5. Arithmetic of the naturals

In order to bring the abstract treatment of the naturals closer to our intuition, we will now define the basic operations of *addition*, *multiplication*, *powers* etc on the naturals and prove the standard relations between them.

5.1 Addition.

We will spend most of the time on addition as other operations are handled analogously. Pick $m \in \mathbb{N}$ and invoke the recursion principle in Theorem 4.5 for the choice $E := \mathbb{N}$, $a := m$ and $\mathfrak{h} := S$ to define $\{X_n : n \in \mathbb{N}\}$ such that

$$X_0 = m \quad \text{and} \quad \forall n \in \mathbb{N}\colon X_{S(n)} = S(X_n). \tag{5.1}$$

Then we denote

$$m + n := X_n. \tag{5.2}$$

As consequence of the construction (5.1) we get a symbol $m + n$ satisfying

(1) $\forall m \in \mathbb{N}\colon m + 0 = m$, and
(2) $\forall m, n \in \mathbb{N}\colon m + S(n) = S(m + n)$.

From these observation we now derive further facts about addition relying, predominantly, on the Induction Principle.

We will now prove that the operation $m, n \mapsto m + n$ is commutative. We begin by:

Lemma 5.1 $\forall m \in \mathbb{N}\colon 0 + m = m$

Proof. Let P_m denote the logical proposition $0 + m = m$. Then P_0 is TRUE because (1) above implies $0 + 0 = 0$. Next assume P_m holds for some $m \in \mathbb{N}$. Then

$$0 + S(m) \overset{(2)}{=} S(0 + m) \overset{P_m}{=} S(m). \tag{5.3}$$

It follows that $P_m \Rightarrow P_{S(m)}$. By the Induction Lemma, $\{m \in \mathbb{N}\colon 0 + m = m\} = \mathbb{N}$. □

Next we need:

Lemma 5.2 $\forall m, n \in \mathbb{N}\colon m + S(n) = S(m) + n$

Proof. Fix $m \in \mathbb{N}$ and let P_n be the statement $m + S(n) = S(m) + n$. Since

$$m + S(0) \overset{(2)}{=} S(m + 0) \overset{(1)}{=} S(m) \overset{(1)}{=} S(n) + 0 \tag{5.4}$$

we get that P_0 is TRUE. Next assume that P_n is TRUE for some $n \in \mathbb{N}$. Then

$$m + S(S(n)) \overset{(2)}{=} S(m + S(n)) \overset{P_n}{=} S(S(m) + n) \overset{(2)}{=} S(m) + S(n) \tag{5.5}$$

implying $P_{S(n)}$. Hence, $\forall n \in \mathbb{N}\colon P_n \Rightarrow P_{S(n)}$ and, by the Induction lemma, $\{n \in \mathbb{N}\colon m + S(n) = S(m) + n\} = \mathbb{N}$. As this holds for all $m \in \mathbb{N}$, we are done. □

Hence we finally conclude:

Proposition 5.3 (Commutativity of addition)

$$\forall m, n \in \mathbb{N}\colon \; m + n = n + m \tag{5.6}$$

Proof. Let Q_m be the statement $\forall n \in \mathbb{N} \colon m+n = n+m$. Then Q_0 is TRUE by (1) and Lemma 5.1. Assume now that Q_m is TRUE. Then for any $n \in \mathbb{N}$,

$$S(m)+n \overset{\text{Lemma 5.2}}{=} m+S(n) \overset{(2)}{=} S(m+n) \overset{Q_m}{=} S(n+m) \overset{(2)}{=} n+S(m). \tag{5.7}$$

It follows that $Q_m \Rightarrow Q_{S(m)}$. By induction, $\{m \in \mathbb{N} \colon Q_m\} = \mathbb{N}$. □

Similarly we also prove that the operation $m, n \mapsto m+n$ is associative:

Proposition 5.4 (Associativity of addition)

$$\forall m,n,k \in \mathbb{N} \colon \; m+(n+k) = (m+n)+k \tag{5.8}$$

Proof. Left as a homework exercise. Commutativity should not be required. □

5.2 Ordering of the naturals.

A useful property of addition is that it acts injectively:

