The natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}$$

The natural numbers come with an *addition* $+$, a *multiplication* $\cdot$ and an *order* $<$

$$\forall p,\ q \in \mathbb{N},\quad p + q \in \mathbb{N}.$$
$$\forall p,\ q \in \mathbb{N},\quad p \cdot q \in \mathbb{N}.$$

$\forall\ p,\ q \in \mathbb{N}$, exactly one of the following holds:

$$p < q, \qquad q < p, \qquad p = q.$$

1. Basic properties

1.1. **Properties of arithmetic.** Addition is *associative*

$$(p + q) + r = p + (q + r)\ \forall\ p,\ q,\ r \in \mathbb{N},$$

and *commutative*

$$p + q = q + p\ \forall\ p,\ q \in \mathbb{N}.$$

The zero element 0 has the special property

$$p + 0 = p = 0 + p\ \forall\ p \in \mathbb{N}.$$

Multiplication is also *associative*

$$(p \cdot q) \cdot r = p \cdot (q \cdot r)\ \forall\ p,\ q \in \mathbb{N},$$

and *commutative*

$$p \cdot q = q \cdot p\ \forall\ p,\ q \in \mathbb{N}.$$

The element 1 has the property

$$1 \cdot n = n\ \forall\ n \in \mathbb{N}$$

The *Distributive Law* holds:

$$p \cdot (q + r) = (p \cdot q) + (p \cdot r)\ \forall\ p,\ q,\ r \in \mathbb{N}.$$

1.2. **Properties of order.**

$$0 = n\ \vee\ 0 < n \quad \forall\ n \in \mathbb{N}$$
$$p < q \Leftrightarrow p + n < q + n \quad \forall\ n \in \mathbb{N}$$
$$p < q \Leftrightarrow n \cdot p < n \cdot q \quad \forall\ n \in \mathbb{N},\quad n > 0.$$

1.3. **Deductions.** Various other properties can be deduced from those already given.

For example

$$\forall p,\ q \in \mathbb{N},\quad p + q = p \Leftrightarrow q = 0.$$

Proof If $q > 0$ then $p < p + q$. But $p + q = p$ and $p < p$ is impossible. So $q = 0$.

Another example:

$$\forall p \in \mathbb{N},\ 0 \cdot p = 0.$$

Proof $0 \cdot p = (0 + 0) \cdot p = 0 \cdot p + 0 \cdot p$. So $0 \cdot p = 0$.

2. Peano's Axioms

Peano, who died in 1935, formulated his axioms for the strictly positive integers in 1889, using less concise axioms given a year earlier by Richard Dedekind.

2.1. **Axioms for $\mathbb{Z}_+$.** The axioms for the set $\mathbb{Z}_+$ are as follows. Here, the symbol $\subset$ means "is a subset of". We say that A is a subset if B, written $A \subset B$, if every element of A is an element of B.

(1) There is a strictly positive integer called 1, that is, $1 \in \mathbb{Z}_+$
(2) Every strictly positive integer n has a *successor* called $n + 1$.
(3) $1 \neq n + 1$ for any $n \in \mathbb{Z}_+$
(4) If n and $m \in \mathbb{Z}_+$ and $n + 1 = m + 1$ then $n = m$.
(5) If $A \subset \mathbb{Z}_+$, and $1 \in A$, and $n + 1 \in A$ whenever $n \in A$, then $A = \mathbb{Z}_+$, that is,

$$(A \subset \mathbb{Z}_+ \wedge 1 \in A \wedge (n \in A \Rightarrow n + 1 \in A)) \Rightarrow A = \mathbb{Z}_+.$$

From these axioms, the arithmetic and order on the strictly positive integers can be defined, and all the properties relating arithmetic and order can be deduced. The fifth axiom is the axiom is the one which validates *induction*. Induction is an argument which can be carried out for the strictly positive integers, or for the natural numbers, but not for the rational numbers or the real numbers (for example). So it is the fifth axiom which distinguishes the strictly positive integers or natural numbers from the rational or real numbers.

2.2. **Axioms for $\mathbb{N}$.** Peano originally formulated his axioms for $\mathbb{Z}_+$. But the axioms also hold for the set of natural numbers n if we define

$$\mathbb{N} = \mathbb{Z}_+ \cup \{0\},$$

$$0 \notin \mathbb{Z}_+$$

$$n + 0 = n \ \ \forall \ \ n \in \mathbb{N}$$

Also, the successor $0 + 1$ of 0 is 1. The axioms for the set of natural numbers $\mathbb{N}$ are then as follows.

