CHAPTER 13

ARITHMETIC

> *"Abstraction is a crucial feature of [rational] knowledge, because in order to compare and to classify the immense variety of shapes, structures and phenomena around us we cannot take all their features into account, but have to select a few significant ones. Thus we construct an intellectual map of reality in which things are reduced to their general outlines."*
>
> Fritjof Capra

13.1. Topoi as foundations

Category theory promotes the viewpoint that the concept of "arrow" be taken as fundamental in place of "membership", and the development of topos theory substantiates that position. By imposing natural conditions on a topos (extensionality, sections for epics, natural numbers object), we can make it correspond precisely to a model of classical set theory. Thus, to the extent that set theory provides a foundation for mathematics, so too does topos theory. What then are the attractions of this new system?

The first thing one could point to is that the concepts of topos theory are natural ones to the practising mathematician. Category theory was originally developed as a language for use in the areas of topology and algebra. The alternative account it has subsequently produced of the nature of mathematical structures and their essential features is a most compelling one. Entities are characterised by their universal properties, which specify their role in relation to other entities. Thus it is the universal property that a product has that most effectively conveys its usage and function in relation to the two objects from which it is obtained. Once this "operational" description is known, its internal structure – the way it was constructed – is of lesser importance.

It was suggested in Chapter 1 that the purpose of foundational studies is to provide a rigorous explication of the nature of mathematical concepts and entities. There is of course no single correct way to do this. Set theory offers one approach, topos theory another. As against either one might retort that we really know what such things as whole numbers are, and always have. And yet as long as there are mathematicians, there will be new and different attempts to define and describe them. Contexts and perspectives change in the light of new knowledge. Forms of language change to deal with new perspectives. Whenever this occurs, old ideas are re-examined in a different light. To some people, discovering topoi will constitute a revelation. Just re-expressing familiar ideas in a new language, relating them to different concepts, somehow carries the force of *explanation*, even if the new new concepts themselves ultimately require explaining. It may well be, in the future, that those bought up on a solid diet of "arrow-language" will seek to reappraise what to them will have been standard fare. When that happens, new concepts, and new foundations will emerge.

One of the new analyses of mathematical structure developed by the categorial foundation is an alternative account of what sets are and how they behave. Instead of the "universe of (ZF) sets" we are offered the "category of sets". In formal theories like ZF a set is an entity that has members that have members that have members that have .... The membership structure determined by a set can be very rich indeed (think about the membership tree for example of $\mathcal{P}(\omega)$). The informal picture that the ZF-set-theorist has of his universe is an open-ended cone

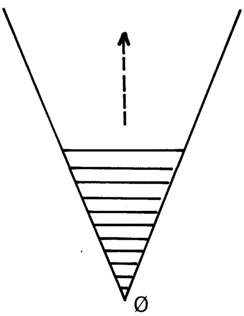

Fig. 13.1.

with the null set at the base point. Starting with $\emptyset$, all the individuals in the universe are built up by repeatedly forming powersets and taking unions. As these operations are iterated, sets of greater and greater complexity appear at higher and higher levels that pile up in the cone ad infinitum.

Now the elements of the collections that are used in mathematics are indeed often sets themselves. Thus a topology is a collection of subsets, as is a powerset, and a Heyting algebra $\mathbf{P}^+$. An analyst deals daily with collections of functions, and with function(al)s whose inputs are themselves functions. Rarely however does one find in practice the need for more than three or four levels of membership. Even then one can distinguish these examples of the use of set theory from the actual conception, the essential idea, of what a set is. As Lawvere [76] puts it, "an abstract set X has elements each of which has no internal structure whatsoever". A set, "naively", is a collection of indeterminate, quite arbitrary, things. Indeed in algebra the word "abstract" is used to convey precisely that sense. One studies abstract group theory when one studies groups as collections that support a certain algebraic structure, the nature of the elements of those collections being immaterial. In general topology, the elements of a topological space are universally called "points", therein a point being, as it was for Euclid, "that which has no parts". Likewise, in the category of sets, a set is an object X that has elements $1 \rightarrow X$, these elements being fundamental and indivisible. Topos theory has shown us how to develop foundations for standard mathematical concepts in these terms.

Intuitive set theory is, and will doubtless remain, central to our metalanguage for the doing of mathematics. It is part of the language in which we speak, whether the object of our discourse be geometry, algebra, or foundations, whether the objects about which we speak be topological spaces, groups, or sets. Seen in this way, topos theory stands not so much as a rival to set theory per se as an alternative to formalised set theory in presenting a rigorous explication, a foundation, of our intuitive notion of "set".

One of the most significant achievements of topos theory is to have crystallised the core of basic set theory in one concept that is manifest in such hitherto diverse contexts. Thus we can apply the "set of points" notion and our familiarity with it to the structures of algebraic geometry, intuitionistic logic, and monoid representations. In this chapter we shall look briefly at how the foundations of the arithmetic of natural numbers can be lifted to any topos with a natural numbers object. The power of the axiomatic method, and the ability of abstraction to simplify and get at the heart of things will perhaps be brought home if one reflects that a "natural number", i.e. element $1 \rightarrow N$ of N, referred to below might in fact be anything from a continuous function between sheaves of sets of germs (local homeomorphisms) to an equivariant mapping of monoid actions, or a natural transformation between set-valued functors defined on an arbitrary small category.

13.2. Primitive recursion

Throughout this section, $\mathscr{E}$ denotes a topos that has a natural numbers object $1 \xrightarrow{O} N \xrightarrow{\mathcal{s}} N$. So for any diagram $1 \xrightarrow{x} a \xrightarrow{f} a$ in $\mathscr{E}$ we have a unique "$\mathscr{E}$-sequence" $h: N \to a$ defined by simple recursion from f and x, i.e. making

$$\begin{tikzcd} & N \arrow[r, "\mathcal{s}"] \arrow[d, "h"] & N \arrow[d, "h"] \\ 1 \arrow[ur, "O"] \arrow[dr, "x"'] & & \\ & a \arrow[r, "f"] & a \end{tikzcd}$$

commute.

