Chapter 1

The Natural Numbers $\mathbb{N}$

The invention of the axiomatic method goes back to the Greeks: Euclid tried to build his geometry on just five postulates, which the Greeks viewed as 'self-evident' truths. It was realized only in the 19th century that these truths were not selfevident at all, but rather a collection of axioms describing Euclidean geometry and distinguishing it from other geometries satisfying other axioms. This insight made mathematicians wonder whether other areas of mathematics could also be desscribed using the axiomatic method.

The axiomatization of modern mathematics was a process that started at the end of the 19th century. In working with Galois groups and, more generally, with permutation groups, mathematicians began to realize that many theorems (Lagrange's result that the order of an element divides the order of the group, Cauchy's theorem that if a prime p divides the order of a group, then the group has an element of order p, Sylow's theorem, or the decomposition of abelian groups like the class group of binary quadratic forms into cyclic subgroups) could be stated and proved for abstract groups. Finding the right axioms of abstract groups was a problem occupying numerous mathematicians from Kronecker to Weber. At the same time, Peano found axiomatic descriptions of the natural numbers and of vector spaces, and Moore came up with the field axioms. Although it was immediately realized that group theory could be built on just the axioms, it took a while until Steinitz did something similar for fields, and the general theory of rings had to wait for Fraenkel and Emmy Noether.

In this chapter we will develop the basic properties of the natural numbers from the Peano axioms; the construction of negative and rational (as well as p-adic, real and hyperreal numbers) will then be built upon the set of natural numbers.

1.1 Peano Axioms

In every deductive theory there are certain statements you must take for granted: you can't prove theorems by assuming nothing. What we are taking for granted here are elementary notions of sets and the basic properties of natural numbers as encoded by the following statements called the Peano axioms: Let $\mathbb{N}$ be a set together with a 'successor' function s such that

N1: $0 \in \mathbb{N}$;

N2: if $x \in \mathbb{N}$, then $s(x) \in \mathbb{N}$;

N3: there is no $x \in \mathbb{N}$ with $s(x) = 0$;

N4: if $s(x) = s(y)$, then $x = y$;

N5: if S is a subset of $\mathbb{N}$ containing 0, and if $s(n) \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

Remark 1. Axiom N1 says that 0 should be a natural number.

Axiom N2 states that s is a map $\mathbb{N} \longrightarrow \mathbb{N}$, that is: each element of $\mathbb{N}$ gets mapped to another element of $\mathbb{N}$.

Think of N3 as saying that 0 is the first natural number, or that '-1' is not an element of $\mathbb{N}$.

Axiom N4 states that the map $s : \mathbb{N} \longrightarrow \mathbb{N}$ is injective. A map $f : A \longrightarrow B$ is called injective (or one-to-one) if $f(a) = f(a')$ for $a, a' \in A$ implies that $a = a'$, in other words: if different elements get mapped to different images.

Axiom N5 is called the Principle of Induction. Assume you want to prove a statement $P(n)$ (say that $n^2 + n$ is even) for all $n \in \mathbb{N}$; let S denote the set of natural numbers $z \in \mathbb{N}$ for which $P(n)$ is true. If you can show that $P(0)$ holds (i.e. that $0 \in S$) and that $P(s(n))$ holds whenever $P(n)$ does (i.e. that $s(n) \in S$ whenever $n \in S$) then this axiom allows you to conclude that $P(n)$ holds for every natural number.

Informally speaking, these axioms describe the basic properties of natural numbers; logicians can prove that if a set $\mathbb{N}$ with a successor function s satisfying N1– N5 exists, then it is essentially unique (this means that the Peano axioms *characterize* the natural numbers), but we won't need this.

What we want to do here is to show how the arithmetic of the natural numbers can be derived from the Peano axioms. We start by giving the natural numbers their usual names: we put $1 := s(0)$, $2 := s(1)$, $3 = s(2)$, $4 = s(3)$, etc.; in particular $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$.

Remark 2. Some mathematicians (including me) prefer not to regard 0 as a natural number and define $\mathbb{N} = \{1, 2, 3, \ldots\}$. The construction of the integers from the naturals, however, would be complicated by the lack of a 0.

