Reflective thinking turns experience into insight.
John Maxwell

1 Numbers

In 1879, Gottlob Frege completed the first step of his program to put mathematics on a solid foundation. His idea was that **logic** should be the foundation of all mathematics, and, following Gottfried von Leibniz (1646–1716) and George Boole (1815–1864), he created a rigorous symbolic language, which he called *Begriffsschrift*, to incorporate all standard principles of logic.

Georg Cantor followed in his footsteps and developed **set theory** from basic logical principles. In 1888, Richard Dedekind took the next step, and presented a **construction of the real numbers** based on set theory.

It should be mentioned that Frege's program was doomed to fail. Frege's construction allowed objects such as "the set of all sets". Bertrand Russell used this to construct a paradox: Let E denote the set of all sets which do not contain themselves as members. Is E an element of E? It can't be, because E contains only sets which are **not** members of themselves. Can E fail to be an element of E? No, since if $E \notin E$, then by the definition of the set E, E is contained in E.

Bertrand Russell's and Alfred Whitehead's attempts to "fix" these problems in their monumental *Principia Mathematica* are generally regarded as artificial and therefore in violation of the spirit of Frege's program.

In response, David Hilbert came up with an alternative program: Use axiomatic systems as the foundation of mathematics together with *meta-mathematics*. Mathematicians "do" mathematics starting from axiomatic systems; meta-mathematics allows to talk about the process "from the outside" addressing issues such as completeness[1] and consistency[2] of a given axiomatic system.

In 1930, Kurt Gödel showed that this approach was equally flawed: It is not possible to show (within the axiomatic system) that an axiomatic system which incorporates the arithmetic of natural numbers is commplete (or consistent).

[1] An axiomatic system is complete, if all statements within the axiomatic system can—in principle—be shown to be true or to be false.

[2] An axiomatic system is said to be consistent, if the axioms can be shown not to lead to contradictions.

1.1 The Natural Numbers

Definition. Richard Dedekind started by giving the following definition of the set of **Natural Numbers**[3]:

> *The natural numbers are a set* $\mathbb{N}$ *together with a special element called* 0*, and a function* $S : \mathbb{N} \to \mathbb{N}$ *satisfying the following axioms:*
>
> **(D1)** *S is injective*[4]*.*
>
> **(D2)** $0 \notin S(\mathbb{N})$.[5]
>
> **(D3)** *If a subset M of $\mathbb{N}$ contains 0 and satisfies $S(M) \subseteq M$, then $M = \mathbb{N}$.*

The function S is called the successor function.

The first two axioms describe the process of counting, the third axiom assures the **Principle of Induction**:

Exercise 1.1
Let $P(n)$ be a predicate with the set of natural numbers as its domain. If

1. $P(0)$ is true, and
2. $P(S(n))$ is true, whenever $P(n)$ is true,

then $P(n)$ holds for all natural numbers.

---

[3] A similar definition of the natural numbers was introduced by Guiseppe Peano in 1889:

> *The natural numbers are a set* $\mathbb{N}$ *together with a special element called* 0*, and a function* $S : \mathbb{N} \to \mathbb{N}$ *satisfying the following axioms:*
>
> **(P1)** $0 \in \mathbb{N}$.
>
> **(P2)** *If $n \in \mathbb{N}$, then $S(n) \in \mathbb{N}$.*
>
> **(P3)** *If $n \in \mathbb{N}$, then $S(n) \neq 0$.*
>
> **(P4)** *If a set A contains 0, and if A contains $S(n)$, whenever it contains n, then the set A contains $\mathbb{N}$.*
>
> **(P5)** *$S(m) = S(n)$ implies $m = n$ for all $m, n \in \mathbb{N}$.*

[4] A function $f : A \to B$ is called *injective* if for all $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
[5] For a function $f : A \to B$, $f(A) := \{b \in B \mid f(a) = b \text{ for some } a \in A\}$.

Existence and Uniqueness. Do natural numbers exist? Following Dedekind, we will say that a set M is **infinite**, if there is an injective map $f : M \to M$ that is not surjective[6].

According to Dedekind's definition, the set of natural numbers is infinite (why?). In fact, one can show that the converse also holds: If there is an infinite set, then there are natural numbers.

