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:

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

The next three exercises show that "$\sim$" defines an equivalence relation on $\mathbb{N} \times \mathbb{N}$:

Exercise 1.22

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

Task 1.23

"$\sim$" 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 obtained in this manner:

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

Addition of integers will be defined component-wise:

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

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

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 $g \star h = n$.

The next five exercises will show that $\mathbb{Z}$ is an Abelian group with respect to addition.

Exercise 1.24
Show that the addition of integers is well-defined (i.e. independent of the chosen representatives of the equivalence classes).

Exercise 1.25
Show that the addition of integers is commutative.

Exercise 1.26
Show that the addition of integers is associative.

Exercise 1.27
Show that the addition of integers has $(0,0)_\sim$ as its neutral element.

Exercise 1.28
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 additive inverse element.

Task 1.29

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 $\phi(\mathbb{N})$.

Task 1.30

1. Define integer multiplication and show that the multiplication is well-defined.
2. Show that $1 = (1, 0)_\sim$ is the neutral element with respect to multiplication.

It is not hard to show that multiplication is commutative and associative. Moreover the distributive law holds in $\mathbb{Z}$.

Exercise 1.31

With ϕ as defined in Task 1.29, show that

$$\phi(m) \cdot \phi(n) = \phi(m \cdot n).$$

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

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

Exercise 1.32
Let $a, b, c, d \in \mathbb{N}$. Then $(a,b)_\sim \leq (c,d)_\sim$ if and only if there is a $k \in \mathbb{N}$ such that

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

The next two exercises show that "$\leq$" is a **total order** on $\mathbb{Z}$:

Exercise 1.33
Show that "$\leq$" is reflexive, anti-symmetric and transitive on $\mathbb{Z}$.

Exercise 1.34
$m \leq n$ or $n \leq m$ for all $m, n \in \mathbb{Z}$.

Exercise 1.35
If $m \leq n$, then $m + k \leq n + k$ for all $k \in \mathbb{Z}$.

Exercise 1.36
If $m \leq n$ and $0 \leq k$, then $m \cdot k \leq n \cdot k$.

1.3 The Rational Numbers

Once again we define the next larger set as certain equivalence classes. On $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$, we define a relation $\cong$ as follows:

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

We write equivalence classes in the familiar way

$$\frac{a}{b} = \{(c, d) \mid (c, d) \cong (a, b)\},$$

and denote the rational numbers by

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus \{0\} \right\}.$$

For integers n we write n instead of $\frac{n}{1}$.

We define an order on $\mathbb{Q}$ as follows:

$$0 \le \frac{a}{b} \text{ if and only if } (0 \le a \text{ and } 0 < b) \text{ or } (a \le 0 \text{ and } b < 0).$$

For $p, q \in \mathbb{Q}$, we write $p \le q$ if $0 \le q - p$.

With the natural addition and multiplication

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

and the order above, the set of rational numbers becomes an **ordered field**:

Theorem. $(\mathbb{Q}, +, \cdot, \le)$ has the following properties:

1. $(\mathbb{Q}, +)$ is an Abelian group with neutral element 0.
2. $(\mathbb{Q} \setminus \{0\}, \cdot)$ is an Abelian group with neutral element 1.
3. $(a + b) \cdot c = a \cdot c + b \cdot c$.
4. $(\mathbb{Q}, \le)$ is a total order.
5. (a) $a \le b$ implies $a + c \le b + c$ for all $a, b, c \in \mathbb{Q}$.
   (b) $a \le b$ implies $a \cdot c \le b \cdot c$ for all $a, b, c \in \mathbb{Q}$ with $0 \le c$.

Exercise 1.37
Let $a, b \in \mathbb{Q}$, and assume $a > b$ and $b > 0$. Then $a^2 > b^2$.

The rational numbers have two more interesting properties. Let us write $a < b$ if $a \leq b$ and $a \neq b$. We will say that a is *positive*, if $0 < a$. Similarly, a is called *negative*, if $0 < -a$.

Exercise 1.38
$\mathbb{Q}$ is *dense in itself*: For all $a, b \in \mathbb{Q}$ with $a < b$ there is a $c \in \mathbb{Q}$ with $a < c < b$.

Exercise 1.39
$\mathbb{Q}$ is *Archimedean*: For all positive $a, b \in \mathbb{Q}$, there is a natural number n such that $b < n \cdot a$.