Lemma 5.5 $\forall m,n,\ell \in \mathbb{N} \colon m+n = m+\ell \Rightarrow n = \ell$

Proof. Let P_m be the statement $\forall n,\ell \in \mathbb{N} \colon m+n = m+\ell \Rightarrow n = \ell$. By (1) and Lemma 5.1, P_0 is TRUE. Now assume P_m is TRUE for some $m \in \mathbb{N}$. For $n, \ell \in \mathbb{N}$ are such that

$$S(m)+n = S(m)+\ell \tag{5.9}$$

then Lemma 5.2 implies $S(m)+n = m+S(n)$ and $S(m)+\ell = \ell+S(n)$

$$m+S(n) \overset{\text{Lemma 5.2}}{=} S(m)+n = S(m)+\ell \overset{\text{Lemma 5.2}}{=} m+S(\ell) \tag{5.10}$$

thus implying $S(n) = S(\ell)$ via P_m. But S is injective by P4 and so we get $n = \ell$. Hence $P_m \Rightarrow P_{S(m)}$ and, by induction, P_m is TRUE for all $m \in \mathbb{N}$. □

This property implies that, given $m \in \mathbb{N}$, for each $n \in \mathbb{N}$ the equation $n = m+s$ has *at most one* solution for s in $\mathbb{N}$. We can formally describe the pairs $(m,n) \in \mathbb{N} \times \mathbb{N}$ for which the solution exists by way of the *less than or equal* relation $\leqslant$ defined by

$$m \leqslant n \quad \Leftrightarrow \quad \exists s \in \mathbb{N} \colon n = m+s. \tag{5.11}$$

Here are some properties of this relation:

Lemma 5.6 *The relation $\leqslant$ is reflexive, antisymmetric and transitive.*

Proof. Reflexivity is immediate from (1) and transitivity follows from the associativity of addition. So the main point to check is antisymmetry. For that assume $m,n \in \mathbb{N}$ are such that $m \leqslant n \wedge n \leqslant m$. Then there are $r,s \in \mathbb{N}$ such that $m = n+s \wedge n = m+r$. Putting these together and invoking the associativity of addition, we get $n = n+(s+r)$. Lemma 5.5 and (1) then force $s+r = 0$. By P3 and (2) above, r cannot be a successor and so $r = 0$. Then also $s = 0$ whereby we conclude

$$\forall m,n \in \mathbb{N} \colon \; m \leqslant n \wedge n \leqslant m \Rightarrow m = n \tag{5.12}$$

meaning that $\leqslant$ is antisymmetric. □

It easy to check that the following properties of $\leqslant$ are true:

Lemma 5.7 *We have*

$$\forall n \in \mathbb{N}\colon\ 0 \leqslant n \tag{5.13}$$

$$\forall n \in \mathbb{N}\colon\ n \leqslant S(n) \tag{5.14}$$

and

$$\forall m, n \in \mathbb{N}\colon m \leqslant n \Rightarrow S(m) \leqslant S(n) \tag{5.15}$$

Proof. Left to a homework exercise. □

An important point of the relation $\leqslant$ is that it is *connex*, meaning that every pair of naturals are ordered one or the other way. This is usually phrased by saying that $\leqslant$ is a *total ordering* in the following sense:

Lemma 5.8 (Total-ordering of $\mathbb{N}$)

$$\forall m, n \in \mathbb{N}\colon \quad m \leqslant n \vee n \leqslant m \tag{5.16}$$

Proof. Let P_m be the statement $\forall n \in \mathbb{N}\colon m \leqslant n \vee n \leqslant m$. Then P_0 is TRUE by (5.13) so assume that P_m holds for some $m \in \mathbb{N}$ and let $n \in \mathbb{N}$. If $n \leqslant m$ or $n = m$ then (5.14) and transitivity imply $n \leqslant S(m)$. In the opposite case we must have $m \leqslant n$ (as P_m was assumed to hold) and $m \neq n$. The definition (5.11) and Lemma 4.2 then show existence of an $r \in \mathbb{N}$ such that

$$n = m + S(r) \overset{\text{Lemma 5.2}}{=} S(m) + r \tag{5.17}$$

proving $S(m) \leqslant n$ and thus also $P_m \Rightarrow P_{S(m)}$. Hence, P_m is TRUE for all $m \in \mathbb{N}$. □

Note that we can re-state Lemma 5.8 as saying that at least one of $n = m + r$ or $m = n + r$ has a solution for r in the naturals.