In order not to get stuck in a finite universe, we will from now on additionally assume that the following axiom holds:

(D4) *There is a set which satisfies Axioms (D1)–(D3).*

Before we give a proof of the "essential" uniqueness of the natural numbers, we will follow Dedekind and establish the following general **Recursion Principle**:

Task 1.2
Let A be an arbitrary set, and let $a \in A$ and a function $f : A \to A$ be given. Then there exists a unique map $\varphi : \mathbb{N} \to A$ satisfying

1. $\varphi(0) = a$, and
2. $\varphi \circ S = f \circ \varphi$.

The setup of the proof is somewhat tricky: Consider all subsets $K \subseteq \mathbb{N} \times A$ with the following properties:

1. $(0, a) \in K$, and
2. If $(n, b) \in K$, then $(S(n), f(b)) \in K$.

Clearly $\mathbb{N} \times A$ itself has these properties; we can therefore define the smallest such set: Let

$$L = \bigcap \{K \subseteq \mathbb{N} \times A \mid K \text{ satisfies (1) and (2)}\}.$$

[6] A function $f : A \to B$ is called *surjective*, if $f(A) \neq B$.

Now show by induction that for every $n \in \mathbb{N}$ there is a unique $b \in A$ with $(n, b) \in L$. This property defines φ by setting $\varphi(n) = b$ for all $n \in \mathbb{N}$.

The Recursion Principles makes it possible to define a recursive procedure (the function φ) via a formula (the function f).

The set of natural numbers is unique in the following sense:

Task 1.3
Suppose that $\mathbb{N}$, $S : \mathbb{N} \to \mathbb{N}$ and 0 satisfy Axioms (D1)–(D3), and that $\mathbb{N}'$, $S' : \mathbb{N}' \to \mathbb{N}'$ and $0'$ satisfy Axioms (D1)–(D3) as well.

Then there is a bijection[7] $\varphi : \mathbb{N} \to \mathbb{N}'$ such that

1. $\varphi(0) = 0'$, and
2. $\varphi \circ S = S' \circ \varphi$.

Arithmetic Properties. **Addition** of natural numbers is established recursively in the following way: For a fixed but arbitrary $m \in \mathbb{N}$ we define

$$\begin{aligned} m + 0 &:= m \\ m + S(n) &:= S(m + n) \text{ for all } n \in \mathbb{N} \end{aligned}$$

Task 1.4
Use the Recursion Principle to make this procedure precise.

Note that we now know in particular that for all natural numbers $S(m) = m + 1$ (here $S(0) := 1$.)

Use induction for the following:

[7] A function $f : A \to B$ is a *bijection*, if it is both injective and surjective.

Exercise 1.5
Show that addition on $\mathbb{N}$ is associative.

Exercise 1.6
Show that addition on $\mathbb{N}$ is commutative.

This last exercise implies in particular that 0 is the (unique) neutral element with respect to addition: $n + 0 = 0 + n$ holds for all $n \in \mathbb{N}$.

Multiplication of natural numbers is also defined recursively as follows: For $m, n \in \mathbb{N}$ we define

$$\begin{aligned} m \cdot 0 &:= 0 \\ m \cdot (n+1) &:= m \cdot n + m \end{aligned}$$

Exercise 1.7
Show that the following distributive law holds for natural numbers:

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

Exercise 1.8

1. Show that multiplication on $\mathbb{N}$ is commutative.
2. Show that multiplication on $\mathbb{N}$ is associative.
3. Show that 1 is the neutral element with respect to multiplication.

Exercise 1.9
Show that multiplication is zero-divisor free:

$$m \cdot n = 0 \text{ implies } m = 0 \text{ or } n = 0.$$

Finally we can impose a **total order**[8] on $\mathbb{N}$ as follows: We say that $m \leq n$, if there is a natural number k, such that $m + k = n$.

Task 1.10
Show that "$\leq$" is indeed a total order:

1. "$\leq$" is reflexive[9].
2. "$\leq$" is anti-symmetric[10].
3. "$\leq$" is transitive[11].
4. For all $m, n \in \mathbb{N}$, $m \leq n$ or $n \leq m$.

