname{Inj} f \wedge G \neq \emptyset) \Rightarrow \{g \circ f | g \in G^F\} = G^E \Rightarrow (\operatorname{Inj} f \vee !\!: G)$$
$$(E \subset F \wedge G \neq \emptyset) \Rightarrow \{g_{|E} | g \in G^F\} = G^E$$
$$(\operatorname{Inj} f \wedge E \neq \emptyset) \Rightarrow \exists g \in E^F, g \circ f = \mathrm{Id}_E$$

Proofs :
$\operatorname{Im} f = F \Rightarrow \forall g, h \in G^F, ((\forall x \in E, g(f(x)) = h(f(x))) \Leftrightarrow (\forall y \in F, g(y) = h(y) \Leftrightarrow g = h))$.
$\forall z, z' \in G, (y \mapsto z) \circ f = (y \mapsto (y \in \operatorname{Im} f?z : z')) \circ f$ thus $\operatorname{Inj}(g \mapsto g \circ f) \Rightarrow (z = z' \vee \operatorname{Im} f = F)$.
$\forall z \in G, \forall h \in G^E, \operatorname{Inj} f \Rightarrow (F \ni y \mapsto (y \in \operatorname{Im} f?h \circ f^{-1}(y) : z)) \circ f = h$.
$\forall z, z' \in G, \forall x \in E$, if $g \in G^F$ is such that $\forall y \in E, g(f(y)) = (y = x?z : z')$, then $\forall y \in E$,
$f(y) = f(x) \Rightarrow g(f(y)) = g(f(x)) = z \Rightarrow (y = x \vee z = z')$.
The last formulas are particular cases of the second one. □

Let $f : E \to F$ and $f^*_F : \mathcal{P}(F) \to \mathcal{P}(E)$ defined by f^*. Then (by $G = V_2$ and $\forall B \subset \operatorname{Im} f, f[f^*(B)] = B$),

$$\begin{aligned} \operatorname{Inj} f &\Leftrightarrow \operatorname{Im} f^*_F = \mathcal{P}(E) \\ \operatorname{Im} f = F &\Leftrightarrow \operatorname{Inj} f^*_F \\ \operatorname{Im} f_* &= \{f[A] | A \subset E\} = \mathcal{P}(\operatorname{Im} f) \end{aligned}$$

Proposition. *Let* $F = \operatorname{Dom} g$. *Then* $\operatorname{Inj} g \Rightarrow \operatorname{Inj}(F^E \ni f \mapsto g \circ f) \Rightarrow (\operatorname{Inj} g \vee E = \emptyset)$.

Proofs: $\forall f, f' \in F^E, (\operatorname{Inj} g \wedge \forall x \in E, g(f(x)) = g(f'(x))) \Rightarrow (\forall x \in E, f(x) = f'(x))$.
Then from the middle formula, $\forall y, z \in F$,
$g(y) = g(z) \Rightarrow g \circ (E \ni x \mapsto y) = g \circ (E \ni x \mapsto z) \Rightarrow (\forall x \in E, y = z) \Rightarrow (y = z \vee E = \emptyset)$. ☐

Proposition. *Let* $f : E \to F$ *and* $\operatorname{Dom} g = F$. *Then*

$$\begin{aligned} g \circ f = \operatorname{Id}_E &\Leftrightarrow (\forall x \in E, \forall y \in F, f(x) = y \Rightarrow g(y) = x) \\ &\Leftrightarrow (\operatorname{Gr} f \subset {}^t\operatorname{Gr} g) \;\Leftrightarrow\; (\forall y \in F, f^\bullet(y) \subset \{g(y)\}) \\ &\Leftrightarrow (\forall x \in E, f(x) \in g^\bullet(x)) \;\Leftrightarrow\; (\operatorname{Inj} f \wedge g_{|\operatorname{Im} f} = f^{-1}) \\ &\Rightarrow E \subset \operatorname{Im} g \end{aligned}$$

$$(g : F \to E \wedge g \circ f = \operatorname{Id}_E) \Rightarrow (\operatorname{Im} f = F \Leftrightarrow \operatorname{Inj} g \Leftrightarrow f \circ g = \operatorname{Id}_F \Leftrightarrow g = f^{-1}).$$

Proof of the last formula: $(\operatorname{Inj} g \wedge g \circ f \circ g = g \circ \operatorname{Id}_F) \Rightarrow f \circ g = \operatorname{Id}_F$. ☐

Proposition. *1) If* f, g *are injective and* $\operatorname{Im} f = \operatorname{Dom} g$, *then* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
2) If $f, h : E \to F$ *and* $g : F \to E$ *then* $(g \circ f = \operatorname{Id}_E \wedge h \circ g = \operatorname{Id}_F) \Leftrightarrow ((g : F \leftrightarrow E) \wedge f = h = g^{-1})$.