5.3 Multiplication, powers, factorial.

Moving to a definition of multiplication, pick $m \in \mathbb{N}$ and use Theorem 4.5 with the choices $E := \mathbb{N}$, $\mathfrak{h}(r) := r + m$ and $a := 0$ to construct $\{X_n\colon n \in \mathbb{N}\}$ such that

$$X_0 = 0 \quad \wedge \quad \forall n \in \mathbb{N}\colon X_{S(n)} = X_n + m. \tag{5.18}$$

We will write $n \cdot m$ for X_n and thus get

$$0 \cdot m = 0 \quad \wedge \quad \forall n \in \mathbb{N}\colon S(n) \cdot m = n \cdot m + m \tag{5.19}$$

We also define the *unity* in $\mathbb{N}$ by

$$1 := S(0) \tag{5.20}$$

and observe that

$$S(n) = S(n + 0) = n + S(0) = n + 1 \tag{5.21}$$

which will eventually allow us to drop the notation using the successor function and write it as "plus one" instead. The following properties are then checked:

Proposition 5.9 (Properties of multiplication on $\mathbb{N}$) *We have:*

(1) (Commutative law) $\forall m, n \in \mathbb{N}\colon m \cdot n = n \cdot m$,
(2) (Associative law) $\forall m, n, k \in \mathbb{N}\colon (m \cdot n) \cdot k = m \cdot (n \cdot k)$,
(3) (Distributive law) $\forall m, n, k \in \mathbb{N}\colon (n + k) \cdot m = (n \cdot m) + (k \cdot m)$
(4) (Zero and unity) $\forall m \in \mathbb{N}\colon 0 \cdot m = 0 \wedge 1 \cdot m = m$
(5) (Injectivity) $\forall m, n, k \in \mathbb{N}\colon k \neq 0 \wedge k \cdot m = k \cdot n \Rightarrow m = n$

Proof. A somewhat tedious but doable exercise that we leave to the reader. □

Multiplication also behaves nicely around the total ordering relation:

Lemma 5.10 *We have*

$$\forall m,n,r \in \mathbb{N}\colon\ m \leqslant n \ \Rightarrow\ r \cdot m \leqslant r \cdot n \tag{5.22}$$

Proof. Left to homework exercise. □

With multiplication in place, we can now define natural *powers*. Here we pick $m \in \mathbb{N}$ and use Theorem 4.5 to construct $\{m^n \colon n \in \mathbb{N}\}$ satisfying

$$m^0 = 1 \quad \wedge \quad \forall n \in \mathbb{N}\colon m^{S(n)} = m \cdot m^n. \tag{5.23}$$

Note that this entails $m^0 = 1$ (even for $m = 0$) while $0^n = 0$ for $n \neq 0$. Similarly, $1^n = 1$ for all $n \in \mathbb{N}$. The following properties will again be of relevance:

Lemma 5.11 (Powers) *Let* $m \in \mathbb{N} \smallsetminus \{0\}$. *Then*

(1) $\forall r,s \in \mathbb{N}\colon m^{r+s} = m^r \cdot m^s$,
(2) $\forall r,s \in \mathbb{N}\colon m^{r \cdot s} = (m^r)^s$.

Proof. Proved readily by induction. □

A related construction permits us to construct the *factorial* of n, with notation $n!$, by imposing

$$0! = 1 \quad \text{and} \quad \forall n \in \mathbb{N}\colon\ S(n)! = S(n) \cdot n! \tag{5.24}$$

By (5.21), the statement in the second part can be written as $(n+1)! = (n+1) \cdot n!$, which is the recursive form of the informal expression $n! = n \cdot (n-1) \cdot \dots \cdot 1$.

Factorials appear frequently in combinatorial arguments (indeed, $n!$ is the number of permutations of n elements) but also appears in analytic expressions (thanks to, for instance, Taylor's theorem).