Proposition 1.1. *If $x \in \mathbb{N}$ and $x \neq 0$, then there exists a $y \in \mathbb{N}$ such that $x = s(y)$.*

Proof. The following proof is fairly typical for much that follows. Put

$$S = \{x \in \mathbb{N} : \ x = s(y) \text{ for some } y \in \mathbb{N}\} \cup \{0\}.$$

We prove that $S = \mathbb{N}$ by induction.

In fact, $0 \in S$ by definition. Assume that $x \in \mathbb{N}$; then $s(x) \in S$ since $s(x)$ is the successor of x. By the induction axiom N5, we have $S = \mathbb{N}$, that is, every nonzero natural number is a successor. □

1.2 Addition

Next we define an operation $+$ on $\mathbb{N}$ that we call addition. We have to say what $m+n$ should mean. How can we do that in terms of our axioms? We can certainly define $m + 0$ by putting

$$m + 0 := m. \tag{1.1}$$

Now assume that we already know what $m+n$ means; we then define

$$m + s(n) := s(m+n); \tag{1.2}$$

in particular, $m + 1 = m + s(0) = s(m+0) = s(m)$, hence $m + (n+1) := (m+n)+1$.

Combining $1 = s(0)$, $2 = s(1)$ and $1 + 1 = 1 + s(0) = s(1+0) = s(1)$, we find that $1 + 1 = 2$; observe that $2 = s(1)$ is a definition, whereas $1 + 1 = 2$ is a theorem. Before we go on, we prove

Proposition 1.2. *Equations (1.1) and (1.2) define addition $m+n$ for all $m, n \in \mathbb{N}$.*

Proof. This is Peano's original proof: Let $m \in \mathbb{N}$ be any natural number. Let S be the set of all $n \in \mathbb{N}$ for which $m + n$ is defined. We want to show that $m + n$ is defined for all $n \in \mathbb{N}$, i.e., that $S = \mathbb{N}$. We shall accomplish this by using Peano's induction axiom N5.

First, we have $0 \in S$ since, by (1.1), $m + 0$ is defined (it equals m).

Next, if $n \in S$, then $m + n$ is defined, and since $m + s(n) = s(m+n)$ by (1.2), so is $m + s(n)$. In other words: if $n \in S$, then $s(n) \in S$.

By the Induction axiom N5, we conclude that $S = \mathbb{N}$, hence addition $m+n$ is defined for all $n \in \mathbb{N}$ (and also for all $m \in \mathbb{N}$ since m was arbitrary). □

The problem with this proof is that we haven't really defined what it means for addition to be defined. Let us make this more exact: we say that (1.1) and (1.2) define addition on $\mathbb{N}$ if there exists a unique function $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ such that

$$\begin{aligned} f(m,0) &= m \quad \text{and} && (1.3) \\ f(m,s(n)) &= s(f(m,n)) && (1.4) \end{aligned}$$

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

Complete Proof of 1.2. Let us first proof that the function f, if it exists, is unique. So assume that f and g are two functions satisfying (1.3) and (1.4) above. Fix $m \in \mathbb{N}$ and put

$$S = \{n \in \mathbb{N} : f(m,n) = g(m,n)\}.$$

Then $0 \in S$ because $f(m,0) = m = g(m,0)$ by (1.3). Now assume that $n \in \mathbb{N}$. Then

$$\begin{aligned} f(m,s(n)) &= s(f(m,n)) && \text{by (1.3)} \\ &= s(g(m,n)) && \text{since } n \in S \\ &= g(m,s(n)) && \text{by (1.3)} \end{aligned}$$

Thus $s(n) \in S$, hence $S = \mathbb{N}$ by induction.

Now we have to prove that such a function f exists. We do that by proving that for every $n \in \mathbb{N}$, we can define $f(m,n)$ for all $m \in \mathbb{N}$ in such a way that (1.3) and (1.4) are satisfied.

