Notes on a (very) Elementary Set Theory—Part IV

1 Ordered pair; ordered n-tuple; Cartesian Product

We continue within informal mathematics until otherwise stated.[1] We will want next to look at Cartesian products. This requires the notion of an ordered pair, that is, an object $\langle a, b\rangle$, where a and b are sets or atoms, whose "value" depends on the *position* of its two members, a and b.

By this we mean that

$$\langle a, b\rangle = \langle a', b'\rangle \Rightarrow a = a' \wedge b = b' \tag{1}$$

By now it has become a habit to omit the obvious universal quantifiers. Thus, the above is "slang" for

$$(\forall a)(\forall b)\big(\langle a, b\rangle = \langle a', b'\rangle \Rightarrow a = a' \wedge b = b'\big)$$

where a, b are variables of type set or atom.

Note that (1) implies that if $a \neq b$ then $\langle a, b\rangle \neq \langle b, a\rangle$, because what I just said is the contrapositive of $\langle a, b\rangle = \langle b, a\rangle \Rightarrow a = b \wedge b = a$.

Thus $\langle \ldots \rangle$ is not the same as $\{\ldots\}$, since we have $\{a, b\} = \{b, a\}$.

So $\langle a, b\rangle$ is an *ordered* pair of elements, unlike $\{a, b\}$. But what sort of animal is it? It would be very awkward to have to introduce a new "type" at this point of our development and have atoms, sets, and "ordered sets". Fortunately, we do not have to do this. We can "implement" the pair *as a set*, using a trick invented by the Polish mathematician Kuratowski.

There are several implementations—that is, possible *definitions* of $\langle a, b\rangle$ in terms of a and b, using set-theoretic operations. The two based on Kuratowski's idea are

(A) Implement $\langle a, b\rangle$ as $\{a, \{a, b\}\}$. We know from a previous assignment that

$$\{a, \{a, b\}\} = \{a', \{a', b'\}\} \Rightarrow a = a' \wedge b = b' \tag{i}$$

so this implementation works—that is, it satisfies (1) above.

[1]But we still apply proper logic to get results proved. In particular, we are responsible for what we assume at every step. Our "assumptions" must be realistic and not wishful thinking.

This implementation is sometimes criticised by purists in that it requires a sledgehammer: foundation. Here is another implementation that does not require foundation.

(B) Implement $\langle a, b\rangle$ as $\{\{a\}, \{a, b\}\}$. To see that this works we assume

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} \tag{2}$$

and prove

$$a = a' \tag{3}$$

and

$$b = b' \tag{4}$$

By $\vdash x = y \Rightarrow t(x, \ldots) = t(y, \ldots)$ of logic, apply $\bigcap$ to both sides of (2) and get

$$\{a\} = \bigcap\{\{a\}, \{a, b\}\} = \bigcap\{\{a'\}, \{a', b'\}\} = \{a'\}$$

from which (3) follows at once.
Now apply $\bigcup$ to both sides of (1), remembering that we have (3):

$$\{a, b\} = \bigcup\{\{a\}, \{a, b\}\} = \bigcup\{\{a\}, \{a, b'\}\} = \{a, b'\}$$

The above yields (4) by an earlier assignment.

To fix ideas, and having tossed a coin, we will adopt implementation (B). Note, of course, that for any a, b that are sets or atoms $\{\{a\}, \{a, b\}\}$ is a set (apply the axiom of [unordered] pair three times). Thus we define

Definition 1.1. For any variables x and y (set or atom type) $\langle x, y\rangle$ stands for the set $\{\{x\}, \{x, y\}\}$. We can use therefore "=":

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}$$

We call x (respectively, y) the first (respectively, second) *component* or *projection* of the ordered pair. ■

The following is useful:

Proposition 1.2.

$$ST \vdash \langle a, b\rangle = \langle a', b'\rangle \equiv a = a' \wedge b = b'$$

Proof. The $\Rightarrow$ is (1) of p.1 via definition 1.1. The $\Leftarrow$ is from the logical theorem $\vdash x = y \wedge x' = y' \Rightarrow t(x, x', \ldots) = t(y, y', \ldots)$ proved in the "the last word on Leibniz" web notes. ■