Proofs:
1) $\forall x \in \operatorname{Dom} f, \forall y \in \operatorname{Im} g, (g \circ f)(x) = y \Leftrightarrow f(x) = g^{-1}(y) \Leftrightarrow x = (f^{-1} \circ g^{-1})(y)$.
Other method: $(g \circ f)^{-1} = (g \circ f)^{-1} \circ g \circ g^{-1} = (g \circ f)^{-1} \circ g \circ f \circ f^{-1} \circ g^{-1} = f^{-1} \circ g^{-1}$.
2) We deduce $f = h$ from $f = h \circ g \circ f = h$, or from $\operatorname{Gr} f \subset {}^t\operatorname{Gr} g \subset \operatorname{Gr} h$. The rest is obvious. ☐

2.7. Properties of binary relations on a set ; ordered sets

A *binary relation on* E is a graph $R \subset E \times E$. Denoting $x\,R\,y \Leftrightarrow (x, y) \in R$ and letting the domain E of quantifiers implicit, it will be said

reflexive	$\Leftrightarrow$	$\forall x,\ x\,R\,x$
irreflexive	$\Leftrightarrow$	$\forall x,\ \neg(x\,R\,x)$
symmetric	$\Leftrightarrow$	$R \subset {}^tR \quad\Leftrightarrow\quad R = {}^tR \quad\Leftrightarrow\quad \overrightarrow{R} = \overleftarrow{R}$
antisymmetric	$\Leftrightarrow$	$\forall x, y,\ (x\,R\,y \wedge y\,R\,x) \Rightarrow x = y$
transitive	$\Leftrightarrow$	$\forall x, y, z,\ (x\,R\,y \wedge y\,R\,z) \Rightarrow x\,R\,z$

For any transitive binary relation R we denote $x\,R\,y\,R\,z \Leftrightarrow ((x\,R\,y) \wedge (y\,R\,z)) \Rightarrow x\,R\,z$.

Example. Let $A \subset E^E$ and $R = \bigcup_{f \in A} \operatorname{Gr} f$. Then
$(\operatorname{Id}_E \in A) \Rightarrow R$ is reflexive
$(\forall f, g \in A, g \circ f \in A) \Rightarrow R$ is transitive
$(\forall f \in A, f : E \leftrightarrow E \wedge f^{-1} \in A) \Rightarrow R$ is symmetric

Preorder. *A preorder* R *on a set* E *is a reflexive and transitive binary relation on* E. *Equivalently,*

$$\forall x, y \in E,\ x\,R\,y \Leftrightarrow \overleftarrow{R}(x) \subset \overleftarrow{R}(y)$$

Proof: $\forall x, y \in E,\ x \in \overleftarrow{R}(x) \subset \overleftarrow{R}(y) \Rightarrow x\,R\,y$; transitivity says $x\,R\,y \Rightarrow \overleftarrow{R}(x) \subset \overleftarrow{R}(y)$. ☐

Note : ${}^tR$ is then also a preorder, i.e. $x\,R\,y \Leftrightarrow \overrightarrow{R}(y) \subset \overrightarrow{R}(x)$.

Ordered set. *An* order *is an antisymmetric preorder. A* preordered set *is a set* E *with a preorder* R. *An* ordered set *is a set with an order, usually written as* $\leq$.

For x, y in an ordered set E, the formula $x \leq y$ can be read "x is less than y", or "y is greater than x". The elements x and y are said *incomparable* when $\neg(x \leq y \vee y \leq x)$. (This implies $x \neq y$).

Any subset F of a set E with an order (resp. a preorder) $R \subset E \times E$, is also ordered (resp. preordered) by its restriction $R \cap (F \times F)$ (which is an order, resp. preorder, on F).

Strict order. *It is a binary relation both transitive and irreflexive; and thus also antisymmetric.*

Strict orders $<$ bijectively correspond to orders $\leq$ by $x < y \Leftrightarrow (x \leq y \wedge x \neq y)$.
The inverse correspondence is defined by $x \leq y \Leftrightarrow (x < y \vee x = y)$.

Total order. *A total order on a set* E *is an order* R *on* E *where no two elements are incomparable :* $\forall x, y \in E, x \leq y \vee y \leq x$, i.e. $R \cup {}^tR = E \times E$.