This is clear if $n = 0$ because (1.3) says that $f(m,0) = m$. Assume now that $f(m,n)$ is defined for some $n \in \mathbb{N}$ and all $m \in \mathbb{N}$; then $f(m,s(n)) = s(f(m,n))$ by 1.4, hence $f(m,s(n))$ is defined. The claim now follows from induction. □

Now we can prove that the addition of natural numbers has the 'well known' properties:

Proposition 1.3 (Associativity of Addition)**.** *For all $x, y, z \in \mathbb{N}$, we have $x + (y + x) = (x + y) + z$.*

Proof. Let $x, y \in \mathbb{N}$ be arbitrary and put

$$S = \{z \in \mathbb{N} : \ x + (y + x) = (x + y) + z\}.$$

Again, S is the set of natural numbers $z \in \mathbb{N}$ for which the claim is true, and our task is to show that $S = \mathbb{N}$.

Now $0 \in S$ because

$$\begin{aligned} x + (y + 0) &= x + y && \text{by (1.1)} \\ &= (x + y) + 0 && \text{by (1.1)} \end{aligned}$$

Next assume that $z \in S$. Then we want to show that $s(z) \in S$, and to this end we have to prove that $x + (y + s(z)) = (x + y) + s(z)$. Here we go:

$$\begin{aligned} x + (y + s(z)) &= x + s(y + z) && \text{by (1.2)} \\ &= s(x + (y + z)) && \text{by (1.2)} \\ &= s((x + y) + z) && \text{since } z \in S \\ &= (x + y) + s(z) && \text{by (1.2)} \end{aligned}$$

By the induction principle, this proves that $S = \mathbb{N}$ and we are done. □

Lemma 1.4. *For all $x \in \mathbb{N}$, we have $0 + x = x$.*

By definition we know that $x + 0 = x$; since we haven't proved commutativity of addition yet, we don't know that $0 + x = x$ at this point.

Proof. Let S denote the set of all $x \in \mathbb{N}$ for which $0 + x = x$. Then $0 \in S$ since $0 + 0 = 0$ by (1.1). Now assume that $x \in S$. Then

$$\begin{array}{rcll} s(x) & = & x + 1 & \text{put } n = 0 \text{ in (1.2)} \\ & = & (0 + x) + 1 & \text{since } x \in S \\ & = & 0 + (x + 1) & \text{by Prop. 1.2} \\ & = & 0 + s(x) & \text{put } n = 0 \text{ in (1.2)} \end{array}$$

Thus $S = \mathbb{N}$ by the induction principle. □

Lemma 1.5. *We have $s(x) + y = x + s(y)$ for all $x, y \in \mathbb{N}$.*

Proof. Fix $x \in \mathbb{N}$ and put $S = \{y \in \mathbb{N} : s(x) + y = x + s(y)\}$. Then $0 \in S$ since $s(x) + 0 = s(x) = s(x + 0) = x + s(0) = x + 1$.

Now assume that $y \in S$. Then

$$\begin{array}{rcll} s(x) + s(y) & = & s(s(x) + y) & \text{by (1.2)} \\ & = & s(x + s(y)) & \text{since } y \in S \\ & = & x + s(s(y)) & \text{by (1.2)} \end{array}$$

Thus $s(y) \in S$, hence $S = \mathbb{N}$ by induction. □

Now we can prove

Proposition 1.6 (Commutativity of Addition)**.** *For all $x, y \in \mathbb{N}$ we have $x + y = y + x$.*

Proof. You know the game by now: for an arbitrary $x \in \mathbb{N}$, let S denote the set of all $y \in \mathbb{N}$ such that $x + y = y + x$. By Lemma 1.2, we have $0 \in S$.

Now assume that $y \in S$. Then

$$\begin{array}{rcll} x + s(y) & = & s(x + y) & \text{by (1.2)} \\ & = & s(y + x) & \text{since } y \in S \\ & = & y + s(x) & \text{by (1.1)} \\ & = & s(y) + x & \text{by Lemma 1.2} \end{array}$$

Thus $S = \mathbb{N}$, and we are done. □

Now it's your turn:

Proposition 1.7 (Cancellation Law)**.** *If $x + z = y + z$ for some $x, y, z \in \mathbb{N}$, then $x = y$.*

The proof is left as an exercise.

Lemma 1.8. *For $x, y \in \mathbb{N}$ and $y \neq 0$, we have $x + y \neq x$.*

Proof. Fix $y \in \mathbb{N}$ with $y \neq 0$ and set $S = \{x \in \mathbb{N} : x + y \neq x\}$. Then $0 \in S$ since $0 + y = y \neq 0$ by assumption. Now assume that $x \in S$. We have to prove that $s(x) \in S$. We know that $x \neq x + y$. Since s is injective by N3, we conclude that $s(x) \neq s(x + y)$. But $s(x + y) = s(x) + y$ by definition of addition and by commutativity. □

This lemma is now needed for the proof of the following result that will eventually allows us to define an order on the natural numbers.