Now there are many basic arithmetical functions that can be defined inductively by more complex forms of recursion than that captured by the axiom NNO. Consider, for example, the process of forming the sum $m+n$ of two numbers. We may do this by holding m fixed and "repeatedly adding 1 to m" to generate the sequence

$$m, m+1, m+2, \ldots, m+n, \ldots$$

Then $m+n$ is defined by "recursion on n" from the equations

$$m+0=m$$

and

$$m+(n+1)=(m+n)+1$$

i.e.

$$m+s(n)=s(m+n).$$

The form of these equations is the same as those that defined the unique $h: I \times \omega \to A$ used to verify NNO for $\mathbf{Bn}(I)$ in §12.2, and readily generalises. The "parameter" m is replaced by an element x of an arbitrary set A, and in place of $m+n$ we define a function $h(x, n)$ with inputs from $A \times \omega$, and outputs in some other set B. To start the induction on n we need a function of the form $h_0 : A \to B$ so that we can put

(1) $$h(x, 0) = h_0(x).$$

Then, assuming a function $f : B \to B$ has been given, repeated application of f will generate h. Thus we put

(2) $$h(x, n+1) = f(h(x, n)).$$

By (1) and (2) the diagram

$$\begin{tikzcd} & A\times\omega \arrow[r, "1_A \times s"] \arrow[d, "h"] & A\times\omega \arrow[d, "h"] \\ A \arrow[ur, "\langle 1_A, O_A\rangle"] \arrow[r, "h_0"'] & B \arrow[r, "f"] & B \end{tikzcd}$$

commutes, and defining h by these equations is the only way that it can commute.

In the case that h_0 is $\mathrm{id}_\omega : \omega \to \omega$ and f is the successor function $s : \omega \to \omega$, the unique h defined recursively from h_0 and f by (1) and (2) is the addition function $+ : \omega \times \omega \to \omega$.

THEOREM 1. (Freyd [72]). *If* $\mathscr{E} \models \mathrm{NNO}$, *then for any diagram* $a \xrightarrow{h_0} b \xrightarrow{f} b$ *there is exactly one* $\mathscr{E}$*-arrow* $h : a \times N \to b$ *such that*

$$\begin{tikzcd} & a\times N \arrow[r, "1_a \times \mathscr{s}"] \arrow[d, "h"] & a\times N \arrow[d, "h"] \\ a \arrow[ur, "\langle 1_a, O_a\rangle"] \arrow[r, "h_0"'] & b \arrow[r, "f"] & b \end{tikzcd}$$

commutes, where O_a *is the composite of* $a \to 1 \xrightarrow{O} N$.

CONSTRUCTION FOR PROOF. h is the "twisted" exponential adjoint of the unique sequence $N \to b^a$ that makes

$$\begin{tikzcd} & N \arrow[r, "\mathscr{s}"] \arrow[d] & N \arrow[d] \\ 1 \arrow[ur, "O"] \arrow[r, "\ulcorner h_0 \urcorner"'] & b^a \arrow[r, "f^a"] & b^a \end{tikzcd}$$

commute. Here f^a is the exponential adjoint of $f \circ ev : b^a \times a \to b$

$$\begin{tikzcd} b^a \times a \arrow[r, "ev"] \arrow[dr, "f \circ ev"'] & b \arrow[d, "f"] \\ & b \end{tikzcd}$$

In **Set**, $f \circ ev$ maps $\langle g, x\rangle \in B^A \times A$ to $f(g(x)) \in B$, so that f^A maps $g \in B^A$ to

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[dr, "f \circ g"'] & B \arrow[d, "f"] \\ & B \end{tikzcd}$$

$f \circ g \in B^A$. □

Applying Theorem 1 to a diagram of the form $b \xrightarrow{\mathbf{1}_b} b \xrightarrow{f} b$, the unique $h : b \times N \to b$ defined by recursion from $\mathbf{1}_b$ and f has in **Set** the recursive equations

$$h(x, 0) = x$$

$$h(x, n+1) = f(h(x, n)).$$

Thus for fixed x, h generates the sequence

$$x, f(x), f(f(x)), f(f(f(x))), \ldots$$

and so h is called the *iterate* of f.

The iterate of the successor arrow $\mathfrak{s} : N \to N$ is, by definition, the addition arrow $\oplus : N \times N \to N$.

EXERCISE 1. What does $\oplus$ look like in $\mathbf{Set}^{\mathscr{C}}$ and $\mathbf{Bn}(I)$?

EXERCISE 2. Let $i(f)$ be the iterate of f. Show that

$$\begin{tikzcd} b \times N \times N \arrow[r, "i(f) \times \mathbf{1}_N"] \arrow[d, "\mathbf{1}_b \times \oplus"'] & b \times N \arrow[d, "i(f)"] \\ b \times N \arrow[r, "i(f)"] & b \end{tikzcd}$$

commutes.

EXERCISE 3. Explain why Exercise 2, in the case $f = \mathfrak{s}$, gives the "associative law for addition".

EXERCISE 4. Show that

$$\begin{tikzcd} b \times N \arrow[r, "f \times 1_N"] \arrow[d, "i(f)"'] & b \times N \arrow[d, "i(f)"] \\ b \arrow[r, "f"] & b \end{tikzcd}$$

and

$$\begin{tikzcd} b \times N \arrow[r, "f \times 1_N"] \arrow[d, "1_b \times \mathfrak{s}"'] & b \times N \arrow[d, "i(f)"] \\ b \times N \arrow[r, "i(f)"] & b \end{tikzcd}$$

commute.

EXERCISE 5. Show that $\langle O_N, 1_N\rangle \circ O = \langle 1_N, O_N\rangle \circ O = \langle O, O\rangle$.

EXERCISE 6. $\oplus \circ \langle O, O\rangle = O$.

EXERCISE 7. $(0 + m = m)$. Show that

$$\begin{tikzcd} N \arrow[r, "\langle O_N, 1_N\rangle"] \arrow[dr, "1_N"'] & N \times N \arrow[d, "\oplus"] \\ & N \end{tikzcd}$$

commutes.

EXERCISE 8. (Commutativity of Addition)

$$\begin{tikzcd} N \times N \arrow[rr, "\langle pr_2, pr_1\rangle"] \arrow[dr, "\oplus"'] & & N \times N \arrow[dl, "\oplus"] \\ & N & \end{tikzcd}$$

commutes. □

The basic idea of recursion captured by Theorem 1 is that $h(x, n)$, having been defined, serves as input to some function f to obtain $h(x, n+1)$ as output. But there are some functions with natural inductive definitions in which $h(x, n+1)$ depends, not just on $h(x, n)$, but also on x and n in a very direct way, i.e. we need to input one or both of x and n as well as $h(x, n)$ to get $h(x, n+1)$. Take for example the multiplication $x \times n$ of x by n, i.e. "x added to itself n times". This is given by the equations

$$x \times 0 = 0$$

$$x \times (n+1) = x + (x \times n)$$

i.e.

$$x \times s(n) = f(x, x \times n)$$

where f is the addition function.

For an example in which $h(x, n+1)$ depends directly on n consider the predecessor function $\rho : \omega \to \omega$ that has $\rho(n) = n-1$ (unless $n = 0$, in which case we put $\rho(n) = 0$). Recursively ρ is specified by

$$\rho(0) = 0$$

$$\rho(n+1) = n.$$

These two considerations may be combined into one: given functions $h_0 : A \to B$ and $f : A \times \omega \times B \to B$ we define $h : A \times \omega \to B$, by "primitive recursion", through the equations

$$h(x, 0) = h_0(x)$$

$$h(x, n+1) = f(x, n, h(x, n)).$$

By putting h_0 as $O_\omega : \omega \to \omega$ and f as the "2nd projection" $pr_2^3 : \omega^3 \to \omega$, the resulting h is the predecessor function ρ. Using the same h_0, but with f the composite of

$$\omega^3 \xrightarrow{\langle pr_1, pr_3 \rangle} \omega^2 \xrightarrow{+} \omega$$

we recover the multiplication function as h.