Equivalently, it is an order related with its strict order $<$ by $\forall x, y \in E, x < y \not\Leftrightarrow y \leq x$.
Still equivalently, it is a transitive relation $\leq$ such that $\forall x, y \in E, x \leq y \Leftrightarrow (y \leq x \Rightarrow x = y)$.

A strict order associated with a total order, called a *strict total order*, is any transitive relation $<$ in E such that $\forall x, y \in E, x < y \not\Leftrightarrow (y < x \vee x = y)$, or equivalently $\forall x, y \in E, x = y \not\Leftrightarrow (y < x \vee x < y)$).

Monotone, antitone, strictly monotone functions

Between ordered sets E and F, a function $f : E \to F$ will be said :
— *monotone* if $\forall x, y \in E, x \leq y \Rightarrow f(x) \leq f(y)$
— *antitone* if $\forall x, y \in E, x \leq y \Rightarrow f(y) \leq f(x)$
— *strictly monotone* if $\forall x, y \in E, x \leq y \Leftrightarrow f(x) \leq f(y)$
— *strictly antitone* if $\forall x, y \in E, x \leq y \Leftrightarrow f(y) \leq f(x)$.

Any composite of a chain of monotone or antitone functions, is monotone if the number of antitone functions in the chain is even, or antitone if it is odd.

Any strictly monotone or strictly antitone function is injective.

If $f \in F^E$ and $g \in E^F$ are both monotone (resp. both antitone) and $g \circ f = \mathrm{Id}_E$, then f is strictly monotone (resp. strictly antitone).

Order on sets of functions

For all sets E, F where F is ordered, the set F^E (and thus any subset of F^E) is ordered by

$$f \leq g \Leftrightarrow (\forall x \in E, f(x) \leq g(x))$$

Then, $\forall f, g \in F^E, \forall h \in E^G, f \leq g \Rightarrow f \circ h \leq g \circ h$, i.e. $f \mapsto f \circ h$ is always monotone.

The particular case $F = V_2$ is that $\mathcal{P}(E)$ (and thus any set of sets) is naturally ordered by $\subset$, and that h^* is monotone from $\mathcal{P}(E)$ to $\mathcal{P}(G)$.

If F and G are ordered and $u \in G^F$ is monotone (resp. antitone) then $F^E \ni f \mapsto u \circ f \in G^E$ is monotone (resp. antitone).

In an ordered set E, a function $f \in E^E$ is said *extensive* if $\forall x \in E, x \leq f(x)$, i.e. $\mathrm{Id}_E \leq f$. The composite of two extensive functions is extensive.

2.8. Canonical bijections

For all objects x, y we shall say that x determines y if there is an invariant functor T such that $T(x) = y$. Then the role of y as free variable can be played by the term $T(x)$, thus by the use of x. This is a preorder on the universe, but not a predicate of set theory as it involves a meta-concept. Instead, it is meant to abbreviate the use of T. Similarly, a function $f : E \to F$ will be said *canonical* if it is defined as $E \ni x \to T(x)$ for some invariant functor T. A bijection f will be said *bicanonical* if both f and f^{-1} are canonical. When a bijection $f : E \leftrightarrow F$ is canonical (resp. bicanonical), we write $f : E \cong F$ (resp. $f : E \equiv F$); or, using its defining functor, $T : E \cong F$ which means that $(E \ni x \mapsto T(x))$ is injective with image F. We shall write $E \cong F$ (resp. $E \equiv F$) to mean the existence of a canonical (resp. bicanonical) bijection, that is kept implicit.

Canonical bijections can fail to be bicanonical especially when their defining functor is not injective: ${V_2}^E \cong \mathcal{P}(E)$, $\{x\}^E \cong \{x\}$ and $E \times \{x\} \cong E$, whereas $\{x\} \times E \equiv E^{\{x\}}$ and $E \equiv \{0\} \times E$.

This is a preorder on the class of sets, preserved by constructions: for example if $E \cong E'$ and $F \cong F'$ then $E \times F \cong E' \times F'$ and $F^E \cong F'^{E'}$ using the direct image of the graph (while we may not have $F^{E'} \cong F'^E$ when E' does not determine E). It will often look like a property of numbers as the existence of a bijection between finite sets implies the equality of their numbers of elements.

The transposition of oriented pairs ($E \times F \equiv F \times E$) extends to graphs ($\mathcal{P}(E \times F) \equiv \mathcal{P}(F \times E)$) and to operations: $G^{E \times F} \equiv G^{F \times E}$ where $f \in G^{E \times F}$ is transposed by ${}^t f(x, y) = f(y, x)$.