(1) There is a natural number called 0, that is, $0 \in \mathbb{N}$
(2) Every natural number n has a *successor* called $n + 1$, with the successor $0 + 1$ of 0 being called 1.
(3) $0 \neq n + 1$ for any $n \in \mathbb{N}$. In contrast, $n + 0$ is defined to be n, for all $n \in \mathbb{N}$.
(4) If n and $m \in \mathbb{N}$ and $n + 1 = m + 1$ then $n = m$.
(5) If $A \subset \mathbb{N}$, and $0 \in A$, and $n + 1 \in A$ whenever $n \in A$, then $A = \mathbb{N}$, that is,

$$(A \subset \mathbb{N} \wedge 0 \in A \wedge (n \in A \Rightarrow n + 1 \in A)) \Rightarrow A = \mathbb{N}.$$

3. Induction

3.1. **Induction for $\mathbb{N}$.** The fifth axiom is the one which makes induction work. Inductive arguments work as follows. Here is the pattern for $\mathbb{N}$. Suppose we want to show that some property holds for all natural numbers n. Then we carry out the following steps.

Base case We prove the property holds for $n = 0$.

Inductive step We prove that if the property holds for a natural number n, then it also holds for $n + 1$.

Finishing off By Peano's fifth axiom, the set of natural numbers for which the property holds is the set $\mathbb{N}$ of all natural numbers.

If we want to write out an inductive argument, we do not need to be quite as formal as this. But we do need each of these three steps, in some form. So we need the following.

Base case Show true for $n = 0$

Inductive step Show that if true for n, then true for $n + 1$.

- Therefore, *by induction*, true for all $n \in \mathbb{N}$.

3.2. **Induction for $\mathbb{Z}_+$.** If we want to prove a property for all strictly positive integers n, then we do very similar steps.

Base case We prove the property holds for $n = 1$.

Inductive step We prove that if the property holds for a strictly positive integer n, then it also holds for $n + 1$.

Finishing off By Peano's fifth axiom, the set of strictly positive integers for which the property holds is the set $\mathbb{Z}_+$ of all strictly positive integers.

3.3. **Induction for $n \geq k$.** If $k \in \mathbb{N}$ we want to prove a property for all integers $n \geq k$ (which are, of course, all natural numbers, because if $n \geq k$ then $n \geq 0$) then the steps in the proof are as follows.

Base case We prove the property holds for $n = k$.

Inductive step We prove that if the property holds for an integer $n \geq k$, then it also holds for $n + 1$.

Finishing off Let A be the set of natural numbers such that either $n < k$ or the property holds for n. Then $0 \in A$, because either $0 < k$, or $0 = k$, and in this second case the property holds for k. Now we show that if $n \in A$ then $n + 1 \in A$. We see this as follows. If $n < k$ then $n + 1 \leq k$ and so $n + 1 \in A$. If $n \in A$ and the property holds for n then by the Inductive Step, the property holds for $n + 1$, and $n + 1 \in A$. So now by Peano's fifth axiom for $\mathbb{N}$, we have $A = \mathbb{N}$, and the property holds for all $n \geq k$.

Writing this out correctly, it is fine to use the following outline

Base case Show true for $n = k$

Inductive step Show that, if true for an integer $n \geq k$, then also true for $n + 1$.

- Therefore, *by induction*, true for all integers $n \geq k$.

4. Induction examples

4.1. **Example.** Show that, for all $n \in \mathbb{N}$, $2^n > n$.

Base case $2^0 = 1 > 0$, so $2^n > n$ holds for $n = 0$.

Inductive step If $n \in \mathbb{N}$, then

$$2^n > n \Rightarrow 2^{n+1} = 2^n + 2^n \geq (n + 1) + (n + 1) = 2n + 2 \geq n + 2 > n + 1,$$

that is, if $n \in \mathbb{N}$, then $2^n > n \Rightarrow 2^{n+1} > n+1$.

- Therefore, by induction, $2^n > n$ for all $n \in \mathbb{N}$.

4.2. **Example.** Show that, if $x_0 = 1$ and $x_{n+1} = 2x_n + 1$ for all $n \in \mathbb{N}$, then $x_n = 2^{n+1} - 1$ for all $n \in \mathbb{N}$.