PRIMITIVE RECURSION THEOREM (Freyd [72]). *If $\mathscr{E} \models$ NNO, then for any $\mathscr{E}$-arrows $h_0 : a \to b$ and $f : a \times N \times b \to b$ there is a unique $\mathscr{E}$-arrow $h : a \times N \to b$ making*

$$\begin{tikzcd} & a \times N \arrow[d, "h"] \\ a \arrow[ur, "\langle 1_a, O_a \rangle"] \arrow[r, "h_0"'] & b \end{tikzcd} \qquad \begin{tikzcd} a \times N \arrow[r, "1_a \times s"] \arrow[d, "\langle 1_{a \times N}, h \rangle"'] & a \times N \arrow[d, "h"] \\ a \times N \times b \arrow[r, "f"] & b \end{tikzcd}$$

commute.

CONSTRUCTION FOR PROOF. By Theorem 1, there is a unique h' such that

$$\begin{tikzcd} & a\times N \arrow[r, "1_a\times\sigma"] \arrow[d, "h'"'] & a\times N \arrow[d, "h'"] \\ a \arrow[ur, "\langle 1_a, O_a\rangle"] \arrow[r, "\langle 1_a, O_a, h_0\rangle"'] & a\times N\times b \arrow[r, "\langle pr_1, pr_2, f\rangle"] & a\times N\times b \end{tikzcd}$$

commutes.

In **Set** $\langle pr_1, pr_2, f\rangle$ takes $\langle x, n, y\rangle$ to $\langle x, n, f(x, n, y)\rangle$. Hence h' has the equations

$$h'(x, 0)=\langle x, 0, h_0(x)\rangle$$

$$h'(x, n+1)=\langle x, n, f(x, n, h'(x, n))\rangle.$$

The desired $\mathscr{E}$-arrow h is the composite

$$\begin{tikzcd} a\times N \arrow[r, "h'"] \arrow[dr, "h"'] & a\times N\times b \arrow[d, "pr_b"] \\ & b \end{tikzcd}$$

of h' and the projection to b. □

COROLLARY. *If h is defined recursively from h_0 and f as in the Theorem, then for any elements $x:1\to a$ and $y:1\to N$ of a and N we have*

(i) $h\circ\langle x, 0\rangle=h_0\circ x$

$$\begin{tikzcd} & 1 \arrow[dl, "\langle x, O\rangle"'] \arrow[dr, "h_0\circ x"] & \\ a\times N \arrow[rr, "h"] & & b \end{tikzcd}$$

(ii) $h\circ\langle x, \sigma\circ y\rangle=f\circ\langle x, y, h\circ\langle x, y\rangle\rangle$

$$\begin{tikzcd} 1 \arrow[r, "\langle x, y, h\circ\langle x, y\rangle\rangle"] \arrow[d, "\langle x, \sigma\circ y\rangle"'] & a\times N\times B \arrow[d, "f"] \\ a\times N \arrow[r, "h"] & b \end{tikzcd}$$

PROOF. Apply the elements $x:1\to a$ and $\langle x, y\rangle:1\to a\times N$ to the two diagrams of the Primitive Recursion Theorem, and use the rules for product arrows given in the Exercises of §3.8.

The original formulation of the Primitive Recursion Theorem, in the context of well-pointed categories, is due to Lawvere [64] and states that there is a unique h satisfying the two conditions of the corollary. A full proof of this is given by Hatcher [68], wherein extensionality is invoked to show uniqueness of h.

Some special cases

(1) (*Independence of* n). Given $h_0: a \to b$ and $f: a \times b \to b$, there is a unique $h: a \times N \to b$ making

$$\begin{tikzcd} & a \times N \arrow[d, "h"] \\ a \arrow[ur, "\langle 1_a, O_a\rangle"] \arrow[r, "h_0"'] & b \end{tikzcd} \qquad \begin{tikzcd} a \times N \arrow[r, "1_a \times s"] \arrow[d, "\langle pr_a, h\rangle"'] & a \times N \arrow[d, "h"] \\ a \times b \arrow[r, "f"] & b \end{tikzcd}$$

commute. (h is obtained by primitive recursion from h_0 and $f \circ \langle pr_a, pr_b\rangle : a \times N \times b \to b$, using $\mathbf{1}_{a \times N} = \langle pr_a, pr_N\rangle$.)

(2) (*Independence of* x). Given $h_0: a \to b$ and $f: N \times b \to b$ there is a unique $h: a \times N \to b$ making

$$\begin{tikzcd} & a \times N \arrow[d, "h"] \\ a \arrow[ur, "\langle 1_a, O_a\rangle"] \arrow[r, "h_0"'] & b \end{tikzcd} \qquad \begin{tikzcd} a \times N \arrow[r, "1_a \times s"] \arrow[d, "\langle pr_N, h\rangle"'] & a \times N \arrow[d, "h"] \\ N \times b \arrow[r, "f"] & b \end{tikzcd}$$

commute.

(3) (*Dependence only on* n). Given $h_0: 1 \to b$ and $f: N \to b$ there is a unique $h: N \to b$ such that

$$\begin{tikzcd} & N \arrow[d, "h"] \\ 1 \arrow[ur, "O"] \arrow[r, "h_0"'] & b \end{tikzcd} \qquad \begin{tikzcd} N \arrow[rr, "s"] \arrow[dr, "f"'] & & N \arrow[dl, "h"] \\ & b & \end{tikzcd}$$

commute (this comes from Case (2), defining $h': 1 \times N \to b$ from h_0 and $f \circ pr_N : N \times b \to b$ and using the isomorphism $1 \times N \cong N$).

(4) (*Iteration*). Theorem 1 is itself a special case: given $h_0: a \to b$, $f: b \to b$, the unique $h: a \times N \to b$ is defined by primitive recursion from h_0 and $f \circ pr_b : a \times N \times b \to b$.

Using the Primitive Recursion Theorem and its special cases, we can define in any topos with a natural numbers object analogues of many arithmetical operations.

Definition (*Predecessor*). $\rho: N \to N$ is defined by recursion from $O: 1 \to N$ and $1_N: N \to N$ (Case (3)) as the unique arrow that exists to make

$$\begin{tikzcd} & N \arrow[d, "\rho"] \\ 1 \arrow[ur, "O"] \arrow[r, "O"'] & N \end{tikzcd} \qquad \begin{tikzcd} N \arrow[r, "s"] \arrow[dr, "1_N"'] & N \arrow[d, "\rho"] \\ & N \end{tikzcd}$$

commute.