We are familiar with ordered pairs from analytic geometry: For example the coordinates of a point on the Cartesian plane are an ordered pair of real numbers. The Cartesian plane consists of all those points that are characterised by coordinates that have both the first and second projection in $\mathbb{R}$ (set of all reals). There is notation for that: If we identify the arbitrary point on the plane with the pair of real numbers, $\langle a, b\rangle$, that are its coordinates, we then write $\langle a, b\rangle \in \mathbb{R} \times \mathbb{R}$. This leads to the general definition of "$\times$":

Definition 1.3 (Cartesian Product). For any set variables S and T, $S \times T$ stands for the collection—that we will shortly show is "small enough" to be a set—$\{\langle x, y\rangle | x \in S \wedge y \in T\}$. Since this is a set, we can write $S \times T = \{\langle x, y\rangle | x \in S \wedge y \in T\}$.

We call $S \times T$ the Cartesian product of S and T (in that order). ∎

The following theorem uses the specific implementation—of 1.1—that we chose for the ordered pair. *This is the last time we will refer to the implementation.* After this, all we need to remember is that the ordered pair is a set that satisfies (1) of p.1.

Theorem 1.4. *For any choice of sets S and T, $S \times T$ of definition 1.3 is a set.*

Proof. (Informal) So, what we collect in $S \times T$ are pairs $\langle x, y\rangle$ where $x \in S$ and $y \in T$. Thus,

$$\{x\} \subseteq S \tag{1}$$

and

$$\{x, y\} \subseteq S \cup T \tag{2}$$

We rewrite (1) and (2) using the definition of $\mathscr{P}(a)$ for sets a:

$$\{x\} \in \mathscr{P}(S) \tag{1$'$}$$

and

$$\{x, y\} \in \mathscr{P}(S \cup T) \tag{2$'$}$$

Hence,

$$\{\{x\}, \{x, y\}\} \subseteq \mathscr{P}(S) \cup \mathscr{P}(S \cup T) \tag{3}$$

by (1′) and (2′). Rewriting (3) as before, we get

$$\{\{x\}, \{x, y\}\} \in \mathscr{P}\big(\mathscr{P}(S) \cup \mathscr{P}(S \cup T)\big)$$

or, using the ordered pair implementation 1.1,

$$\langle x, y\rangle \in \mathscr{P}\big(\mathscr{P}(S) \cup \mathscr{P}(S \cup T)\big)$$

This shows that $S \times T$ is part of the set[2] $\mathscr{P}\big(\mathscr{P}(S) \cup \mathscr{P}(S \cup T)\big)$ so it is itself a set by the axiom of subsets. ■

Remark 1.5. Of course (see Part I notes), $\{\langle x, y\rangle | x \in S \wedge y \in T\}$ is shorthand for

$$\Big\{z | (\exists x)(\exists y)\big(z = \langle x, y\rangle \wedge x \in S \wedge y \in T\big)\Big\}$$

In a formal setting one would now want to verify the "obvious":

$$\langle x, y\rangle \in S \times T \equiv x \in S \wedge y \in T$$

Of course, in an informal setting you omit proofs of the "obvious".[3] Here goes a formal proof:

$$\begin{aligned}
& \langle x, y\rangle \in S \times T \\
\equiv & \\
& \langle x, y\rangle \in \Big\{z | (\exists x)(\exists y)\big(z = \langle x, y\rangle \wedge x \in S \wedge y \in T\big)\Big\} \\
\equiv & \Big\langle \text{Change dummies to avoid clash with the "external" } x, y\text{; use } \in\text{-elim.} \Big\rangle \\
& (\exists u)(\exists v)\big(\langle x, y\rangle = \langle u, v\rangle \wedge u \in S \wedge v \in T\big) \\
\equiv & \Big\langle \text{Proposition 1.2 and sWLUS} \Big\rangle \\
& (\exists u)(\exists v)\big(x = u \wedge y = v \wedge u \in S \wedge v \in T\big) \\
\equiv & \Big\langle \text{1pt rule and WLUS} \Big\rangle \\
& (\exists u)\big(x = u \wedge u \in S \wedge y \in T\big) \\
\equiv & \Big\langle \text{1pt rule} \Big\rangle \\
& x \in S \wedge y \in T
\end{aligned}$$

■

[2] Use power-set and union axioms to see that this is a set indeed.