Base case $x_0 = 1 = 2^1 - 1$, so $x_n = 2^{n+1} - 1$ holds for $n = 0$.

Inductive step If $n \in \mathbb{N}$, and $x_n = 2^{n+1} - 1$, then

$$x_{n+1} = 2x_n + 1 = 2(2^{n+1} - 1) + 1 = 2^{n+2} - 2 + 1 = 2^{(n+1)+1} - 1.$$

So, for $n \in \mathbb{N}$,

$$x_n = 2^{n+1} - 1 \Rightarrow x_{n+1} = 2^{(n+1)+1} - 1.$$

- So, by induction, $x_n = 2^{n+1} - 1$ for all $n \in \mathbb{N}$.

4.3. **Example.** This example uses sum notation. By definition, for $n \in \mathbb{Z}_+$,

$$1 + 2 + \cdots + (n-1) + n = \sum_{k=1}^{n} k.$$

So, for example,

$$\sum_{k=1}^{1} k = 1, \quad \sum_{k=1}^{2} k = 1 + 2 = 3, \quad \sum_{k=1}^{3} k = 1 + 2 + 3 = 6.$$

Now the problem is to show, using induction, that, for all $n \in \mathbb{Z}_+$,

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Base case $\sum_{k=1}^{1} k = 1 = 1(1+1)/2$, so the case $n = 1$ is true.

Inductive step

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \Rightarrow \sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2n + 2}{2}$$

$$= \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1)(n+1+1)}{2}.$$

So if $n \in \mathbb{Z}_+$,

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{k=1}^{n+1} k = \frac{(n+1)(n+1+1)}{2}.$$

- So, by induction, for all $n \in \mathbb{Z}_+$,

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

4.4. **Example.** Show that $2^n < n!$ for all integers $n \geq 4$

Base case If $n = 4$ then $2^n = 16$ and $n! = 24$. So $2^n < n!$ is true for $n = 4$.

Inductive step If $n \geq 4$,

$$2^n < n! \;\Rightarrow\; 2 \times 2^n < (n+1) \times n! \;\Rightarrow\; 2^{n+1} < (n+1)!.$$

- So, by induction, $2^n < n!$ for all integers $n \geq 4$.

4.5. **Example.** Show that $n^2 < 2^n$ for all integers $n \geq 5$.

Base case $5^2 = 25$ and $2^5 = 32$. So $n^2 < 2^n$ is true for $n = 5$.

Inductive step Suppose that $n \in \mathbb{N}$ and $n \geq 5$. Then

$$(n+1)^2 = n^2 \times \left(1 + \frac{1}{n}\right)^2 \leq \left(1 + \frac{1}{5}\right)^2 \cdot n^2 \leq \left(\frac{6}{5}\right)^2 \cdot n^2$$
$$= \frac{36}{25} \cdot n^2 < 2n^2.$$

So for $n \in \mathbb{N}$ with $n \geq 5$,

$$n^2 < 2^n \;\Rightarrow\; (n+1)^2 = n^2 \times \left(1 + \frac{1}{n}\right)^2 < 2 \times n^2 < 2 \times 2^n = 2^{n+1},$$

that is,

$$n^2 < 2^n \;\Rightarrow\; (n+1)^2 < 2^{n+1}.$$

- So by induction, $n^2 < 2^n$ for all integers $n \geq 5$.

4.6. **Example.** Suppose that a sequence of real numbers x_n is defined by $x_0 = 1$, and, for all $n \in \mathbb{N}$, x_{n+1} is defined in terms of x_n by

$$x_{n+1} = \frac{2x_n + 3}{x_n + 2}.$$

Show that $1 \leq x_n < 2$ for all $n \in \mathbb{N}$.

Base case Since $x_0 = 1$, it is true that $1 \leq x_n < 2$ when $n = 0$.