Corollary. *s is monic.*

Proof. If $s \circ f = s \circ g$, $\rho \circ s \circ f = \rho \circ s \circ g$, i.e. $1_N \circ f = 1_N \circ g$.

Exercise 9. Show that ρ is epic. $\square$

Definition (*Subtraction*). $\dot{-}: N \times N \to N$ is the iterate of ρ, i.e. the unique arrow for which

$$\begin{tikzcd} & N \times N \arrow[r, "1 \times s"] \arrow[d, "\dot{-}"] & N \times N \arrow[d, "\dot{-}"] \\ N \arrow[ur, "\langle 1_N, O_N \rangle"] \arrow[r, "1_N"'] & N \arrow[r, "\rho"] & N \end{tikzcd}$$

commutes.

Exercise 10. Verify that in **Set**

$$m \dot{-} n = \begin{cases} m - n & \text{if } m \geqslant n \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 11.

$$\begin{tikzcd} N \times N \arrow[r, "1_N \times s"] \arrow[d, "\langle \oplus, pr_2 \rangle"'] & N \times N \arrow[d, "\langle \oplus, pr_2 \rangle"] \\ N \times N \arrow[r, "s \times s"] & N \times N \end{tikzcd}$$

commutes.

EXERCISE 12. $((n+1)\dot{-}1=n)$. The diagram

$$\begin{tikzcd} N \arrow[r, "\langle s, s\circ O_N\rangle"] \arrow[dr, "1_N"'] & N\times N \arrow[d, "\dot{-}"] \\ & N \end{tikzcd}$$

commutes. □

THEOREM 2. (1) $[(m+1)\dot{-}(n+1)=m\dot{-}n]$

$$\begin{tikzcd} N\times N \arrow[rr, "s\times s"] \arrow[dr, "\dot{-}"'] & & N\times N \arrow[dl, "\dot{-}"] \\ & N & \end{tikzcd}$$

commutes.

(2) $[(m+n)\dot{-}n=m]$

$$\begin{tikzcd} N\times N \arrow[rr, "\langle \oplus, pr_2\rangle"] \arrow[dr, "pr_1"'] & & N\times N \arrow[dl, "\dot{-}"] \\ & N & \end{tikzcd}$$

commutes.

PROOF. (1) Consider

$$\begin{tikzcd} N\times N \arrow[rr, "s\times s"] \arrow[dr, "s\times 1_N"] \arrow[dd, "1"'] & & N\times N \arrow[dd, "\dot{-}"] \\ & N\times N \arrow[ur, "1_N\times s"'] \arrow[dl, "\rho\times 1_N"] & \\ N\times N \arrow[rr, "\dot{-}"'] & & N \end{tikzcd}$$

That the upper triangle commutes is a standard exercise (3.8.8) in product arrows. For the other triangle we have

$$\begin{aligned} \rho\times 1_N\circ s\times 1_N &= \rho\circ s\times 1_N\circ 1_N \qquad (3.8.8)\\ &= 1_N\times 1_N \\ &= 1_{N\times N}. \end{aligned}$$

But the lower part of the diagram commutes by the second diagram of Exercise 4 above (tipped over). Hence the boundary of the diagram commutes as required.

(2) Consider

$$\begin{tikzcd}
 & N\times N \arrow[r, "1_N\times s"] \arrow[d, "\langle\oplus, pr_2\rangle"] & N\times N \arrow[d, "\langle\oplus, pr_2\rangle"] \\
N \arrow[ur, "\langle 1_N, O_N\rangle"] \arrow[r, "\langle 1_N, O_N\rangle"] \arrow[dr, "1_N"'] & N\times N \arrow[r, "s\times s"] \arrow[d, "\dot{-}"] & N\times N \arrow[d, "\dot{-}"] \\
 & N \arrow[r, "1_N"] & N
\end{tikzcd}$$

The upper square commutes by Exercise 11, the lower one by part (1) of this theorem. The lower triangle is part of the definition of $\dot{-}$, and for the upper triangle we have

$$\begin{aligned}\langle\oplus, pr_2\rangle\circ\langle 1_N, O_N\rangle &= \langle\oplus\circ\langle 1_N, O_N\rangle, pr_2\circ\langle 1_N, O_N\rangle\rangle \\ &= \langle 1_N, O_N\rangle \qquad \text{(definition } \oplus).\end{aligned}$$

Thus the whole diagram commutes, showing (Theorem 1) that $\dot{-}\circ\langle\oplus, pr_2\rangle$ is the unique iterate of 1_N. But it is a simple exercise that the iterate of 1_N is $pr_1 : N\times N\to N$. □

COROLLARY.

(1)
$$\begin{tikzcd}
N\times N \arrow[r, "\langle\oplus, pr_2\rangle"] \arrow[dr, "1"'] & N\times N \arrow[d, "\langle\dot{-}, pr_2\rangle"] \\
 & N\times N
\end{tikzcd}$$

commutes.

(2) $\langle\oplus, pr_2\rangle : N\times N\to N\times N$ and $\langle pr_1, \oplus\rangle : N\times N\to N\times N$ *are both monic.*

PROOF. (1)

$$\begin{aligned}&\langle\dot{-}, pr_2\rangle\circ\langle\oplus, pr_2\rangle \\ &= \langle\dot{-}\circ\langle\oplus, pr_2\rangle, pr_2\circ\langle\oplus, pr_2\rangle\rangle \\ &= \langle pr_1, pr_2\rangle \qquad \text{(Theorem, part (2))} \\ &= 1_{N\times N}.\end{aligned}$$

(2) From (1) (as in the proof that s is monic), we get $\langle \oplus, pr_2\rangle$ monic. But then, since

$$\begin{tikzcd} N\times N \arrow[rr, "\langle pr_2, pr_1\rangle"] \arrow[dr, "\langle \oplus, pr_1\rangle"'] & & N\times N \arrow[dl, "\langle \oplus, pr_2\rangle"] \\ & N\times N & \end{tikzcd}$$

commutes, using Exercise 8, and so too does

$$\begin{tikzcd} N\times N \arrow[rr, "\langle \oplus, pr_1\rangle"] \arrow[dr, "\langle pr_1, \oplus\rangle"'] & & N\times N \arrow[dl, "\langle pr_2, pr_1\rangle"] \\ & N\times N & \end{tikzcd}$$

the fact that the twist arrow $\langle pr_2, pr_1\rangle$ is iso means that $\langle pr_1, \oplus\rangle$ is monic.