[3] The catch is that if *your* "obvious" is not obvious to the person to whom you are selling your proof, then you are stuck.

Remark 1.6. As we know, set equality and set inclusion are proved by arguments that start with "let $z \in$ lhs".

If the lhs (left hand side) is $S \times T$, a Cartesian product, we informally simplify matters by starting such proofs with

(1) Let $\langle x, y\rangle \in S \times T$
(2) Hence $x \in S \wedge y \in T$ by 1.5
(3) Etc.

In other words, we at once recognise that in "let $z \in S \times T$" z must be an ordered pair.

The wisdom in this can be seen in at least two ways: *Informally* first, when we say "let $z \in S \times T$" we are next presented with two cases:

1. z is *not* an ordered pair. Then "let $z \in S \times T$" is false, and it thus implies anything we want. Done.
2. z *is* an ordered pair. So it has the form $\langle x, y\rangle$ for some x and y, and our "let" becomes Let $\langle x, y\rangle \in S \times T$. We take it from here; this is the case with any real work in it.

There is a *formal* way in which we can also see that our short-cut "let" is legitimate. Let us trace the first few steps of a formal proof that wants to show $S \times T$ is a subset of some set:

(1)	$z \in S \times T$	$\big($assume$\big)$
(2)	$(\exists u)(\exists v)(z = \langle u, v\rangle \wedge u \in S \wedge v \in T)$	$\big($elaboration on (1)$\big)$
(3)	$z = \langle x, y\rangle \wedge x \in S \wedge y \in T$	$\big($assume by (2); x and y are fresh$\big)$
(4)	$x \in S \wedge y \in T$	$\big($(3) and taut. impl.$\big)$
(5)	Etc.	

Step (4) above corresponds exactly to step (2) of the informal approach. We have saved a couple of proof lines in the latter. ■

Example 1.7. Let us prove that $\emptyset \times S = \emptyset$.

First off, we get the $\supseteq$ direction "for free" (we know $A \supseteq \emptyset$ no matter which set A is). Thus we prove only the $\subseteq$ part.

We want to prove the implication $z \in \text{lhs} \Rightarrow z \in \emptyset$, that is,[4]

[4] By $\in$-elimination in "$z \in \{x|\mathit{false}\}$" and Leibniz.

$$z \in \text{lhs} \Rightarrow \textit{false} \tag{1}$$

OK, let us do an informal proof first:

Let $\langle x, y\rangle \in$ lhs. Thus (definition of $\times$) $x \in \emptyset$. But this is false.

Now, let us do the same formally:

$$
\begin{aligned}
& z \in \emptyset \times S \\
\equiv & \left\langle \text{see also 1.5} \right\rangle \\
& (\exists x)(\exists y)(z = \langle x, y\rangle \wedge x \in \emptyset \wedge y \in S) \\
\equiv & \left\langle ST \vdash x \in \emptyset \equiv \textit{false} \text{ and sWLUS} \right\rangle \\
& (\exists x)(\exists y)(z = \langle x, y\rangle \wedge \textit{false} \wedge y \in S) \\
\equiv & \left\langle \text{WLUS and taut. equiv.} \right\rangle \\
& (\exists x)(\exists y)\textit{false} \\
\equiv & \left\langle A \equiv (\exists x)A \text{ if } x \text{ not free in } A \right\rangle \\
& \textit{false}
\end{aligned}
$$

This time the formal approach allowed us to do the two directions simultaneously. ■

Example 1.8. Let us prove that $S \times (T \cup T') = (S \times T) \cup (S \times T')$.

$$
\begin{aligned}
& \langle x, y\rangle \in S \times (T \cup T') \\
\equiv & \Big\langle 1.5 \Big\rangle \\
& x \in S \wedge y \in T \cup T' \\
\equiv & \Big\langle \text{def. of union} \Big\rangle \\
& x \in S \wedge (y \in T \vee y \in T') \\
\equiv & \Big\langle \wedge \text{ over } \vee \Big\rangle \\
& (x \in S \wedge y \in T) \vee (x \in S \wedge y \in T') \\
\equiv & \Big\langle 1.5 \text{ and Leib.} \Big\rangle \\
& \langle x, y\rangle \in S \times T \vee \langle x, y\rangle \in S \times T' \\
\equiv & \Big\langle \text{def. of union} \Big\rangle \\
& \langle x, y\rangle \in (S \times T) \cup (S \times T')
\end{aligned}
$$