Inductive step Suppose that $n \in \mathbb{N}$ and $1 \leq x_n < 2$. Then $2x_n + 3 = x_n + 2 + (x_n + 1) > x_n + 2$ – just because $x_n + 1 > 0$. Since $x_n + 2 > 0$, dividing by $x_n + 2$ preserves inequalities. So

$$x_{n+1} = \frac{2x_n + 3}{x_n + 2} > \frac{x_n + 2}{x_n + 2} = 1.$$

So

$$1 \leq x_n < 2 \Rightarrow 1 < x_{n+1}.$$

Also, $2x_n + 3 < 2x_n + 4$, and once again, since $x_n + 2 > 0$, dividing by $x_n + 2$ preserves inequalities. So, just from the assumption that $1 \leq x_n$, we have

$$x_{n+1} = \frac{2x_n + 3}{x_n + 2} < \frac{2x_n + 4}{x_n + 2} = 2,$$

that is

$$1 \leq x_n < 2 \Rightarrow 1 \leq x_{n+1} < 2.$$

In fact, looking at the working we have the stronger statement

$$1 \leq x_n \Rightarrow 1 \leq x_{n+1} < 2.$$

- So, by induction, $1 \leq x_n < 2$ for all $n \in \mathbb{N}$.

4.7. **Example.** Here is another example which uses sum notation. Let $a \in \mathbb{R}$ with $a \neq 1$. Show that, for any $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} a^k = \frac{1 - a^{n+1}}{1 - a}.$$

This is the well known formula for the sum of a finite *geometric series*.

Base case When $n = 0$,

$$\sum_{k=0}^{n} a^k = a^0 = 1 \quad \text{and} \quad \frac{1 - a^{n+1}}{1 - a} = \frac{1 - a}{1 - a} = 1.$$

So the formula is true for $n = 0$.

Inductive step Suppose the formula is true for n. Then

$$\sum_{k=0}^{n+1} a^k = \sum_{k=0}^{n} a^k + a^{n+1} = \frac{1-a^{n+1}}{1-a} + a^{n+1} = \frac{1-a^{n+1}+a^{n+1}-a^{n+2}}{1-a}$$

$$= \frac{1-a^{n+2}}{1-a} = \frac{1-a^{(n+1)+1}}{1-a}.$$

- So if the formula is true for n, it is also true for $n+1$. So by induction the formula is true for all $n \in \mathbb{N}$.

There is another way to prove this formula, which is sometimes known as the *method of telescoping sums*. This is proved as follows.

$$\sum_{k=0}^{n} a^k = \frac{1-a^{n+1}}{1-a} \quad \Leftrightarrow \quad (1-a)\cdot\sum_{k=0}^{n} a^k = 1-a^{n+1}$$

$$\Leftrightarrow \quad \sum_{k=0}^{n}(1-a)a^k = 1-a^{n+1} \quad \Leftrightarrow \quad \sum_{k=0}^{n}(a^k-a^{k+1}) = 1-a^{n+1}$$

But the last statement is true because

$$\sum_{k=0}^{n}(a^k-a^{k+1}) = 1-a+(a-a^2)+\cdots(a^{n-1}-a^n)+(a^n-a^{n+1}) = 1-a^{n+1}.$$

This has been written a bit informally but this will suffice.

5. Setting up arithmetic and order in the natural numbers

Peano's axioms in Section 2 do not mention addition of positive integers in general: all that is given is that a postive integer plus 1 is defined and is another positive integer called the successor of the first one. Nothing is said about multiplication or subtraction or order. All the definitions can be made, and properties derived, using Peano's axioms. In this section, we show how to do at least some of this.

Theorem 5.1. *If $n \in \mathbb{N}$, then either $n = 0$ or n is the successor of some $m \in \mathbb{N}$, that is, $n = m+1$ for some $m \in \mathbb{N}$.*

Proof. Let

$$A = \{0\} \cup \{n \in \mathbb{N} : \exists m \in \mathbb{N}, n = m+1\}.$$

Then, by the definition of A,

$$0 \in A \wedge (n \in A \Rightarrow n+1 \in A).$$

So by Peano's fifth axiom for $\mathbb{N}$, we have $A = \mathbb{N}$, and therefore the theorem holds. □

A very similar theorem holds for $\mathbb{Z}_+$.

Theorem 5.2. *If $n \in \mathbb{Z}_+$, then either $n = 1$ or n is the successor of some $m \in \mathbb{N}$, that is, $n = m+1$ for some $m \in \mathbb{Z}_+$.*

The proof is very similar to that for $\mathbb{N}$, just using Peano's fifth axiom for $\mathbb{Z}_+$ instead of the one for $\mathbb{N}$.

We also have the following.

Theorem 5.3. *If $n \in \mathbb{N}$ then $n \neq n+1$ for any $n \in \mathbb{N}$.*

Proof. **Base case** $0 \neq 1 = 0+1$, so $n \neq n+1$ is true for $n = 0$.