□

Order relations

The standard ordering $\leqslant$ on ω yields the relation

$$L=\{\langle m, n\rangle : m\leqslant n\}.$$

Since, in general, $m\leqslant n$ iff for some $p\in\omega$, $m+p=n$, we have

$$L=\{\langle m, m+p\rangle : m, p\in\omega\}.$$

But $\langle m, m+p\rangle$ is the output of the function $\langle pr_1, \oplus\rangle : \omega\times\omega\to\omega\times\omega$, for input $\langle m, p\rangle$, so we have the epi-monic factorisation

$$\begin{tikzcd} \omega\times\omega \arrow[rr, "\langle pr_1, \oplus\rangle"] \arrow[dr, two heads, "\langle pr_1, \oplus\rangle^*"'] & & \omega\times\omega \\ & L \arrow[ur, hook] & \end{tikzcd}$$

Thus in $\mathscr{E}$ we may define the order relation on N to be that subobject of $N\times N$ that arises from the epi-monic factorisation of $\langle pr_1, \oplus\rangle$. Since, as we have just seen, this arrow is monic already, we may take *it* to represent the order on N.

The strict order $<$ on ω is given from $\leqslant$ by the condition

$$m<n \quad \text{iff} \quad m+1\leqslant n.$$

Thus in $\mathscr{E}$ we define $\circledless : N\times N \rightarrowtail N\times N$ by the diagram

$$\begin{tikzcd} N\times N \arrow[rr, "\mathfrak{s}\times 1_N"] \arrow[dr, "\circledless"'] & & N\times N \arrow[dl, "\langle pr_1, \oplus\rangle"] \\ & N\times N & \end{tikzcd}$$

$\mathfrak{s}\times 1_N$ is monic, being a product of monics, and so $\circledless$ is indeed a subobject of $N\times N$.

EXERCISE 13. Define the $\mathscr{E}$-arrows corresponding to the relations

$$\{\langle m, n\rangle : m \geqslant n\}$$

and

$$\{\langle m, n\rangle : m > n\}$$

on ω. $\square$

DEFINITION (*Multiplication*). $\otimes : N\times N \to N$ is defined recursively from O_N and $\oplus$ (Special Case (1)) as the unique arrow making

$$\begin{tikzcd} & N\times N \arrow[d, "\otimes"] \\ N \arrow[ur, "\langle 1_N, O_N\rangle"] \arrow[r, "O_N"'] & N \end{tikzcd} \qquad \begin{tikzcd} N\times N \arrow[r, "1_N\times \mathfrak{s}"] \arrow[d, "\langle pr_1, \otimes\rangle"'] & N\times N \arrow[d, "\otimes"] \\ N\times N \arrow[r, "\oplus"] & N \end{tikzcd}$$

commute.

EXERCISE 14. Show that, for $x:1\to N$ and $y:1\to N$

$$\begin{tikzcd} N\times N \arrow[rr, tail, "\langle pr_1, \oplus\rangle"] & & N\times N \\ & 1 \arrow[ul, dashed] \arrow[ur, "\langle x, y\rangle"'] & \end{tikzcd}$$

$\langle x, y\rangle \in \langle pr_1, \oplus\rangle$ iff for some $z:1\to N$, $\oplus\circ\langle x, z\rangle = y$.

EXERCISE 15. Show that $\langle x, y\rangle \in \circledless$ iff for some z, $\oplus\circ\langle \mathfrak{s}\circ x, z\rangle = y$.

EXERCISE 16. Show for any $x:1\to N$, that

$$\otimes\circ\langle x, \mathfrak{s}\circ O\rangle = x.$$

EXERCISE 17. Define in $\mathscr{E}$ analogues of the following arithmetical arrows in **Set**

(i) $\exp(m, n) = m^n$

(ii) $|m-n| = \begin{cases} m-n & \text{if } m \geqslant n \\ n-m & \text{otherwise} \end{cases}$

(iii) $\max(m, n) =$ maximum of m and n

(iv) $\min(m, n) =$ minimum of m and n. □

Further information about recursion on natural numbers objects in topoi is given by Brook [74], on which much of this section has been based.

13.3. Peano postulates

In **Set** one can prove of the system $1 \xrightarrow{O} \omega \xrightarrow{s} \omega$ that

(1) $s(x) \neq 0$, all $x \in \omega$.

(2) $s(x) = s(y)$ only if $x = y$, all $x, y \in \omega$.

(3) if $A \subseteq \omega$ satisfies

(i) $0 \in A$, and

(ii) whenever $x \in A$ then $s(x) \in A$,

then $A = \omega$.

Statement (3) formalises the principle of Finite Mathematical Induction. Any natural number is obtainable from 0 by repeatedly adding 1 a finite number of times. (i) and (ii) tell us that this process always results in a member of A.

The three statements (1), (2), (3), known as the Peano Postulates, provide the basis for an axiomatic development of classical number theory. They characterise ω in **Set**, in the sense that if $1 \xrightarrow{O'} \omega' \xrightarrow{s'} \omega'$ was any other system satisfying the analogues of (1), (2), (3), then the unique $h : \omega \to \omega'$ for which

$$\begin{tikzcd} & \omega \arrow[r, "s"] \arrow[d, "h"] & \omega \arrow[d, "h"] \\ 1 \arrow[ur, "O"] \arrow[dr, "O'"'] & & \\ & \omega' \arrow[r, "s'"] & \omega' \end{tikzcd}$$

commutes would be iso (i.e. a bijection) in **Set**. (1)′ and (2)′ are used to show that h is injective, and (3)′ applied to $h(\omega) \subseteq \omega'$ shows that $h(\omega) = \omega'$, i.e. h is surjective.

In this section we show that an nno in any topos satisfies analogues of (1), (2), (3). We will then appeal to some deep results of Freyd [72] to show that the notion of a natural numbers object is exactly characterised by categorial Peano Postulates.

It should be clear to the reader how the condition "$s(x) \neq 0$" abstracts to

PO: $O \notin s$, i.e.

$$\begin{tikzcd} & 1 \arrow[dl, "x"'] \arrow[dr, "O"] & \\ N \arrow[rr, "s"] & & N \end{tikzcd}$$

does not commute for any "natural number" $x: 1 \to N$.

Alternatively, Postulate (1) asserts that

$$s^{-1}(\{0\}) = \emptyset,$$

where $s^{-1}(\{0\}) = \{x \in \omega : s(x) = 0\}$ is the inverse image of $\{0\}$ under s. According to §3.13, the inverse image of a subset of the codomain arises by pulling the inclusion of that subset back along the function in question. Hence we contemplate another abstraction of Postulate (1)

P1:

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & 1 \arrow[d, "O"] \\ N \arrow[r, "s"] & N \end{tikzcd}$$

is a pullback.