∎

Now that we have ordered pairs, we can also have ordered triples, quadruples, etc. For example, "overloading" the symbol $\langle \ldots \rangle$, we want ordered triples to obey

$$\langle a, b, c\rangle = \langle a', b', c'\rangle \Rightarrow a = a' \wedge b = b' \wedge c = c' \tag{1}$$

We can implement triples using pairs in at least two ways:[5]

(a) Either set

$$\langle a, b, c\rangle \stackrel{\text{Def.}}{=} \langle \langle a, b\rangle, c\rangle$$

This is the "left-associative solution".

(b) Or set

$$\langle a, b, c\rangle \stackrel{\text{Def.}}{=} \langle a, \langle b, c\rangle\rangle$$

This is the "right-associative solution".

Similarly one can define quadruples, using triples and pairs, and so on.

By the way, you can see immediately that either the left or right associative solutions give us (1).

[5] We saw a third way in class.

Instead of taking the "and so on" approach, let us compact these infinitely many definitions into one by using a recursive (inductive) definition of "n-tuple", for $n \geq 0$:

Definition 1.9 (n-tuples). Overloading once again the $\langle \ldots \rangle$ symbol we define by recursion (induction) on $n \geq 1$, where $a, a_1, \ldots$ that we use below are arbitrary terms of set theory:

$$\langle a \rangle \stackrel{\text{Def.}}{=} a$$
$$\langle a_1, \ldots, a_n, a_{n+1} \rangle \stackrel{\text{Def.}}{=} \langle \langle a_1, \ldots, a_n \rangle, a_{n+1} \rangle$$

The outermost $\langle \ldots \rangle$-application in the right hand side of the second equation above is the ordered pair of definition 1.1. The symbol $\langle a_1, \ldots, a_n \rangle$ is called an ordered n-tuple. The a_i is its i-th component or projection. ■

Note that 1.9 yields $\langle a, b \rangle = \langle \langle a \rangle, b \rangle$, thus the basis in the definition is the right one: We want $\langle a \rangle = a$ in order to be consistent.

Exercise 1.10. By induction on n prove informally that

$$ST \vdash \langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle \equiv a_1 = b_1 \wedge a_2 = b_2 \wedge \cdots \wedge a_n = b_n$$

■

Equipped with n-tuples we can now define $A \times B \times C$ and, in general,

$$A_1 \times A_2 \times \cdots \times A_n \stackrel{\text{Def.}}{=} \{\langle x_1, x_2, \cdots, x_n \rangle | x_1 \in A_1 \wedge x_2 \in A_2 \wedge \cdots \wedge x_n \in A_n\}$$

Since $\langle a, b, c, d \rangle = \langle \langle \langle a, b \rangle, c \rangle, d \rangle$, and so on for the n-tuple case,

$$A_1 \times A_2 \times \cdots \times A_n = (\cdots (A_1 \times A_2) \times A_3) \times A_4) \times \cdots) \times A_n)$$

i.e., brackets are inserted from left to right.

In particular, $A \times B \times C$ means $(A \times B) \times C$ by definition. However, $A \times B \times C \neq A \times (B \times C)$ since $\langle x, y, z \rangle = \langle \langle x, y \rangle, z \rangle \neq \langle x, \langle y, z \rangle \rangle$. Why? For otherwise we need $\langle x, y \rangle = x$, that is, $\{\{x\}, \{x, y\}\} = x$.[6] Can we have that? No, for it implies $x \in \{x\} \in x$, a pattern I can repeat forever and get an infinite descending chain, contradicting foundation.

[6] OK. So what's a small white lie between friends? This is one more time that I had to use the implementation of $\langle \ldots \rangle$, even though I promised on p.3 just before theorem 1.4 that it was, then, "the last time".

Sometimes $A_1 = A_2 = \ldots = A_n = B$. Then, instead of $A_1 \times A_2 \times \cdots \times A_n$ we may write B^n.

2 Binary Relations

So far we have seen relations as "concrete" (interpreted) predicates. Such as the various $\prec$ relations that we discussed in Part III, and also like $\subset$, $\subseteq$, $=$, etc. Any such (concrete) predicate P gives rise to an atomic formula $P(x, y)$, which is normally written in *infix* as xPy.