Theorem 1.9 (Trichotomy Law for Addition)**.** *For any $x, y \in \mathbb{N}$, exactly one of the following three statements is true:*

(i) $x = y$*;*

(ii) $x = y + z$ *for some nonzero* $z \in \mathbb{N}$*;*

(iii) $y = x + z$ *for some nonzero* $z \in \mathbb{N}$*.*

Proof. We first show that no two of these statements can hold simultaneously.

Assume that (i) and (ii) are both true. Then $x = x + z$, contradicting Prop. 1.2.

The claim that (i) and (iii) [or (ii) and (iii)] cannot hold simultaneously is left as an exercise.

Now we have to prove that, given $x, y \in \mathbb{N}$, at least one of these claims is true. We consider an arbitrary $y \in \mathbb{N}$ and do induction on x, that is, we put

$$S = \{x \in \mathbb{N} : (i) \text{ or } (ii) \text{ or } (iii) \text{ is true}\}.$$

We claim that $x = 0 \in S$. If $0 = y$, then $x = y$, hence (i) holds. Assume therefore that $0 \neq y$. In this case, $y = x + z$ for $z = y$ since $x = 0$.

Now we claim that $x \in S$ implies $s(x) \in S$, so assume that $x \in S$. Then we are in exactly one of three cases:

a) $x = y$; then $s(x) = s(y) = y + 1$, so (ii) holds with $z = 1$;

b) $x = y + z$ for some $z \in \mathbb{N}$; then $s(x) = s(y + z) = y + s(z)$, so again (ii) is true.

c) $y = x + z$ for some nonzero $z \in \mathbb{N}$. If $z = 1$, then $y = s(x)$, and (i) holds. If $z \neq 1$, then $z = s(v)$ for some nonzero $v \in \mathbb{N}$, hence

$$y = x + z = x + s(v) = s(x) + v,$$

where we have used Lemma 1.2, so (iii) holds.

Thus if $x \in S$, then $s(x) \in S$, hence $S = \mathbb{N}$ by induction, and we are done. □

Finally, a simple but useful observation:

Lemma 1.10. *If* $m, n \in \mathbb{N}$ *satisfy* $m + n = 0$*, then* $m = n = 0$*.*

Proof. If $n = 0$, the claim is clear. If $n \neq 0$, then $n = s(x)$ for some $x \in \mathbb{N}$ by Prop. 1.1; this implies $0 = m + n = m + s(x) = s(m + n)$, contradicting the axiom N3. □

1.3 Multiplication

We are now going to define how to multiply natural numbers. For the definition of $x \cdot z$ we use induction. First we put

$$x \cdot 0 = 0 \tag{1.5}$$

Now assume that we have defined $x \cdot y$; then we put

$$x \cdot s(y) = x \cdot y + x \tag{1.6}$$

(in other words: we put $x \cdot (y+1) := x \cdot y + x$). It should be obvious by now that the induction principle guarantees that xy is defined for any $x, y \in \mathbb{N}$. In general, we omit the multiplication sign $\cdot$ and write xy instead of $x \cdot y$. We shall also write $xy + z$ instead of $(xy) + z$ and agree that we always evaluate expressions by multiplying first and then adding the products.

Next we prove the basic properties of multiplication:

Lemma 1.11. *We have $x \cdot 1 = x$ for all $x \in \mathbb{N}$.*

Proof. $x \cdot 1 = x \cdot s(0) = x \cdot 0 + x = 0 + x = x$. □

Proposition 1.12 (Left Distributive Law)**.** *For all $x, y, z \in \mathbb{N}$ we have $x(y + z) = xy + xz$.*

Proof. Take $x, y \in \mathbb{N}$ and do induction on z. We find

$$\begin{array}{rcll} x(y+1) & = & x \cdot s(y) & \text{by (1.1)} \\ & = & xy + x & \text{by (1.6)} \\ & = & xy + x \cdot 1 & \text{by (1.5).} \end{array}$$