Sums of sets, sums of functions

If $S = \coprod_{i \in I} E_i$ then $\coprod : \prod_{i \in I} \mathcal{P}(E_i) \cong \mathcal{P}(S)$, whose inverse $S \supset R \mapsto \overrightarrow{R}_I = (I \ni i \mapsto \overrightarrow{R}(i))$ depends on I. In particular for two sets E and F we have $(\mathcal{P}(F))^E \cong \mathcal{P}(E \times F)$.

The sum over I of functions f_i where $\forall i \in I, E_i = \mathrm{Dom}\, f_i$ is defined by

$$\coprod_{i \in I} f_i = (S \ni (i, x) \mapsto f_i(x))$$

$$f = \coprod_{i \in I} f_i \Leftrightarrow (\mathrm{Dom}\, f = S \wedge \forall i \in I, f_i = \overrightarrow{f}(i) = f \circ j_i) \quad \text{where } j_i = (E_i \ni x \mapsto (i, x))$$

Thus the canonical bijections (bicanonical if $I = \mathrm{Dom}\, S$, thus if $E \neq \emptyset$ in the case $I \times E$)

$$\prod_{i \in I} F^{E_i} \cong F^S \qquad \prod_{i \in I} \prod_{x \in E_i} F_{(i,x)} \cong \prod_{c \in S} F_c$$

$$(F^E)^I \cong F^{I \times E} \qquad (E \times F) \times G \equiv E \times F \times G$$

$$(f_i)_{i \in I} \in (F^E)^I \Rightarrow \coprod_{i \in I} \mathrm{Gr}\, f_i \subset \mathcal{P}(I \times (E \times F)) \equiv \mathcal{P}((I \times E) \times F) \supset \mathrm{Gr} \coprod_{i \in I} f_i$$

Product of functions or recurrying

Transposing a relation R exchanges its curried forms $\overrightarrow{R}$ and $\overleftarrow{R}$, by a bijection $(\mathcal{P}(F))^E \leftrightarrow (\mathcal{P}(E))^F$ with parameter F. Similarly we have a bijection $(F^E)^I \leftrightarrow (F^I)^E$, canonical if $I \neq \emptyset$ (to let $(F^E)^I$ determine E), defined by a binder $\prod$ called the *product* of the functions $f_i \in F^E$ for $i \in I$:

$$\begin{aligned}
(f_i)_{i\in I} \in \prod_{i\in I} F_i^E \cong (\prod_{i\in I} F_i)^E \ni \prod_{i\in I} f_i = (E \ni x \mapsto (f_i(x))_{i\in I})\\
\forall g, g = \prod_{i\in I} f_i \Leftrightarrow (g : E \to \prod_{i\in I} \operatorname{Im} f_i \wedge \forall i \in I, f_i = \pi_i \circ g)\\
\operatorname{Dom} f = \operatorname{Dom} g = E \Rightarrow \quad f \times g = (E \ni x \mapsto (f(x), g(x)))\\
I^E \times F^E \equiv (I \times F)^E\\
\coprod_{\phi\in I^E} \prod_{x\in E} F_{\phi(x)} \equiv (\coprod_{i\in I} F_i)^E.
\end{aligned}$$

2.9. Equivalence relations and partitions

Indexed partitions

A family of sets $(A_i)_{i\in I}$ is called *pairwise disjoint* when any pair of them is disjoint :

$$\forall i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset$$

Equivalently, $(\forall (i, x), (j, y) \in \coprod_{k\in I} A_k, x = y \Rightarrow i = j)$, thus $\exists f, \operatorname{Gr} f = {}^t\coprod_{i\in I} A_i$ with

$$\begin{aligned}
\operatorname{Dom} f = \operatorname{Im} \coprod_{i\in I} A_i = \bigcup_{i\in I} A_i\\
\operatorname{Im} f = \{i \in I | A_i \neq \emptyset\}
\end{aligned}$$

Inversely, any $f \in F^E$ defines a family $f^\bullet_F = (f^\bullet(y))_{y\in F} \in \mathcal{P}(E)^F$ of pairwise disjoint sets :

$$\forall y, z \in F, f^\bullet(y) \cap f^\bullet(z) \neq \emptyset \Rightarrow \exists x \in f^\bullet(y) \cap f^\bullet(z), y = f(x) = z$$

An *indexed partition* of a set E is a family of nonempty, pairwise disjoint subsets of E, whose union is E. It is always injective : $\forall i, j \in I, A_i = A_j \Rightarrow A_i \cap A_j = A_i \neq \emptyset \Rightarrow i = j$.