Such an atomic formula is a "device" that, intuitively, on "input" $\langle a, b\rangle$ returns the "output" aPb that is $\mathbf{t}$ or $\mathbf{f}$.

We can look at relations also as being sets: In fact we can define the *extension*, $\mathbb{P}$, of P by

$$\mathbb{P} = \{\langle x, y\rangle | xPy\} \tag{1}$$

Wait a minute! How do we know that $\mathbb{P}$ in (1) is a set no matter what the P?

We don't. It is not. But we will simply restrict attention to predicates P that lead to sets $\mathbb{P}$.

For example, if P is "=" then $\mathbb{P}$ is $\{\langle x, x\rangle | \mathit{true}\}$ which has one element, $\langle x, x\rangle$ for *every* x. Thus $\mathbb{P}$ is as big as $\mathbb{V}$ so it is not a set.

We often (almost always) abuse notation (1) and use the same typeface for the *intention* P and the extension $\mathbb{P}$. Thus mathematicians rewrite (1) as

$$P = \{\langle x, y\rangle | xPy\} \tag{2}$$

which leads to the important

$$\boxed{\langle x, y\rangle \in P \equiv xPy} \tag{3}$$

"Important" because it allows the infix shorthand to represent the cumbersome $\langle x, y\rangle \in P$.

Example 2.1 (Two weird examples of (3)).

$$\langle x, y\rangle \in\ <\ \equiv x < y$$

$$\langle x, y\rangle \in\ \in\ \equiv x \in y$$

■

The forgoing discussion motivates the set-theoretic (as opposed to the logic-theoretic that views them as predicates) definition of relations, R, as arbitrary two-column tables like

input	output
$\vdots$	$\vdots$
a	b
$\vdots$	$\vdots$

that denote the (extension of) R as *a set of pairs.*

What set of pairs? *Exactly those that appear as table rows.*

Thus a row like the one illustrated above appears iff aRb. By (3) (p.9) this is tantamount to $\langle a, b\rangle \in R$.

Note that in the predicate point of view we look at the entire pair $\langle a, b\rangle$ as input and **t** or **f**—as the case may be—the output.

However, set theoretically we think of the "a" in aRb as the input, and the b as one of the many possible outputs. For example, the table—written as a set of rows—$P = \{\langle 1, 2\rangle, \langle 1, 0\rangle\}$ has exactly two rows. On input 1 there are two possible outputs, 2 or 0.

This point of view, that the left component is input and the right one is output, will be useful when we look at the special relations that are also "functions".

To summarise:

Definition 2.2 (Binary Relations). A *binary relation*, or simply *relation*, is any set of ordered pairs. ■

"Binary" because they are sets of pairs. We can also define "ternary" relations—sets of triples—and in general n-ary, for $n > 2$.

We will not though: If $n > 2$, then $\langle a_1, \ldots, a_{n-1}, a_n\rangle = \langle\langle a_1, \ldots, a_{n-1}\rangle, a_n\rangle$. Thus the n-tuple is also a pair and we gain no new insights by studying n-ary relations, for $n \neq 2$, as different kinds of objects.

There is also such a thing as a 1-ary or *unary* relation. That is, any set whose elements are *not* all pairs—in short, *any set* that is not a binary relation is a unary relation. For example $\{1, \langle 1, 2\rangle, \langle 1, 2, 3\rangle\}$ and $\{1, 2, 5\}$ are unary relations.

Example 2.3. Thus, $\emptyset$ is a relation and so is $A \times B$ for any sets A and B. ■

We will define a few concepts associated with relations. By the way, for the balance of this Part IV "relation" means "set-theoretic binary relation".

So let R be any relation. First off, its first column (think of R as a table) forms a set called the *domain* of R. Its second column forms a set called the *range* of the relation.

We often have a set in mind, A, where all the inputs are coming from. However, not all these inputs need produce outputs. For example, we may want inputs to come from $\mathbb{N}$. But then the relation $\{\langle 1, 0\rangle, \langle 1, 6\rangle\}$ produces no output on input 5. This A that we fix, the set of all "legal" (or "allowed") inputs of R, is called the *left field* of R.