Next we assume that the left distributive law holds for z and prove that it also holds for $s(z)$:

$$\begin{array}{rcll} x(y+s(z)) & = & x \cdot (s(y+z)) & \text{by (1.2)} \\ & = & x(y+z) + x & \text{by (1.6)} \\ & = & (xy + xz) + x & \text{by assumption} \\ & = & xy + (xz + x) & \text{by Prop. 1.2} \\ & = & xy + x \cdot s(z) & \text{by (1.6)} \end{array}$$

This proves the claim by induction. □

Where there's a left distributive law, there's a right distributive law as well:

Proposition 1.13 (Right Distributive Law)**.** *We have $(x + y)z = xz + yz$ for all $x, y, z \in \mathbb{N}$.*

This proof is left as an exercise. Note that right distributivity would follow immediately from left distributivity if we already knew that multiplication was commutative. Fact is, however: we don't. But it comes right next: we start out with commutativity for multiplication by 0:

Lemma 1.14. *For all $x \in \mathbb{N}$, we have $0 \cdot x = 0$.*

Proof. Let $S = \{x \in \mathbb{N} : 0 \cdot x = 0\}$; then $0 \in S$ since $0 \cdot 0 = 0$ by (1.5). Assume now that $x \in S$; then

$$\begin{aligned} 0 \cdot s(x) &= 0 \cdot x + 0 && \text{by (1.6)} \\ &= 0 + 0 && \text{since } x \in S \\ &= 0 && \text{by (1.1)}, \end{aligned}$$

hence $s(x) \in S$ and therefore $S = \mathbb{N}$ by induction. □

and then do induction:

Proposition 1.15 (Commutativity of Multiplication)**.** *For all $x, y \in \mathbb{N}$, we have $xy = yx$.*

Yet another exercise:

Proposition 1.16 (Associativity of Multiplication)**.** *For $x, y, z \in \mathbb{N}$, we have $x(yz) = (xy)z$.*

And another one:

Proposition 1.17 (Cancellation Law of Multiplication)**.** *If $xz = yz$ for x, y, $z \in \mathbb{N}$ with $z \neq 0$, then $x = y$.*

Now that we know how to multiply, we can go forth and define exponentiation a^n for $a, n \in \mathbb{N}$ with $a \neq 0$: we put $a^0 = 1$, and if a^n is already defined, then $a^{s(n)} = a^n \cdot a$. Armed with this definition, we can now prove

1. a^n is defined for all $a, n \in \mathbb{N}$,

2. $a^{m+n} = a^m a^n$ for $a, m, n \in \mathbb{N}$,

3. $a^{mn} = (a^m)^n$ for $a, m, n \in \mathbb{N}$,

4. $a^n b^n = (ab)^n$ for $a, b, n \in \mathbb{N}$.

There is one last set of properties of the naturals that we have not yet touched upon: those based on the relation $<$.

1.4 $\mathbb{N}$ as a well-ordered set

We start by defining the relevant concept. For $x, y \in \mathbb{N}$ we say that

$$x \leq y \quad \text{if there is an } n \in \mathbb{N} \text{ such that } x + n = y. \tag{1.7}$$

Remark. If we had used the convention $\mathbb{N} = \{1, 2, 3, \ldots\}$, it would have been natural to start by defining $x < y$ to be equivalent with $x + n = y$ for some $n \in \mathbb{N}$. Since $0 \in \mathbb{N}$ in our approach, we prefer to use $\leq$ as the fundamental relation.

Proposition 1.18. *The relation $\leq$ on $\mathbb{N}$ has the following properties:*

1. *If $x \leq y$ and $y \leq x$ then $x = y$;*
2. *For all $x, y \in \mathbb{N}$, we have $x \leq y$ or $y \leq x$;*
3. *If $x \leq y$ and $y \leq z$, then $x \leq z$.*

Proof. Assume that $x \leq y$ and $y \leq x$; then there exist $m, n \in \mathbb{N}$ such that $x + m = y$ and $y + n = x$. This implies $x + m + n = x$, hence $m + n = 0$ by the cancellation law. Now Lemma 1.2 gives us $m = n = 0$, hence $x = y$ as claimed.