Postulate (2) states precisely that the successor function is injective, and so becomes

P2: $N \xrightarrow{s} N$ *is monic.*

In Postulate (3), the subset $A \subseteq \omega$ is replaced by a monic $f: a \rightarrowtail N$. Hypothesis (i) becomes $O \in f$, i.e. there is some $x: 1 \to a$ for which

$$\begin{tikzcd} & 1 \arrow[dl, "x"'] \arrow[dr, "O"] & \\ a \arrow[rr, tail, "f"] & & N \end{tikzcd}$$

commutes. Hypotheses (ii) states that $s(A) \subseteq A$, where $s(A) = \{s(x): x \in A\}$ is the image of A under s. Recalling the discussion of images at the beginning of §12.6, $s(A)$ generalises to $\mathscr{s}[f]=\mathrm{im}(\mathscr{s}\circ f)$, and since $\mathscr{s}$ and f are monic, $\mathscr{s}[f]\simeq\mathscr{s}\circ f$. Thus (ii) becomes the statement that in Sub(N), $\mathscr{s}\circ f\subseteq f$, i.e.

$$\begin{tikzcd} & a \arrow[dl, "g"'] \arrow[d, "\mathscr{s}\circ f"] \\ a \arrow[r, tail, "f"'] & N \end{tikzcd}$$

commutes for some g.

Altogether then Postulate (3) becomes

P3: *For any subobject* $a\overset{f}{\rightarrowtail}N$ of N, *if*

(i) $O\in f$, *and*
(ii) $\mathscr{s}\circ f\subseteq f$
then $f\simeq 1_N$.

THEOREM 1. *Any natural numbers object* $1\overset{O}{\to}N\overset{\mathscr{s}}{\to}N$ *satisfies P0, P2, and P3.*

PROOF. *P0:* If $\mathscr{s}\circ x=O$ for some $x:1\to N$, then

$$\rho\circ\mathscr{s}\circ x=\rho\circ O$$

and so

$$1_N\circ x=O$$

i.e.

$$x=O \qquad \text{(by definition of } \rho)$$

But then we have $\mathscr{s}\circ O=\mathscr{s}\circ x=O$, and so if h is defined by recursion

$$\begin{tikzcd} & N \arrow[r, "\mathscr{s}"] \arrow[d, "h"] & N \arrow[d, "h"] \\ 1 \arrow[ur, "O"] \arrow[r, "false"'] & \Omega \arrow[r, "\neg"'] & \Omega \end{tikzcd}$$

from *false* and $\neg$ we would have

$$\begin{aligned} true &= \neg\circ false \\ &= h\circ\mathscr{s}\circ O \\ &= h\circ O \\ &= false \end{aligned}$$

which would make $\mathscr{C}$ degenerate.

P2: $\mathscr{s}$ was shown to be monic in the last section.

P3: Suppose $f \subseteq \mathbf{1}_N$, and there are commuting diagrams

$$\begin{tikzcd} & 1 \arrow[dl, "x"'] \arrow[dr, "O"] & \\ a \arrow[rr, tail, "f"] & & N \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} & a \arrow[dl, "g"'] \arrow[dr, "\mathscr{s} \circ f"] & \\ a \arrow[rr, "f"] & & N \end{tikzcd}$$

Let h be defined from x and g by simple recursion and consider

$$\begin{tikzcd} & N \arrow[r, "\mathscr{s}"] \arrow[d, "h"] & N \arrow[d, "h"] \\ 1 \arrow[ur, "O"] \arrow[r, "x"] \arrow[dr, "O"'] & a \arrow[r, "g"] \arrow[d, "f"] & a \arrow[d, "f"] \\ & N \arrow[r, "\mathscr{s}"] & N \end{tikzcd}$$

The upper triangle and square commute by definition of h, the lower two by the previous diagrams. Hence the whole diagram commutes, revealing $f \circ h$ as the unique arrow defined by recursion from O and $\mathscr{s}$. But obviously these last two arrows recursively define $\mathbf{1}_N$. Hence

$$\begin{tikzcd} & N \arrow[dl, "h"'] \arrow[dr, "\mathbf{1}_N"] & \\ a \arrow[rr, tail, "f"] & & N \end{tikzcd}$$

commutes, showing that $\mathbf{1}_N \subseteq f$, and so $\mathbf{1}_N \simeq f$. □

EXERCISE 1. Derive *P0* from *P1*. □

The elements of N in **Set** are of course just the finite ordinals $n \in \omega$. Correspondingly, in $\mathscr{C}$ we define, for each $n \in \omega$, an arrow $\mathbf{n}: 1 \to N$ by

$$\mathbf{n} = \underbrace{\mathscr{s} \circ \mathscr{s} \circ \ldots \circ \mathscr{s}}_{n \text{ times}} \circ O$$

The arrows $\mathbf{n}$ will be called the *finite ordinals of* $\mathscr{C}$. Using these, and the more general natural numbers $x: 1 \to N$ of $\mathscr{C}$, we can formulate two variants of the third Peano postulate.

P3A: *For any* $a \overset{f}{\rightarrowtail} N$, *if*

(i) $O \in f$, *and*

(ii) $x \in f$ *implies* $s \circ x \in f$, *all* $1 \xrightarrow{x} N$

then $f \simeq 1_N$.

P3B: *For any* $a \overset{f}{\rightarrowtail} N$, *if*

(i) $O \in f$, *and*
(ii) $\mathbf{n} \in f$ *implies* $s \circ \mathbf{n} \in f$, *all* $n \in \omega$
then $f \simeq 1_N$.

EXERCISE 1. Show that in $\mathbf{Bn}(I)$, $\mathbf{n}$ is the section of $pr_I : I \times \omega \to I$ that has $\mathbf{n}(i) = \langle i, n \rangle$, all i.

EXERCISE 2. Show that in $\mathbf{Bn}(\omega)$, the diagonal map $\Delta : \omega \to \omega \times \omega$ is a natural number $\Delta : 1 \to N$, with $\Delta \neq \mathbf{n}$, all n.

EXERCISE 3. Show that *P3B* implies *P3A* and *P3A* implies *P3* in general.

EXERCISE 4. Show that *P3B* holds in $\mathbf{Set}^{\mathscr{C}}$ and in $\mathbf{Bn}(I)$ and $\mathbf{Top}(I)$.

EXERCISE 5. Use Theorem 7.7.2 to show that in a well-pointed topos *P3* implies *P3A*. □

Before examining *P1*, we look at two further properties of ω in **Set**. First we observe that

$$\omega \underset{s}{\overset{\mathrm{id}}{\rightrightarrows}} \omega \xrightarrow{!} \{0\}$$

is a co-equaliser diagram in **Set**. For if

$$\begin{tikzcd} \omega \arrow[r, shift left, "\mathrm{id}_\omega"] \arrow[r, shift right, "s"'] & \omega \arrow[r, "!"] \arrow[dr, "f"'] & \{0\} \arrow[d, "x"] \\ & & A \end{tikzcd}$$

$f \circ s = f \circ \mathrm{id}_\omega = f$, then for each $n \in \omega$, $f(n+1) = f(n)$, and hence (by induction) $f(n) = f(0)$ all n. Thus f is a constant function with $f(0)$ its sole output. Putting $x(0)=f(0)$ then makes the last diagram commute, and clearly x is uniquely defined and exists iff $f\circ s=f$.