Inductive step Suppose that $n \neq n+1$. By Peano's fourth axiom for $\mathbb{N}$,

$$n+1 = (n+1)+1 \Rightarrow n = n+1$$

So

$$n \neq n+1 \Rightarrow n+1 \neq (n+1)+1.$$

- So by induction, $n \neq n+1$ for all $n \in \mathbb{N}$.

□

5.4. **Definition of addition.** Theorem 5.1 makes it possible to define addition $m+n$ for any m and $n \in \mathbb{N}$. We define $m+0 = m$, and $m+1$ is just the integer which is called the successor of m, in Peano's axioms. So $n+m$ is defined for $m = 0$ and $m = 1$. Since $m+0 = m$ and $0+1 = 1$ for any $m \in \mathbb{N}$, we have

$$(m+0)+1 = m+1 = m+(0+1).$$

Now if $m \in \mathbb{N}$ and $m+n$ is defined for some $n \in \mathbb{N}$, then we define

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

that is, $m+(n+1)$ is the successor of $m+n$. This is consistent with the definitions of $m+0$ and $m+1$, as we have just seen. then we have the following.

Theorem 5.5. *If $m \in \mathbb{N}$ then $m+n$ is defined for all $n \in \mathbb{N}$.*

Proof. Fix $m \in \mathbb{N}$. Let A be the set of $n \in \mathbb{N}$ such that $m+n$ is defined. Then $0 \in A$. Also, if $n \in A$ then $n+1 \in A$, because $m+(n+1)$ is defined to be the successor of $m+n$. So

$$0 \in A \wedge (n \in A \Rightarrow n+1 \in A).$$

So $A = \mathbb{N}$ by Peano's fifth axiom, and $m+n$ is defined for all $n \in A$. □

Theorem 5.6. $0+n = n$ *for all* $n \in \mathbb{N}$.

Proof.

Base case By definition, $0+0 = 0$. So $0+n = n$ is true for $n = 0$.

Inductive step Suppose that $n \in \mathbb{N}$ and $0+n = n$. Then $0+(n+1) = (0+n)+1$ by the definition of $0+(n+1)$ as the successor of $0+n$. We have seen that this holds for $n = 0$ also. So

$$0+n = n \Rightarrow 0+(n+1) = n+1.$$

- So by induction, $0+n = n$ for all $n \in \mathbb{N}$.

□

Since $n+0 = n$ for all $n \in \mathbb{N}$, by definition, Theorem 5.5 implies the following.

Additive property of 0

$$0+n = n = n+0 \quad \forall \quad n \in \mathbb{N}.$$

Theorem 5.7. *For all $n \in \mathbb{N}$, and $m \in \mathbb{N}$, and $p \in \mathbb{N}$,*

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

Proof. Let m and $n \in \mathbb{N}$. Then $m+(n+p) = (m+n)+p$ is true for $p = 0$, because $m+(n+0) = m+n$ by the definition of $n+0$, and $(m+n)+0 = m+n$ by the definition of $(m+n)+0$. So to prove the theorem for some m and $n \in \mathbb{N}$, we only need to prove it for all $p \in \mathbb{Z}_+$.

Base case $m + (n + 1) = (m + n) + 1$by the definition of $m + (n + 1)$ as the successor $(m + n) + 1$ of $m + n$. So $m + (n + p) = (m + n) + p$ is true for $p = 1$.

Inductive step If $p \in \mathbb{Z}_+$ and

$$m + (n + p) = (m + n) + p,$$

then

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

by the definition of $n + (p + 1)$ as the successor $(n + p) + 1$ of $n + p$, and

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

by the definition of $m + ((n + p) + 1)$ as the successor $(m + (n + p)) + 1$ of $m + (n + p)$. So these three equations give

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

But by the definition of $(m+n)+(p+1)$ as the successor $((m+n)+p)+1$, we have

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

So, for $p \in \mathbb{Z}_+$

$$m + (n + p) = (m + n) + p \quad \Rightarrow m + (n + (p + 1)) = (m + n) + (p + 1).$$

- So, by induction, $m + (n + p) = (m + n) + p$ for all $p \in \mathbb{Z}_+$.

So, for any m and $n \in \mathbb{N}$, and any $p \in \mathbb{N}$,

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

□

This is the theorem which gives: **Associativity of addition** For all m, n, $p \in \mathbb{N}$,

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

Now we have some theorems which lead to what is called *commutativity* of addition.