Next let $x, y \in \mathbb{N}$. By the trichotomy law, we have $x = y$, $x = y + z$ or $x + z = y$ for some (nonzero) $z \in \mathbb{N}$. By (1.7), this implies $x \leq y$, $x \leq y$ and $y \leq x$, respectively.

Now assume that $x \leq y$ and $y \leq z$. Then there exist $m, n \in \mathbb{N}$ such that $x + m = y$ and $y + n = z$. This gives $x + (m + n) = (x + m) + n = y + n = z$, that is, $x \leq z$. □

We now define some more relations from (1.7):

1. $x \geq y$ if $y \leq x$;
2. $x < y$ if $x \leq y$ and $x \neq y$;
3. $x > y$ if $y < x$.

We say that a set R is simply ordered if we have a relation $<$ such that the following conditions are satisfied for all $x, y, z \in R$:

O1 Trichotomy: We either have $x < y$ or $x = y$ or $x > y$.

O2 Transitivity: if $x < y$ and $y < z$ then $x < z$.

The proofs of the following claim is now straight forward:

Proposition 1.19. *The set $\mathbb{N}$ of natural numbers is simply ordered.*

Proof. By definition of $<$, we can't have $x < y$ and $x = y$ simultaneously, and the same is true for $y < x$ and $y = x$. Finally, if we had $x < y$ and $y < x$, then $x \leq y$ and $y \leq x$, hence $x = y$, which again contradicts e.g. $x < y$. Thus at most one of the assertions $x < y$, $x = y$ or $x > y$ is true.

Now we know that $x \leq y$ or $y \leq x$ is true; in the first case, $x < y$ or $x = y$, in the second case $y > x$ or $y = x$. This proves that at least on of the assertions $x < y$, $x = y$ or $x > y$ holds.

Now assume that $x < y$ and $y < z$. Then $x \leq y$ and $y \leq z$, hence $x \leq z$. If we had $x = z$, then $y \leq z = x$ and $x \leq y$ imply $x = y$ contradicting $x < y$. This proves O2. □

Observe that we have actually proved that any set with a relation $\leq$ satisfying 1.4.1, 2, 3 is simply ordered.

Proposition 1.20. *For $x, y, z \in \mathbb{N}$, $<$ and $\leq$ have the following properties:*

1. *If $x < y$, then $x + z < y + z$ for $z \in \mathbb{N}$ and conversely.*

2. *If $x \leq y$ then $xz \leq yz$ for $z \in \mathbb{N}$.*

3. *If $x < y$ and $z \neq 0$, then $xz < yz$.*

Proof. Exercise. □

For a subset $S \in \mathbb{N}$, we say that S has a smallest element if there is an $s \in S$ such that $s \leq t$ for all $t \in S$. The following result is basic (we say that $\mathbb{N}$ is well-ordered):

Theorem 1.21. *Every nonempty subset $S \in \mathbb{N}$ has a smallest element.*

Proof. Let $S \subseteq \mathbb{N}$ be non-empty, and define

$$R = \{x \in \mathbb{N} : x \leq y \text{ for all } y \in S\}.$$

Then $0 \in R$ since $0 \leq y$ for all $y \in \mathbb{N}$, in particular for all $y \in S$.

Since S is non-empty, there is a $y \in S$; this implies $y + 1 \notin R$: otherwise we would have $y + 1 \leq y$, which does not hold (we have $y \leq y + 1$ by (1.7), so $y + 1 \leq y$ would imply $y + 1 = y$, hence $1 = 0$ and $s(0) = 0$ in contradiction with N3).

Thus R contains 0 but $R \neq \mathbb{N}$; the induction axiom then implies that there must exist an $x \in R$ such that $x + 1 = s(x) \notin R$. We claim that x is a smallest element of S.