Thus we formulate

F1: $\quad N \xrightarrow{!} 1$ *is the co-equaliser of* $\mathscr{s}$ *and* 1_N.

EXERCISE 6. According to §3.12 the codomain of the co-equaliser of id_ω and s is the quotient set ω/R, where R is the smallest equivalence relation on ω having $nRs(n)$, all $n\in\omega$. Show that there is only one such R, namely the universal relation $R=\omega\times\omega$, having $\omega/R=\{\omega\}$, a terminal object in **Set**. □

Since, in **Set**, $\mathrm{Im}\, s=\{1,2,3,\ldots\}$, we have $\{0\}\cup \mathrm{Im}\, s=\omega$. But (Postulate (1)) $\{0\}\cap \mathrm{Im}\, s=\emptyset$, and so the union is a disjoint one $-\{0\}+\mathrm{Im}\, s\cong\{0\}\cup \mathrm{Im}\, s=\omega$. Identifying $\{0\}$ with $O:1\to\omega$ and $\mathrm{Im}\, s$ with the monic s we have

$$[0,s]\colon 1+\omega\cong\omega,$$

and thus we formulate

F2: $\quad$ *The co-product arrow* $[O,\mathscr{s}]:1+N\to N$ *is iso.*

THEOREM 2. *F1 and F2 hold for any natural numbers object.*

PROOF. *F1:* Suppose that

$$\begin{tikzcd} N \arrow[r, shift left, "1_N"] \arrow[r, shift right, "\mathscr{s}"'] & N \arrow[r, "!"] \arrow[dr, "f"'] & 1 \arrow[d, dashed, "x"] \\ & & a \end{tikzcd}$$

$f\circ\mathscr{s}=f$. Put $x=f\circ O$,

$$\begin{tikzcd} & 1 \arrow[dl, "O"'] \arrow[dr, "x"] & \\ N \arrow[rr, "f"] & & a \end{tikzcd}$$

so that

$$\begin{tikzcd} & N \arrow[r, "\mathscr{s}"] \arrow[d, "f"] & N \arrow[d, "f"] \\ 1 \arrow[ur, "O"] \arrow[dr, "x"'] & & \\ & a \arrow[r, "1_a"] & a \end{tikzcd}$$

commutes. But

$$\begin{tikzcd}
& N \arrow[r, "s"] \arrow[d, "!"] & N \arrow[d, "!"] \\
1 \arrow[ur, "O"] \arrow[dr, "x"'] & 1 \arrow[d, "x"'] & 1 \arrow[d, "x"] \\
& a \arrow[r, "1_a"] & a
\end{tikzcd}$$

commutes, and so by the axiom NNO,

$$\begin{tikzcd}
N \arrow[r, "!"] \arrow[dr, "f"'] & 1 \arrow[d, "x"] \\
& a
\end{tikzcd}$$

commutes as required. That there can be only one such x making this diagram commute follows from the fact that $!: N \to 1$ is epic. To see why, observe that

$$\begin{tikzcd}
1 \arrow[r, "O"] \arrow[dr, "1_1"'] & N \arrow[d, "!"] \\
& 1
\end{tikzcd}$$

commutes, and use the fact that 1_1 is epic (or derive the result directly).

F2: Let $t: 1+N \to 1+N$ be the arrow $j \circ [O, s]$

$$\begin{tikzcd}
1 \arrow[r, "i"] \arrow[dr, "O"'] & 1+N \arrow[d, "{[0, s]}"] & N \arrow[l, "j"'] \arrow[dl, "s"] \\
& N \arrow[d, "j"] & \\
& 1+N &
\end{tikzcd}$$

where i and j are the injections. Let g be defined by recursion from i and t, and consider

$$\begin{tikzcd}
 & N \arrow[r, "\mathscr{s}"] \arrow[d, "g"] & N \arrow[d, "g"] \\
1 \arrow[ur, "O"] \arrow[r, "i"] \arrow[dr, "O"'] & 1+N \arrow[r, "t"] \arrow[d, "{[O,\mathscr{s}]}"] & 1+N \arrow[d, "{[O,\mathscr{s}]}"] \\
 & N \arrow[r, "\mathscr{s}"] & N
\end{tikzcd}$$

Since i is an injection, $[O, \mathscr{s}]\circ i = O$. Since j is an injection, $[O, \mathscr{s}]\circ t = [O, \mathscr{s}]\circ j\circ[O, \mathscr{s}] = \mathscr{s}\circ[O, \mathscr{s}]$. Hence the whole diagram commutes. NNO then gives $[O, \mathscr{s}]\circ g = \mathbf{1}_N$.

Now the diagrams

$$\begin{tikzcd}
 & N \arrow[r, "\mathscr{s}"] \arrow[dd, "j"] & N \arrow[dd, "j"] \\
1 \arrow[ur, "O"] \arrow[dr, "j\circ O"'] & & \\
 & 1+N \arrow[r, "t"] & 1+N
\end{tikzcd}$$

and

$$\begin{tikzcd}
 & N \arrow[r, "\mathscr{s}"] \arrow[dd, "g\circ\mathscr{s}"] & N \arrow[dd, "g\circ\mathscr{s}"] \\
1 \arrow[ur, "O"] \arrow[dr, "j\circ O"'] & & \\
 & 1+N \arrow[r, "t"] & 1+N
\end{tikzcd}$$

both commute. The first is left as an exercise. For the second, observe from the previous diagram that $t\circ g = g\circ\mathscr{s}$. This yields $t\circ g\circ\mathscr{s} = g\circ\mathscr{s}\circ\mathscr{s}$ as desired, and also $t\circ g\circ O = g\circ\mathscr{s}\circ O$. But $t\circ g\circ O = j\circ[O, \mathscr{s}]\circ g\circ O = j\circ\mathbf{1}_N\circ O = j\circ O$, hence $j\circ O = g\circ\mathscr{s}\circ O$, as also desired.