Similarly on defines the *right field* of R, say B, as the set where all the outputs will be.

Each of A and B we may be forced to define to be larger (more inclusive) than the domain and range respectively of any particular relation R. For example, A or B may indicate the "type" of the inputs or outputs (say, both of type $\mathbb{N}$) and we may be studying an arbitrary number of relations simultaneously, a situation that renders it meaningless to take the set of "legal outputs" equal to the range—to the range of which one relation if we are studying infinitely many different relations? We might be looking at once at all of

$$\{\langle 0, 0\rangle\}, \{\langle 0, 0\rangle, \langle 1, 1\rangle\}, \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle\}, \ldots$$

Note how the domains and ranges keep "growing" forcing us to choose as left and right fields $\mathbb{N}$ itself, or sets A and B that each contains $\mathbb{N}$ as a subset. Yet all these relations have domains and ranges that are finite subsets of $\mathbb{N}$.

To summarise:

Definition 2.4. Let R be a relation. If A is a fixed set where the inputs of R come from, and B is a fixed where its outputs go, then clearly $R \subseteq A \times B$.[7]

We say "R is from A to B" and write this as "$R : A \to B$" or "$A \xrightarrow{R} B$".

We call A the left and B the right field of R.

[7] If aRb—that is, $\langle a, b\rangle \in R$—then since a is an input, it is in A. Similarly, $b \in B$. Thus, $\langle a, b\rangle \in R \Rightarrow \langle a, b\rangle \in A \times B$.

Moreover we define domain and range:

$$\mathrm{dom}(R) \stackrel{\text{Def.}}{=} \{x|(\exists y)xRy\}$$

$$\mathrm{ran}(R) \stackrel{\text{Def.}}{=} \{y|(\exists x)xRy\}$$

If $A = \mathrm{dom}(R)$, then we say that “R is *total*”. Otherwise it is *nontotal*. We use the (standard!) wishy-washy terminology “*partial*” to indicate that R *may* be nontotal (but we either don't know for sure, or don't care).

If $B = \mathrm{ran}(R)$ then we call R *onto*. ■

Example 2.5. Let $R = \{\langle 1,1\rangle, \langle 1,2\rangle\}$, $S = \{\langle 0,1\rangle, \langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle, \ldots\}$ and $T = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \ldots\}$. Let the common left field be $\mathbb{N}$ and the common right field be also $\mathbb{N}$.

Then R is nontotal and also not onto. S is total, but not onto. T is both total and onto.

However, we may, if we want, ignore the information on the left field side and call all three partial relations. ■

3 Operations on Relations

Since relations are sets, we can operate on them with any of $\cup, \bigcup, \cap, \bigcap, -, \times$.

However, the most interesting is a new operation, peculiar to (binary) relations:

Definition 3.1 (Composition). Let us have $R : A \to B$ and $S : B \to C$, or, written conjunctionally,

$$A \xrightarrow{R} B \xrightarrow{S} C$$

Then we can define a relation $R \circ S : A \to C$, pronounced “the composition of R and S” by

$$R \circ S \stackrel{\text{Def.}}{=} \{\langle x, y\rangle | (\exists z)(xRz \wedge zSy)\} \tag{1}$$

■

By (3) on p.9 and eliminating “$\{\ldots\}$” in (1) above we may rewrite the definition as

$$xR \circ Sy \stackrel{\text{Def.}}{\equiv} (\exists z)(xRz \wedge zSy) \tag{2}$$

Thus, at the intuitive level, what the composition builds is a relation that has an input-output rule that is a result of the cascaded action of R and

S in that order: An input x to $R \circ S$ causes an output y iff x causes an appropriate output via R, let us call it z, such that when S *next* acts on z generates (among possibly other outputs) y.

Example 3.2. Let $R = \{\langle 1, 2\rangle\}$ and $S = \{\langle 2, 1\rangle\}$. Then $R \circ S = \{\langle 1, 1\rangle\}$ and $S \circ R = \{\langle 2, 2\rangle\}$.

Thus, we must not expect to prove $(\forall R)(\forall S)(R \circ S = S \circ R)$ as it is false in the special case above. As we say "$R \circ S = S \circ R$ is false *in general*".