Equivalence relation associated with a function

An *equivalence relation* is a symmetric preorder. Any $f : E \to F$ defines an equivalence relation on E by

$$\underset{f}{\sim} = \{(x, y) \in E | f(x) = f(y)\} = \coprod (f^\bullet \circ f)$$

Its composite $g = h \circ f$ with any $h \in G^F$ satisfies $\underset{f}{\sim} \subset \underset{g}{\sim}$, with

$$\underset{f}{\sim} = \underset{g}{\sim} \Leftrightarrow \operatorname{Inj} h_{|\operatorname{Im} f} \Rightarrow f = (h_{|\operatorname{Im} f})^{-1} \circ g$$

In particular, $\underset{f}{\sim}$ coincides with the equality relation $\operatorname{Gr}\operatorname{Id}_E$ on E when f is injective.

As $\underset{f}{\overrightarrow{\sim}} = f^\bullet \circ f$, the injectivity of the indexed partition $f^\bullet_{\operatorname{Im} f}$ (that we will abusively denote as $f^\bullet$) gives the characteristic identity of equivalence relations : $x \underset{f}{\sim} y \Leftrightarrow \underset{f}{\overrightarrow{\sim}}(x) = \underset{f}{\overrightarrow{\sim}}(y)$.

If $F = \operatorname{Im} f$, the injection (2.6) $G^F \ni h \mapsto h \circ f$ has image $\{g \in G^E | \underset{f}{\sim} \subset \underset{g}{\sim}\}$: letting $H = \operatorname{Im}(f \times g)$, $(\underset{f}{\sim} \subset \underset{g}{\sim} \Leftrightarrow \forall (y, z), (y', z') \in H, y = y' \Rightarrow z = z') \wedge \operatorname{Dom} H = F \wedge (\forall h \in G^F, g = h \circ f \Leftrightarrow H \subset \operatorname{Gr} h)$.

For any functions f, g such that $\operatorname{Dom} f = \operatorname{Dom} g \wedge \underset{f}{\sim} \subset \underset{g}{\sim}$, the function with graph $\operatorname{Im}(f \times g)$ is called the *quotient* $g/f : \operatorname{Im} f \twoheadrightarrow \operatorname{Im} g$, and is the only function h such that $\operatorname{Dom} h = \operatorname{Im} f \wedge g = h \circ f$.

Inversion comes as a particular case: $\operatorname{Inj} f \Rightarrow f^{-1} = \operatorname{Id}_{\operatorname{Dom} f}/f$.

Remark. *if R is reflexive and $\forall x, y, z, (x\ R\ y \wedge z\ R\ y) \Rightarrow z\ R\ x$ then R is an equivalence relation.*

Proof : symmetry is verified as: $\forall x, y, (x\ R\ y \wedge y\ R\ y) \Rightarrow y\ R\ x$. Then comes transitivity. $\square$

Partition, canonical surjection

A *partition of* E is a set of nonempty, pairwise disjoint sets whose union is E, thus the image of any indexed partition $f^\bullet$ of E (where f is any function with domain E): $P = \operatorname{Im} f^\bullet = \operatorname{Im}(f^\bullet \circ f)$.

$\forall R \subset E \times E, \forall P \subset \mathcal{P}(E)$, if $P = \operatorname{Im} \overrightarrow{R}_E$ then

$$(\forall x, y \in E, x \in \overrightarrow{R}(y) \Leftrightarrow \overrightarrow{R}(x) = \overrightarrow{R}(y)) \Leftrightarrow (\forall x \in E, \forall A \in P, x \in A \Leftrightarrow \overrightarrow{R}(x) = A) \Leftrightarrow \operatorname{Id}_P = (\overrightarrow{R}_E)^\bullet$$

Thus if R is an equivalence relation then P is a partition.

Conversely for any partition P of E, $\exists! g \in P^E, \operatorname{Id}_P = g^\bullet$ thus $P = \operatorname{Dom} g^\bullet = \operatorname{Im} g$ and

$$R = \coprod g \subset E \times E \Rightarrow \operatorname{Id}_P = (\overrightarrow{R}_E)^\bullet$$

thus R is an equivalence relation, where $x\ R\ y \Leftrightarrow (\exists A \in P, x \in A \wedge y \in A) \Leftrightarrow (\forall A \in P, x \in A \Rightarrow y \in A)$.

The partition $\operatorname{Im} \overrightarrow{R}$ associated with an equivalence relation R on E is called the *quotient of* E *by* R and denoted E/R; the function $\overrightarrow{R}$ is the *canonical surjection* from E to E/R. For all $x \in E$, $\overrightarrow{R}(x)$ is the only element of E/R containing x, and called the *class of* x *by* R.