First, $x \in R$ implies $x \leq y$ for all $y \in S$, so we only need to show that $x \in S$. Assume $x \notin S$; then $x \leq y$ for all $y \in S$ implies $x < y$ (because we can't have equality), hence $x + 1 = s(x) \leq y$ for all $y \in S$, which by definition of R shows that $x + 1 \in R$ in contradiction to the construction of x. □

Let us also prove a simple result that will evolve into the Archimedean property of the reals:

Proposition 1.22. *If $0 < x < y$ are natural numbers, then there exists an $n \in \mathbb{N}$ such that $nx > y$.*

Proof. Put $n = y + 1$. □

1.5 Elementary Number Theory

In this section we will develop the number theory known to Euclid. First we will show that there is a 'Euclidean algorithm' on $\mathbb{N}$:

Proposition 1.23. *For every $a, b \in \mathbb{N}$ with $b \neq 0$, there exist unique numbers $q, r \in \mathbb{N}$ with $a = bq + r$ and $0 \leq r < b$.*

Proof. Let us prove uniqueness first. Assume $a = bq + r = bq' + r'$ with $0 \le r, r' < b$, and assume that $r < r'$. Then $q > q'$, and we have $r + t = r'$ and $q = q' + u$ for some $t, u \ge 1$. This gives $bq' + bu + r = bq' + r + t$, and the cancellation law gives $t = bu \ge b$ and $r' = r + t \ge b$: contradiction.

The existence of q and r is proved by induction on a. If $a = 0$, then $q = r = 0$ do it. Assume that $a = bq + r$ with $0 \le r < b$. Then If $r < b - 1$, then $a + 1 = bq + (r + 1)$, and if $r = b - 1$, then $a + 1 = b(q + 1) + 0$. This concludes the proof. □

Let a, b be natural numbers. We say that b divides a (and write $b \mid a$) if there is a $c \in \mathbb{N}$ such that $a = bc$. A natural number $p > 1$ is called irreducible if $p = ab$ for $a, b \in \mathbb{N}$ implies $a = 1$ or $b = 1$, that is, if p has only trivial factorizations. We say that p is prime if it has the following property: whenever $p \mid ab$ for $a, b \in \mathbb{N}$, we have $p \mid a$ or $p \mid b$.

Proposition 1.24. *Primes are irreducible.*

Proposition 1.25. *Irreducibles are prime.*

Theorem 1.26 (Unique Factorization Theorem)**.**

Proof. Induction. □

Proposition 1.27. *Assume that $a, b \in \mathbb{N}$ satisfy $\gcd(a, b) = 1$. If $ab = x^2$ for some $x \in \mathbb{N}$, then $a = r^2$ and $b = s^2$.*

1.6 Historical Remarks

Natural numbers 1, 2, 3, ... have always been regarded as 'numbers', with the exception of Greek mathematicians like Euclid, for whom 1 was the unit and a number was a proper multiple of 1. In particular, 1 wasn't a prime number for Euclid because it wasn't a number.

The history of 0 is not as simple. The Egyptians had a number system with base 10, but it was not positional: they had different symbols for 1, 10, 100, 1000 and so on, and for writing e.g. 35 the wrote down three sumbols for 10 and 5 for 1. The Babylonians, on the other hand, developed a positional system with base 60: they had only one symbol for 1, 60, 3600, ..., and its value was determined by its place. The only problem was that they did not have a 0, so strictly speaking they could not distinguish notationally between 2 and 120. Later, several writers developed various symbols to denote an empty position, but this was never used at the end of a number.

Our decimal system was 'invented' by the Hindus, who also came up with the 0. At first, 0 was only regarded as a symbol, not a number, but eventually Indian mathematicians worked out rules for adding, subtracting, multiplying, and even dividing by 0.

The Hindu numerals made it into the Arabic countries around the 8th century, and when they were introduced to Europe (and popularized e.g. by Fibonacci) they became known as Arabic numerals. The Arabic word for 0, siphr, was the origin for both 'cipher' and 'zero'.

Although geometry had been axiomatized by Euclid, the idea of writing down axioms characterizing natural numbers was perceived first by Dedekind and Peano. Along with the axiomatization of geometries by Hilbert and the emergence of the concept of abstract structures (groups, rings and fields), the desire to axiomatize the whole of mathematics emerged. The original hope that mathematics could be reduced to a finite set of axioms was dealt a deadly blow by Gödel, who proved that such an axiom system could not be complete in the sense that there must exist statements that can neither be proved nor disproved within such an axiom system.

Exercises

1.1 Consider the set $N = \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\}$ with successor function $s(n) = n+1$. Show that this system satisfies all Peano axioms except one – which one?