Let also $T = \{\langle 1, 3\rangle\}$. Then $T \circ S = \emptyset$, while $S \circ T = \{\langle 2, 3\rangle\}$. ■

Theorem 3.3 (Associativity of $\circ$). *For any relations R, S, T,*

$$R \circ (S \circ T) = (R \circ S) \circ T$$

is provable in set theory.

Proof. You will recall our discussion regarding proofs that must start with "let $z \in S$" where S is a set of ordered pairs (see 1.6, p.5). We explained why informally one might as well start with "let $\langle x, y\rangle \in S$" instead—and that this is correct.

Moreover, since a set of pairs is a relation by definition, we can use a proof-start such as "let aSb". This is the normal way such proofs begin. Of course, if one wishes to use an equational proof, then the first line will be "aSb".

With this preamble out of the way, here is the chugga-chugga that does it:

$$
\begin{aligned}
& xR \circ (S \circ T)y \\
\equiv & \Big\langle \text{def. of “}\circ\text{”} \Big\rangle \\
& (\exists z)\big(xRz \wedge z(S \circ T)y\big) \\
\equiv & \Big\langle \text{def. of “}\circ\text{” and sWLUS} \Big\rangle \\
& (\exists z)\big(xRz \wedge (\exists w)(zSw \wedge wTy)\big) \\
\equiv & \Big\langle \text{“}\exists - \wedge\text{-rule” [no free } w \text{ in } xRz\text{] and sWLUS} \Big\rangle \\
& (\exists z)(\exists w)\big(xRz \wedge zSw \wedge wTy\big) \\
\equiv & \Big\langle \text{“}\exists - \exists \text{ commute”} \Big\rangle \\
& (\exists w)(\exists z)\big(xRz \wedge zSw \wedge wTy\big) \\
\equiv & \Big\langle \text{“}\exists - \wedge\text{-rule” [no free } z \text{ in } wTy\text{] and sWLUS} \Big\rangle \\
& (\exists w)\big((\exists z)(xRz \wedge zSw) \wedge wTy\big) \\
\equiv & \Big\langle \text{def. of “}\circ\text{” and sWLUS} \Big\rangle \\
& (\exists w)\big(xR \circ Sw \wedge wTy\big) \\
\equiv & \Big\langle \text{def. of “}\circ\text{”} \Big\rangle \\
& x(R \circ S) \circ Ty
\end{aligned}
$$

Note. In the above proof I used sWLUS throughout regardless of whether some steps required only WLUS. We can do this because any time WLUS is applicable then so is sWLUS. ■

What good is associativity for? It allows us to omit brackets in a chain of compositions as long as we keep the order of the participating relations fixed. How brackets were originally inserted is irrelevant by associativity.

In particular, in a chain like $R \circ R \circ R \circ R$ all that matters is how many R's we have. Thus, we write the chain with the shorthand R^4.

Imagine now that $R : A \to B$ where $A = \{1, 2, 3, \ldots\}$—the set of all positive integers—and $B = \{\ldots, -3, -2, -1\}$—the set of all negative integers. Thus, $R \circ R = \emptyset$. It follows that $R \circ R \circ R = \emptyset$—because $\emptyset \circ R = \emptyset$; do you believe this?

I am making a point here: If I compose R over and over with itself and it is $R : A \to B$ with $A \neq B$, then I may get situations where the results R^2, R^3, etc are rather trivial.

To ensure interesting results, we study relational powers in a *restricted context*, that is, for relations $R : A \to A$ for some A. That is, we want the left and right field to be equal.

Definition 3.4. If we have $R : A \to A$, then we say that <u>R is a relation on A.</u> ■

For the balance of Part IV, we deal with relations on some set A

Definition 3.5 (Identity Relation on A). The identity relation on A, in symbols $1_A : A \to A$, is given by

$$1_A = \{\langle x, x\rangle | x \in A\}$$

The identity relation is also called the *diagonal relation*—symbol Δ_A—or *unit relation*. When A is understood we may simply write 1 and Δ respectively, omitting the subscript A. ■

Remark 3.6. Definition 3.5 and a simple argument show that

$$(\forall x)(\forall y)(x 1_A y \equiv x = y) \tag{1}$$

where the $(\forall x)$ and $(\forall y)$ are shorthand for $(\forall x \in A)$ and $(\forall y \in A)$. Indeed, one need only establish (1) without the quantifiers (because we can generalise in set theory).