Order quotient of a preorder

Any preordered set (E, R) is reflected through $\overleftarrow{R}$ by the ordered set $(\operatorname{Im} \overleftarrow{R}, \subset)$, with

$$\overleftarrow{R}(x) = \overleftarrow{R}(y) \Leftrightarrow (\overleftarrow{R}(x) \subset \overleftarrow{R}(y) \wedge \overleftarrow{R}(y) \subset \overleftarrow{R}(x)) \Leftrightarrow (x\ R\ y \wedge y\ R\ x)$$

so that $\overleftarrow{R}$ is injective if and only if R is an order. Through $\overleftarrow{R}$, the preorder R is reduced to the order relation $\subset$ in $\operatorname{Im} \overleftarrow{R}$, which plays the role of the quotient of R in the quotient set $E/(R \cap {}^tR)$.

On each (ordered) set E, only one order will usually be considered, denoted $\leq_E$, or abusively $\leq$. This may be justified by defining ordered sets as sets of sets, ordered by $\subset$, ignoring their elements.

2.10. Axiom of choice

The axiom of choice is a claim with several equivalent formulations, named as an "axiom" because it cannot be deduced from other axioms of set theory but it "feels true" and, when taken as an axiom, it does not increase the risk of contractions but has convenient consequences. But we will actually not need it in the rest of this work.

Axiom of choice (AC). *It says* $\forall_{\text{Set}} X, \text{AC}_X$, *where* AC_X *names the following equivalent claims*
(1) $\forall_{\text{Set}} E, \forall R \subset X \times E, (\forall x \in X, \exists y \in E, xRy) \Rightarrow (\exists f \in E^X, \forall x \in X, xRf(x))$.
Or in short : for any graph $R, X = \operatorname{Dom} R \Rightarrow \exists f \in (\operatorname{Im} R)^X, \operatorname{Gr} f \subset R$.
(2) Any product over X *of nonempty sets is nonempty :* $(\forall x \in X, A_x \neq \emptyset) \Rightarrow \prod_{x \in X} A_x \neq \emptyset$.
(3) $\forall_{\text{Fnc}} g, \operatorname{Im} g = X \Rightarrow \exists f \in (\operatorname{Dom} g)^X, g \circ f = \operatorname{Id}_X$.

Proof of equivalence :
(1) $\Rightarrow$ (2) by $R = \coprod_{x \in X} A_x$;
(2) $\Rightarrow$ (3) by $A_x = g^\bullet(x)$;
(3) $\Rightarrow$ (1) $\operatorname{Im} \pi_{0|R} = \operatorname{Dom} R = X \Rightarrow \exists (h \times f) \in R^X, h = \operatorname{Id}_X \wedge \operatorname{Gr} f \subset R$. □

(We also have (2) $\Rightarrow$ (1) by $A_x = \overrightarrow{R}(x)$, and (1) $\Rightarrow$ (3) by $R = {}^t\operatorname{Gr} g$)

Theorem. *Each of the following claims is equivalent to the axiom of choice:*
(4) For any set E *of sets,* $\emptyset \notin E \Rightarrow (\prod_{A \in E} A) \neq \emptyset$.
(5) For any partition P *of a set* $E, \exists K \subset E, \forall A \in P, \exists! : K \cap A$
(6) For any sets E, F, G *and any* $g : F \twoheadrightarrow G, \{g \circ f | f \in F^E\} = G^E$.

Proofs: (2) $\Rightarrow$ (4) is obvious ;
(4) $\Rightarrow$ (5) $(x \in \prod_{A \in P} A \wedge K = \operatorname{Im} x) \Rightarrow (K \subset E \wedge \forall A \in P, x_A \in A \wedge \forall B \in P, x_B \in A \cap B \Rightarrow A = B)$
(5) $\Rightarrow$ (3) Let $P = \operatorname{Im} g^\bullet$. Then $f = (X \ni x \mapsto \epsilon(K \cap g^\bullet(x))) = g_{|K}^{-1} \Rightarrow g \circ f = \operatorname{Id}_X$.
$(\text{AC}_E 1) \Rightarrow (6)$ $\forall h \in G^E, (\forall x \in E, \exists y \in F, g(y) = h(x)) \Rightarrow (\exists f \in F^E, \forall x \in E, g(f(x)) = h(x))$
$(\text{AC}_G 3) \Rightarrow (6)$: $\exists i \in F^G, g \circ i = \operatorname{Id}_G \wedge \forall h \in G^E, i \circ h \in F^E \wedge g \circ i \circ h = h$.
(6) $\Rightarrow$ (3) : $E = G \Rightarrow \operatorname{Id}_E \in \{g \circ f | f \in F^E\}$. □

Remarks:

(4) $\Rightarrow$ (2) is also easy : $\emptyset \notin \{A_i | i \in I\} = E$, then $f \in \prod_{A \in E} A \Rightarrow (f(A_i))_{i \in I} \in \prod_{i \in I} A_i$.

