

## 1.2 The Integers

**Definition.** Integers can be written as differences of natural numbers. The set of integers  $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$  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 1.21

1. “ $\sim$ ” is reflexive.
2. “ $\sim$ ” is symmetric<sup>12</sup>.

### Task 1.22

“ $\sim$ ” 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:

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

---

<sup>12</sup>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 1.23**

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

**Exercise 1.24**

Show that the addition of integers is commutative.

**Exercise 1.25**

Show that the addition of integers is associative.

**Exercise 1.26**

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

**Exercise 1.27**

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 1.28**

1. The map  $\phi : \mathbb{N} \rightarrow \mathbb{Z}$  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  $\phi(\mathbb{N})$ .

We will also write  $a - b$  instead of  $(a, b)_\sim$ . For instance  $-5$  is the equivalence class of all elements in  $\mathbb{N} \times \mathbb{N}$  equivalent to  $(0, 5)$ .

**Task 1.29**

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

**Task 1.30**

With  $\phi$  as defined in Task 1.28, show that

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

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 1.31**

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

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

**Task 1.32**

Show that “ $\leq$ ” defines a total order on  $\mathbb{Z}$ .

**Exercise 1.33**

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

**Exercise 1.34**

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:

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

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

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.**  $(\mathbb{Q}, +, \cdot, \leq)$  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.  $(\mathbb{Q}, \leq)$  is a total order.
5. (a)  $a \leq b$  implies  $a + c \leq b + c$  for all  $a, b, c \in \mathbb{Q}$ .  
 (b)  $a \leq b$  implies  $a \cdot c \leq b \cdot c$  for all  $a, b, c \in \mathbb{Q}$  with  $0 \leq c$ .

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 1.35

$\mathbb{Q}$  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 1.36

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

## 1.4 The Real Numbers

**Completeness.** While the rational numbers have nice algebraic properties with respect to their addition, their multiplication and their order, they have one crucial deficiency: They have “holes”.

For instance, the increasing sequence of rational numbers

$$1, 1.4, 1.41, 1.414, 1.4142, \dots$$

approaches the non-rational number  $\sqrt{2}$ , a fact well known since antiquity.

We want to remedy this deficiency: we want to construct an ordered field  $F$  containing the rational numbers, which is “complete” in the following sense:

(C1) Every increasing bounded sequence of elements in  $F$  converges to an element in  $F$ .<sup>13</sup>

Calculus books usually introduce completeness of the set of real numbers in this fashion.

It is convenient to describe completeness also in a slightly different way.

We say a **non-empty** set  $A \subseteq F$  is *bounded from above*, if there is a  $b \in F$  such that  $a \leq b$  for all  $a \in A$ . Such an element  $b$  is then called an upper bound for the set  $A$ .

If  $A \subseteq F$  is bounded from above, we say that  $A$  has a *least upper bound*, denoted by  $\sup(A) \in F$ , if

1.  $\sup(A)$  is an upper bound of  $A$ , and
2. for all upper bounds  $b$  of  $A$ , we have  $\sup(A) \leq b$ .

Note that  $\sup(A)$  must be in  $F$ , but we do not require that  $\sup(A)$  is an element of  $A$ .

---

<sup>13</sup>A *sequence* is a function  $\phi : \mathbb{N} \rightarrow F$ .

A sequence  $\phi : \mathbb{N} \rightarrow F$  is called *increasing*, if  $m \leq n$  implies  $\phi(m) \leq \phi(n)$ .

An increasing sequence  $\phi : \mathbb{N} \rightarrow F$  is called *bounded*, if there is a  $b \in F$  such that  $\phi(n) \leq b$  for all  $n \in \mathbb{N}$ .

We say that the increasing sequence  $\phi$  *converges* to  $a \in F$ , if for all  $\varepsilon > 0$  there is an  $N \in \mathbb{N}$  such that  $a - \varepsilon \leq \phi(n) \leq a$  for all  $n \geq N$ .