From these last two diagrams, NNO gives $g\circ\mathscr{s} = j$. From the previous one we have $g\circ O = i$. Thus $g\circ[O, \mathscr{s}] = [g\circ O, g\circ\mathscr{s}] = [i, j] = \mathbf{1}_{1\times N}$. Thus we have shown that g is an inverse to $[O, \mathscr{s}]$, making the latter iso. □

EXERCISE 7. In deriving *F1* we used the fact that $! : N \to 1$ is epic. Show in any category with 1, that if a is non-empty, i.e. has an element $x : 1 \to a$, then $! : a \to 1$ is epic. □

LEMMA. *In any topos, if*

$$\begin{tikzcd} d \arrow[r, tail, "g"] \arrow[d, "f"'] & a \arrow[d, "k"] \\ b \arrow[r, "h"] & c \end{tikzcd}$$

is a pushout with g *monic, then* h *is monic and the square is a pullback.*

PROOF. By the Partial Arrow Classifier Theorem (§11.8), using the classifier $\eta_b : b \to \tilde{b}$ associated with b, we have a diagram

$$\begin{tikzcd} d \arrow[r, tail, "g"] \arrow[d, "f"'] & a \arrow[d, "k"] \arrow[ddr, bend left, "\tilde{f}"] & \\ b \arrow[r, "h"] \arrow[drr, tail, bend right, "\eta_b"'] & c \arrow[dr, dashed, "x"] & \\ & & \tilde{b} \end{tikzcd}$$

whose boundary is a pullback. The co-universal property of pushouts then implies the existence of the unique x as shown to make the whole diagram commute. That the original square is also a pullback is then a straightforward exercise. Finally, since $x \circ h = \eta_b$ is monic, h must be too.

□

THEOREM 3. *Any natural numbers object satisfies*

P1:

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & 1 \arrow[d, "O"] \\ N \arrow[r, "s"] & N \end{tikzcd}$$

is a pullback.

PROOF. Since, by *F2* we have an isomorphism $[O, s] : 1 + N \to N$, it is readily established that

$$1 \xrightarrow{O} N \xleftarrow{s} N$$

is a co-product diagram in $\mathscr{E}$. The co-universal property of co-products then makes it immediate that the diagram for *P1* is a pushout, and so the result follows by the Lemma, since $0 \to 1$ is monic (§3.16). □

THEOREM 4. *The conditions P1, P2, and P3 together imply F1 and F2 for any diagram*

$$1 \xrightarrow{O} N \xrightarrow{s} N$$

in a topos.

PROOF. *F1:* Suppose that $f \circ s = f$, and let $g : b \rightarrowtail N$ be the equaliser

$$\begin{tikzcd} b \arrow[r, tail, "g"] & N \arrow[r, "!_N"] \arrow[dr, "f"'] & 1 \arrow[d, "f \circ O"] \\ & & a \end{tikzcd}$$

of f and $f \circ O \circ !_N$. Let $f \circ O \circ !_N = h$. Then since

$$\begin{tikzcd} 1 \arrow[r, "O"] \arrow[dr, "1_1"'] & N \arrow[d, "!_N"] \\ & 1 \end{tikzcd}$$

$!_N \circ O = 1_1$, it follows that $h \circ O = f \circ O$. Since g equalises f and h, O must then factor through g, hence $O \in g$.

Next, observe that

$$\begin{tikzcd} N \arrow[r, "s"] \arrow[dr, "!_N"'] & N \arrow[d, "!_N"] \\ & 1 \end{tikzcd}$$

$!_N \circ s = !_N$, from which it follows readily that $h \circ s \circ g = h \circ g$. But $h \circ g = f \circ g = f \circ s \circ g$. Thus $h \circ (s \circ g) = f \circ (s \circ g)$, implying that $s \circ g$ must factor through the equaliser g, i.e. $s \circ g \subseteq g$. The postulate *P3* then gives $g \simeq 1_N$, so that g is iso, in particular epic, the latter being enough to give $f = h = f \circ O \circ !_N$. Hence

$$\begin{tikzcd} N \arrow[r, shift left, "1_N"] \arrow[r, shift right, "s"'] & N \arrow[r, "!"] \arrow[dr, "f"'] & 1 \arrow[d, "f \circ O"] \\ & & a \end{tikzcd}$$

commutes. But $!: N \to 1$ is epic, since N has the element $O: 1 \to N$, and so $f \circ O$ is the only element of a that will make this diagram commute. This establishes *F1*.

F2: By *P2* and *P1*, $\mathfrak{s}$ and O are disjoint monics, so the Lemma associated with Theorem 5.4.3 gives $[O, \mathfrak{s}]$ as monic. To prove *F2* then, it suffices to show that $[O, \mathfrak{s}]$ is epic.

Suppose then that $f \circ [O, \mathfrak{s}] = g \circ [O, \mathfrak{s}]$

$$\begin{tikzcd}
1 \arrow[r, "i"] \arrow[dr, "O"'] & 1+N \arrow[d, "{[O,\mathfrak{s}]}"] & N \arrow[l, "j"'] \arrow[dl, "\mathfrak{s}"] \\
 & N \arrow[d, shift right, "f"'] \arrow[d, shift left, "g"] & \\
 & a &
\end{tikzcd}$$

From the diagram we see that $f \circ O = g \circ O$ and $f \circ \mathfrak{s} = g \circ \mathfrak{s}$. Then if $h: b \rightarrowtail N$ equalises f and g we must have $O \in h$, and since then $f \circ \mathfrak{s} \circ h = g \circ \mathfrak{s} \circ h$, $\mathfrak{s} \circ h$ factors through h, i.e. $\mathfrak{s} \circ h \subseteq h$. Postulate *P3* then gives $h \simeq \mathbf{1}_N$, from which $f = g$ follows. Thus $[0, \mathfrak{s}]$ is right cancellable.

COROLLARY. *In any topos $\mathscr{E}$, the following are equivalent for a diagram of the form $1 \xrightarrow{O} N \xrightarrow{\mathfrak{s}} N$.*

(1) *The diagram is a natural numbers object.*

(2) *The diagram satisfies the Peano Postulates P1, P2, and P3.*

(3) *The diagram satisfies the Freyd Postulates F1 and F2.*

PROOF. (1) implies (2): Theorems 1 and 3.

(2) implies (3): Theorem 4.

(3) implies (1): Freyd [72], Theorem 5.4.3. □

The equivalence of (1) and (3) established by Freyd requires techniques beyond our present scope. Freyd also establishes the equivalence in any topos of

(a) *there exists a natural numbers object,*

(b) *there exists a monic $f: a \rightarrowtail a$ and an element $x: 1 \to a$ of its domain for which*

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & 1 \arrow[d, "x"] \\
a \arrow[r, tail, "f"] & a
\end{tikzcd}$$

is a pullback, and

(c) *there exists an isomorphism of the form* $1+a \cong a$.

With regard to (c), observe that in **Finset**, where there is no nno, isomorphic objects are finite sets with the same number of elements, and $1+a$ has one more element than a.

The intuitive import of (b) is that the sequence $x, f(x), f(f(x)), \ldots$ has all terms distinct and so forms a subset $\{x, f(x), \ldots\}$ of a isomorphic to ω. The natural numbers object then arises as the "intersection" of all subobjects $g : b \rightarrowtail a$ that contain this set, i.e. have $x \in g$ and $f \circ g \subseteq g$. These ideas are formalised in another approach to the characterisation of natural numbers objects developed by Osius [75].

Exercise 8. Derive *P1* and *P2* directly from *F2*. □