(6) has a converse : $(\operatorname{Dom} g = F \wedge E \neq \emptyset \wedge \{g \circ f | f \in F^E\} = G^E) \Rightarrow \operatorname{Im} g = G$.

AC_X can be proven for finite X : for small X by using one variable per element; a general proof using an abstract definition of finiteness will be presented later.

2.11. Notion of Galois connection

The set of fixed points of a function f is written $\operatorname{Fix} f = \{x \in \operatorname{Dom} f | f(x) = x\} \subset \operatorname{Im} f$. Then,
$\operatorname{Im} f \subset \operatorname{Fix} g \Leftrightarrow ((\operatorname{Im} f \subset \operatorname{Dom} g) \wedge (g \circ f = f))$
$\operatorname{Im} f = \operatorname{Fix} f \Leftrightarrow ((\operatorname{Im} f \subset \operatorname{Dom} f) \wedge (f \circ f = f))$: such a function f is called *idempotent*.

Definition. *For any ordered sets E, F, and $F^- = F$ with the transposed order, the sets of antitone Galois connections between E and F, and monotone Galois connections from E to F, are defined by*

$$\operatorname{Gal}(E,F) = \{(\perp,\top) \in F^E \times E^F | \forall x \in E, \forall y \in F, x \leq_E \top(y) \Leftrightarrow y \leq_F \perp(x)\} = {}^t\operatorname{Gal}(F,E)$$
$$\operatorname{Gal}^+(E,F) = \{(u,v) \in F^E \times E^F | \forall x \in E, \forall y \in F, x \leq_E v(y) \Leftrightarrow u(x) \leq_F y\} = \operatorname{Gal}(E,F^-)$$

Fundamental example. Any relation $R \subset X \times Y$ defines a $(\perp,\top) \in \operatorname{Gal}(\mathcal{P}(X),\mathcal{P}(Y))$ by

$$\forall A \subset X, \perp(A) = \{y \in Y | \forall x \in A, x\ R\ y\} = \bigcap_{x \in A} \overrightarrow{R}(x)$$
$$\forall B \subset Y, \top(B) = \{x \in X | \forall y \in B, x\ R\ y\} = \{x \in X | B \subset \overrightarrow{R}(x)\}$$
$$\perp(\emptyset) = Y \qquad \top(\emptyset) = X$$

Proof : $\forall A \subset X, \forall B \subset F, \quad A \subset \top(B) \Leftrightarrow (\forall x \in A, \forall y \in B, x\ R\ y) \Leftrightarrow B \subset \perp(A)$. ☐

This will later be shown to be a bijection : $\operatorname{Gal}(\mathcal{P}(X),\mathcal{P}(Y)) \cong \mathcal{P}(X \times Y)$.

Lemma. $\forall \perp \in F^E, !\top \in E^F, (\perp,\top) \in \operatorname{Gal}(E,F)$.

Proof: $\forall \top \in E^F, (\perp,\top) \in \operatorname{Gal}(E,F) \Leftrightarrow \overleftarrow{\leq}_E \circ \top = \perp^* \circ \overrightarrow{\leq}_F$, but $\overleftarrow{\leq}_E$ is injective. ☐

Properties. For all $(\perp,\top) \in \operatorname{Gal}(E,F)$, the closures $\operatorname{Cl} = \top \circ \perp \in E^E$ and $\operatorname{Cl}' = \perp \circ \top \in F^F$ satisfy
1) Cl and Cl' are extensive.
2) $\perp$ and $\top$ are antitone
3) Cl and Cl' are monotone
4) $\perp \circ \top \circ \perp = \perp$, and similarly $\top \circ \perp \circ \top = \top$
5) $\operatorname{Im} \top = \operatorname{Im} \operatorname{Cl} = \operatorname{Fix} \operatorname{Cl}$, called the set of *closed* elements of E
6) $\operatorname{Cl} \circ \operatorname{Cl} = \operatorname{Cl}$
7) ($\perp$ strictly antitone) $\Leftrightarrow \operatorname{Inj} \perp \Leftrightarrow \operatorname{Cl} = \operatorname{Id}_E \Leftrightarrow \operatorname{Im} \top = E$
8) $\forall x, x' \in E, \perp(x) \leq \perp(x') \Leftrightarrow (\operatorname{Im} \top \cap \overrightarrow{\leq}(x) \subset \overrightarrow{\leq}(x'))$.
9) Denoting $K = \operatorname{Im} \top$, $\top \circ \perp_{|K} = \operatorname{Id}_K$ thus $\perp_{|K}$ is strictly antitone and ${\perp_{|K}}^{-1} = \top_{|\operatorname{Im} \perp}$.