1.2 Consider the set $N = \{0\}$ with successor function $s : 0 \longmapsto 1$. Show that this system satisfies all Peano axioms except one – which one?

1.3 Consider the set $N = \{0\}$ with successor function $s : N \longrightarrow N : 0 \longmapsto 0$. Show that this system satisfies all Peano axioms except one – which one?

1.4 Consider the set $N = \{0, 1\}$ with successor function $s : N \longrightarrow N$ mapping $0 \longmapsto 1$ and $1 \longmapsto 0$. Show that this system satisfies all Peano axioms except one – which one?

1.5 Consider the set $N = \mathbb{N} \cup (\mathbb{N} + \omega)$, where ω is a symbol, $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{N} + \omega = \{0 + \omega, 1 + \omega, \ldots\}$. Define a successor function $s : N \longrightarrow N$ by mapping $n \longmapsto n + 1$ and $n + \omega \longmapsto (n + 1) + \omega$ for all $n \in \mathbb{N}$. Show that this system satisfies all Peano axioms except one – which one?

1.6 An axiom system is called independent if no axiom can be deduced from the others. Why do the exercises above show that the Peano axioms are independent?

1.7 Which Peano axioms are satisfied by the ring $\mathbb{Z}$ of integers and successor function $z \longmapsto z + 1$?

1.8 Prove the Cancellation Law (Prop. 1.2) for addition of natural numbers. (Hint: induction on z.)

1.9 For integers $x_1, \ldots, x_n, \ldots \in \mathbb{N}$ define $\sum_{k=1}^{n} x_k$ inductively by

$$\sum_{k=1}^{1} x_k = x_1 \tag{1.8}$$

and

$$\sum_{k=1}^{s(n)} = \Big(\sum_{k=1}^{n} x_k\Big) + x_{n+1}. \tag{1.9}$$

Prove that

$$\begin{aligned}
\sum_{k=n+1}^{n+m} x_k &= \sum_{k=1}^{m} x_{n+k} \\
\sum_{k=1}^{n} x_k + \sum_{k=1}^{m} x_{n+k} &= \sum_{k=1}^{n+m} x_k \\
\sum_{k=1}^{n} x_k + \sum_{k=1}^{n} y_k &= \sum_{k=1}^{n} (x_k + y_k).
\end{aligned}$$

1.10 Prove the following generalization of associativity: the sum $\sum_{k=1}^n x_k$ is by definition equal to $((((x_1 + x_2) + x_3) + x_4) + \ldots) + x_n$; prove that this sum does not depend on how we place the brackets. A concise formulation of this property is the following: if $x_1, \ldots, x_n$ is a finite set of natural numbers, and if $y_1, \ldots, y_n$ is a permutation of the x_k, then $\sum_{k=1}^n x_k = \sum_{k=1}^n y_k$.

1.11 Prove Proposition 1.4

1.12 Prove that the order relation on $\mathbb{N}$ has the following properties:

1. $x \geq 0$ for all $x \in \mathbb{N}$;
2. $x < s(y)$ if and only if $x \leq y$, where $x, y \in \mathbb{N}$;
3. $s(y) \leq x$ if and only if $y < x$, where $x, y \in \mathbb{N}$;

1.13 Prove that $a\Big(\sum_{k=1}^n x_n\Big) = \sum_{k=1}^n (ax_n)$ for $a, x_1, \ldots, x_n \in \mathbb{N}$.

1.14 Define $\prod_{k=1}^n x_k$ for $x_1, \ldots, x_k \in \mathbb{N}$.

1.15 Prove that $\prod_{k=1}^m x_k \prod_{k=m+1}^n x_k = \prod_{k=1}^n x_k$.

1.16 Prove that $\prod_{k=1}^n x_k \prod_{k=1}^n y_k = \prod_{k=1}^n (x_k y_k)$.

1.17 Consider the set $\{1, 2, 3\}$ with the relation $<$ defined by $E = \{(1, 2), (2, 3), (3, 1)\}$ (this means that $1 < 2$, $2 < 3$ and $3 < 1$, but not $2 < 1$ or $1 < 3$. Show that O1 holds, but O2 does not.

1.18 Consider the set $\{1\}$ with the relation $<$ defined by $E = (1, 1)$ (this means that we have $1 < 1$. Show that O2 holds, but O1 does not.