Task 1.11
Show the following compatibility laws:

1. If $m \leq n$, then $m + k \leq n + k$ for all $k \in \mathbb{N}$.
2. If $m \leq n$, then $m \cdot k \leq n \cdot k$ for all $k \in \mathbb{N}$.

[8] A relation $\sim$ on A is called a *total order*, if $\sim$ is reflexive, anti-symmetric, transitive, and has the property that for all $a, b \in A$, $a \sim b$ or $b \sim a$ holds.

[9] A relation $\sim$ on A is *reflexive* if for all $a \in A$, $a \sim a$.

[10] A relation $\sim$ on A is *anti-symmetric* if for all $a, b \in A$ the following holds: $a \sim b$ and $b \sim a$ implies that a=b.

[11] A relation $\sim$ on A is *transitive* if for all $a, b, c \in A$ the following holds: $a \sim b$ and $b \sim c$ implies that $a \sim c$.

1.2 The Integers

Definition. Integers can be written as differences of natural numbers. The set of integers $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ will therefore be defined as certain equivalence classes of the two-fold Cartesian product of $\mathbb{N}$.

We define a relation on $\mathbb{N} \times \mathbb{N}$ as follows:

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

Exercise 1.12
Show that "$\sim$" defines an equivalence relation on $\mathbb{N} \times \mathbb{N}$:

1. "$\sim$" is reflexive.
2. "$\sim$" is symmetric[12].
3. "$\sim$" is transitive.

We will denote equivalence classes as follows:

$$(a, b)_\sim := \{(c, d) \mid (c, d) \sim (a, b)\}.$$

The set of integers $\mathbb{Z}$ is the set of all equivalence classes thus obtained:

$$\mathbb{Z} = \{(a, b)_\sim \mid a, b \in \mathbb{N}\}.$$

Arithmetic Properties. **Addition** of integers will be defined component-wise:

$$(a, b)_\sim + (c, d)_\sim = (a + c, b + d)_\sim.$$

The next two exercises will show that $\mathbb{Z}$ is an *Abelian group*[13] with respect to addition.

[12] A relation $\sim$ on A is called *symmetric*, if for all $a, b \in A$ the following holds: $a \sim b$ implies $b \sim a$.

[13] A set G with a binary operation $\star$ is called an *Abelian group* if $\star$ is commutative and associative, if $(A, \star)$ has a neutral element n satisfying $g \star n = g$ for all $g \in G$, and if $(A, \star)$ has inverse elements, i.e., for all $g \in G$ there is an $h \in G$ satisfying $g \star h = n$.

Exercise 1.13

1. Show that the addition of integers is well-defined (i.e. independent of the chosen representatives of the equivalence classes).
2. Show that the addition of integers is commutative.
3. Show that the addition of integers is associative.

Exercise 1.14

1. Show that the addition of integers has $(0,0)_\sim$ as its neutral element.
2. Show that for all $a, b \in \mathbb{N}$ the following holds: $(a,b)_\sim + (b,a)_\sim = (0,0)_\sim$. Thus every element in $\mathbb{Z}$ has an inverse element.

Exercise 1.15

1. The map $\phi : \mathbb{N} \to \mathbb{Z}$ defined by $\phi(n) = (n,0)_\sim$ is injective.
2. For all $m, n \in \mathbb{N}$ the following holds: $\phi(m) + \phi(n) = \phi(m+n)$.

From now on we will identify $\mathbb{N}$ with $\phi(\mathbb{N})$ and write $a - b$ instead of $(a,b)_\sim$. For instance -5 is the equivalence class of all elements equivalent to $(0,5)$.

Task 1.16

Define integer multiplication (make sure it is well-defined), and show that multiplication is commutative, associative, and has 1 as its neutral element.

Last not least we will define a **total order** on $\mathbb{Z}$ as follows:

$$m \leq n \text{ if and only if } n - m \in \mathbb{N}.$$

Exercise 1.17

1. Show that "$\leq$" defines a total order on $\mathbb{Z}$.
2. If $m \leq n$, then $m + k \leq n + k$ for all $k \in \mathbb{Z}$.
3. If $m \leq n$ and $0 \leq k$, then $m \cdot k \leq n \cdot k$.