Proofs:
1) $\perp(x) \leq \perp(x) \Rightarrow x \leq \top(\perp(x))$.
1) $\Rightarrow$ 2) $\forall x, y \in E, x \leq y \leq \top(\perp(y)) \Rightarrow \perp(y) \leq \perp(x)$.
1) $\wedge$ 2) $\Rightarrow$ 4) $\operatorname{Id}_E \leq \operatorname{Cl} \Rightarrow \perp \circ \operatorname{Cl} \leq \perp \leq \operatorname{Cl}' \circ \perp = \perp \circ \top \circ \perp$.
4) $\Rightarrow$ 5) $\operatorname{Cl} = \top \circ \perp \Rightarrow \operatorname{Im} \operatorname{Cl} \subset \operatorname{Im} \top$; $\operatorname{Cl} \circ \top = \top \Rightarrow \operatorname{Im} \top \subset \operatorname{Fix} \operatorname{Cl} \subset \operatorname{Im} \operatorname{Cl}$.
2) $\Rightarrow$ 3) and 4) $\Rightarrow$ 6) are obvious.
7) $(\operatorname{Inj} \perp \wedge \perp \circ \operatorname{Cl} = \perp) \Leftrightarrow \operatorname{Cl} = \operatorname{Id}_E \Leftrightarrow (\operatorname{Im} \top = E \wedge \operatorname{Cl} \circ \top = \top)$;
$\operatorname{Cl} = \operatorname{Id}_E \Rightarrow \perp$ strictly antitone $\Rightarrow \operatorname{Inj} \perp$.
8) $\perp(x) \leq \perp(x') \Leftrightarrow (\forall y \in F, x \leq \top(y) \Rightarrow x' \leq \top(y))$.
9) $K = \operatorname{Fix}(\top \circ \perp) \Rightarrow \top \circ \perp \circ \operatorname{Id}_K = \operatorname{Id}_K$. Other proof : $(\perp_{|K}, \top) \in \operatorname{Gal}(K,F)$ with $\top$ surjective.
In $\top_{|\operatorname{Im} \perp} \circ \perp_{|K} = \operatorname{Id}_K$ the roles of $\top$ and $\perp$ are symmetrical. ☐

Remark. *Properties 1) and 2) conversely imply that* $(\perp,\top) \in \operatorname{Gal}(E,F)$.

Proof: $\forall x \in E, \forall y \in F, x \leq \top(y) \Rightarrow y \leq \perp(\top(y)) \leq \perp(x)$. ☐

Analogues of the above properties for monotone Galois connections are obtained by reversing the order in F: if $(u,v) \in \operatorname{Gal}^+(E,F)$ then u and v are monotone, $v \circ u$ is extensive and $u \circ v \leq \operatorname{Id}_F$.

Closure. A closure of an ordered set E is an $f \in E^E$ such that, equivalently:
1) There exists a set F and an $(u,v) \in \operatorname{Gal}(E,F)$ or $\operatorname{Gal}^+(E,F)$ such that $v \circ u = f$
2) f is monotone, idempotent and extensive
3) $\forall x \in E, \forall y \in \operatorname{Im} f, x \leq y \Leftrightarrow f(x) \leq y$, i.e. $(f, \operatorname{Id}_K) \in \operatorname{Gal}^+(E,K)$ where $K = \operatorname{Im} f$.

Proof : 3) $\Rightarrow$ 1) $\Rightarrow$ 2); for 2) $\Rightarrow$ 3), $\forall x \in E, \forall y \in K, x \leq f(x) \leq y \Rightarrow x \leq y \Rightarrow f(x) \leq f(y) = y$. ☐

Notes:
2) $\Rightarrow$ 3) is a particular case of the remark: $f \circ f = f \Rightarrow f \circ \operatorname{Id}_K \leq \operatorname{Id}_K$ (extensivity of $f \circ \operatorname{Id}_K$ in K^-).
$\forall K \subset E, \forall f \in K^E, (f, \operatorname{Id}_K) \in \operatorname{Gal}^+(E,K) \Rightarrow \operatorname{Im} f = K$ from 7) with Id_K injective.