Arguing informally, let $a \in A$ and $a = b$. So, by 3.5, $a 1_A a$, and replacing the second a by b, I get $a 1_A b$.

For the other direction, let $a 1_A b$. This means

$$\langle a, b\rangle \in \{z | (\exists x)(z = \langle x, x\rangle \wedge x \in A)\}$$

Thus, $(\exists x)(\langle a, b\rangle = \langle x, x\rangle \wedge x \in A)$ is true by $\in$-elimination.[8]

Let c be a value of x that works,[9] i.e.,

$$\langle a, b\rangle = \langle c, c\rangle \wedge c \in A$$

It follows that $a = c = b$. Thus we got what we were after. ■

[8]When one argues informally one tends to say "is true" rather than "is a theorem", or "is provable".

[9]Formally, c would be a fresh variable and we would embark here on a proof by auxiliary variable.

We can now prove

Theorem 3.7. $1_A \circ R = R \circ 1_A = R$.

Proof. We prove only $1_A \circ R = R$, since the proof of $R \circ 1_A = R$ is very similar. The a, b below are in A, of course, and $(\exists z)$ is short for $(\exists z \in A)$.

$$
\begin{aligned}
& a 1_A \circ R b \\
\equiv & \left\langle \text{def. of } \circ \right\rangle \\
& (\exists z)(a 1_A z \wedge z R b) \\
\equiv & \left\langle \text{by 3.6 and sWLUS} \right\rangle \\
& (\exists z)(a = z \wedge z R b) \\
\equiv & \left\langle \text{1pt rule} \right\rangle \\
& a R b
\end{aligned}
$$

■

We can now get back to the issue of relational powers:

Definition 3.8 (Relational Powers). Let $R : A \to A$.[10] We define by induction on $n \geq 0$:

$$
\begin{aligned}
R^0 &\stackrel{\text{Def.}}{=} 1_A \\
R^{n+1} &\stackrel{\text{Def.}}{=} R \circ R^n
\end{aligned}
$$

■

Remark 3.9. We expect the above definition to yield $R^1 = R$, i.e., R^1 means that we have "one factor" and no $\circ$-operation performed just as in a^1 for a real number a.

We do get that much:

$$R^1 = R^{0+1} \stackrel{\text{2nd equation}}{=} R \circ R^0 \stackrel{\text{1st equation}}{=} R \circ 1_A \stackrel{3.7}{=} R$$

Moreover, a trivial induction on $n \geq 1$ proves that

[10] This apparently incomplete and ungrammatical sentence is not: It says "let R be a relation on A".

$$R^n = \overbrace{R \circ \cdots \circ R}^{n \text{ copies of } R}$$

for $R^1 = R$ provides the basis, and the second equation in 3.8 adds a copy of "R" to n existing ones (which are there by the I.H.) ■

We can now prove

Proposition 3.10. *Let $R : A \to A$. Then $R^n \circ R^m = R^{n+m}$ is a theorem of set theory.*

Proof. What the above really says (of which we have used a shorthand, legitimate by the fact that we can generalise in set theory)

$$(\forall n)(\forall m)R^n \circ R^m = R^{n+m}$$

I use induction on $n \geq 0$:

Basis. I want $R^0 \circ R^m = R^m$. Well, $R^0 = 1_A$ and I am done by 3.7.
I.H. Assume $R^n \circ R^m = R^{n+m}$.
Goto. Prove $R^{n+1} \circ R^m = R^{n+m+1}$.

$$\begin{aligned}
& R^{n+1} \circ R^m \\
= & \Big\langle \text{def. } 3.8 \Big\rangle \\
& (R \circ R^n) \circ R^m \\
= & \Big\langle \text{associativity} \Big\rangle \\
& R \circ (R^n \circ R^m) \\
= & \Big\langle \text{I.H.} \Big\rangle \\
& R \circ R^{n+m} \\
= & \Big\langle \text{def. } 3.8 \Big\rangle \\
& R^{n+m+1}
\end{aligned}$$

■

Corollary 3.11. *The powers of a relation R on A commute with respect to composition.*

Proof. $R^n \circ R^m = R^{n+m} = R^{m+n} = R^m \circ R^n$. ■