Theorem 5.8. *$n + 1 = 1 + n$ for all $n \in \mathbb{N}$.*

Proof.

Base Case This is true for $n = 0$, by the definitions $0 + 1 = 1$ and $1 + 0 = 1$.

Inductive step Suppose that $n \in \mathbb{N}$ and $n + 1 = 1 + n$. Then

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

using Theorem 5.7 for the second equality. So for $n \in \mathbb{N}$,

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

- So by induction, $n + 1 = 1 + n$ for all $n \in \mathbb{N}$.

□

Theorem 5.9. *$m + n = n + m$ for all m and $n \in N$.*

Proof. Let $m \in \mathbb{N}$. We already know that $m + 0 = 0 + m$. So it suffices to prove that $m + n = n + m$ for all , $\in \mathbb{Z}_+$. Once again, we prove this by induction.

Base Case By Theorem 5.8, $m + 1 = 1 + m$. So $m + n = n + m$ is true when $n = 1$.

Inductive step Suppose that $n \in \mathbb{Z}_+$ and $m + n = n + m$. Then, by the definition of $m + (n + 1)$ as the successor $(m + n) + 1$ of $m + n$ for the first equality in the next line, a we have

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

But $n + (m + 1)$ is the successor $(n + m) + 1$ of $n + m$, and $m + 1 = 1 + m$ by Theorem 5.8. So we have

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

Finally, by Theorem 5.7 with n and 1 and m replacing n and n and p, we have

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

So altogether, if $n \in \mathbb{Z}_+$,

$$m + n = n + m \quad \Rightarrow \quad m + (n + 1) = (n + 1) + m$$

- So by induction $m + n = n + m$ for all $n \in \mathbb{Z}_+$.

So $m + n = n + m$ for all $m \in \mathbb{N}$ and $n \in \mathbb{N}$. □

This is the theorem which gives:

Commutativity of addition For all m and $n \in \mathbb{N}$, $m + n = n + m$.

The basic properties involving addition of natural numbers are now complete. It is not possible to give the definitions of the other arithmetic operations (multiplication and subtraction) and their properties without spending a lot more time. Similarly, it would take a long time to define order of natural numbers, and to give all the properties of order, and of order and arithmetic together. Instead, here are some basic definitions, which can be justified.

5.10. **Definition of multiplication.** For any $m \in \mathbb{N}$, we define

$$m \cdot 0 = 0$$

Then if $m \cdot n$ has been defined, we define $m \cdot (n + 1)$ by

$$m \cdot (n + 1) = (m \cdot n) + m.$$

From this definition, it follows that, for all $m \in N$,

$$m \cdot 1 = m.$$

It then follows from Peano's fifth axiom – which really means, by induction — that multiplication $m \cdot n$ is defined for all $m \in \mathbb{N}$ and $n \in N$. One can show that multiplication obeys all the usual rules. Obtaining all of these properties uses induction.

Distributivity $m \cdot (n + p) = (m \cdot n) + (m \cdot p)$. (This property will be set in a tutorial problem on Problem Sheet 3.)

Associativity $m \cdot (n \cdot p) = (m \cdot n) \times p$ for all m, n, $p \in \mathbb{N}$.

Commutativity $m \cdot n = n \cdot m$ for all m, $n \in \mathbb{N}$.

5.11. **Definition of order.** Order of natural numbers can actually be defined using addition of natural numbers. The key to this is the following theorem.

Theorem 5.12. *Let n and $m \in \mathbb{N}$. Then* exactly *one of the following holds*

- $m = n$.
- $n = m + p$ *for some* $p \in \mathbb{Z}_+$.
- $m = n + p$ *for some* $p \in \mathbb{Z}_+$.

This theorem is automatically true for $n = 0$. It can be deduced for $n = 1$ from Theorem 5.1. Then it is proved by induction for all $n \in \mathbb{Z}_+$.

The definition of order is then: $m < n$ if and only if $n = m + p$ for some $p \in \mathbb{Z}_+$. The following basic property of order then follows from Theorem 5.12.

For all m and $n \in \mathbb{N}$, exactly one of the following holds:

- $m = n$.
- $m < n$.
- $n < m$.

One can then obtain all the basic properties of order, and order related to arithmetic, by induction.