**Task 1.37**

Let  $A = \{a \in \mathbb{Q} \mid a^2 < 2\}$ . Show that  $A$  is bounded from above, but fails to have a least upper bound in  $\mathbb{Q}$ .

The *greatest lower bound* of a set is defined analogously:

We say a non-empty set  $A \subseteq F$  is *bounded from below*, if there is a  $b \in F$  such that  $b \leq a$  for all  $a \in A$ . Such an element  $b$  is then called a lower bound for the set  $A$ .

If  $A \subseteq F$  is bounded from below, we say that  $A$  has a *greatest lower bound*, denoted by  $\inf(A) \in F$ , if

1.  $\inf(A)$  is a lower bound of  $A$ , and
2. for all lower bounds  $b$  of  $A$ , we have  $b \leq \inf(A)$ .

**Task 1.38**

Show the following are equivalent:

1. All subsets of  $F$  that are bounded from above have a least upper bound.
2. All subsets of  $F$  that are bounded from below have a greatest lower bound.

Completeness can then be stated as follows:

- (C2) Every subset  $A$  of  $F$ , which is bounded from above, has a least upper bound.

**Task 1.39**

Show that property **(C2)** implies property **(C1)**.

**Task 1.40**

Show that property **(C1)** implies property **(C2)**.

**Constructions of the real numbers.** Historically, three “constructions” of the real numbers gained prominence in the 19th century, due to RICHARD DEDEKIND (Dedekind cuts), GEORG CANTOR (fundamental sequences), and PAUL BACHMANN (nested intervals), respectively. Another approach uses the concept of Cauchy sequences of rational numbers. We will present the first construction below.

**Dedekind Cuts.** Given two sets of rational numbers  $\emptyset \neq L, U \subseteq \mathbb{Q}$ , we say that  $(L, U)$  is a *partition* of  $\mathbb{Q}$  (into two sets), if  $L \cup U = \mathbb{Q}$  and  $L \cap U = \emptyset$ .

A partition  $(L, U)$  of  $\mathbb{Q}$  is called a *Dedekind cut*, if the following properties hold:

1. If  $a \in L$  and  $b \in U$ , then  $a < b$ .
2.  $L$  has no maximal element.

Here, the element  $x$  of a set  $A$  of rational numbers is called *maximal element* of  $A$ , if  $x \geq a$  for all  $a \in A$ .

$L$  and  $U$  are complementary sets:  $U = \mathbb{Q} \setminus L$ , and  $L = \mathbb{Q} \setminus U$ .

Here are two examples of Dedekind cuts:



**Exercise 1.41**

Show that

$$L = \{q \in \mathbb{Q} \mid q < -3\}, \quad U = \{q \in \mathbb{Q} \mid q \geq -3\}$$

defines a Dedekind cut.

The two sets above “meet” at the rational number  $-3$ .

**Exercise 1.42**

Show that

$$L = \{q \in \mathbb{Q} \mid q \leq 0 \text{ or } q^2 < 2\}, \quad U = \{q \in \mathbb{Q} \mid q > 0 \text{ and } q^2 > 2\}$$

defines a Dedekind cut.

Here the two sets of the Dedekind cut “meet” at the irrational number  $\sqrt{2}$ .

Dedekind then defined the set of real numbers to be the set of all Dedekind cuts:

$$\mathbb{R} = \{(L, U) \mid (L, U) \text{ is a Dedekind cut}\}.$$

Note that a rational number  $q \in \mathbb{Q}$  corresponds to the Dedekind cut, defined by  $L = (-\infty, q) \cap \mathbb{Q}$ ,  $U = [q, \infty) \cap \mathbb{Q}$ . We will denote this Dedekind cut by  $\underline{q}$ .

**Addition of Dedekind cuts.** Given two Dedekind cuts  $(L_1, U_1)$  and  $(L_2, U_2)$  we define their sum to be the Dedekind cut  $(X, Y)$ , where

$$X = \{x \in \mathbb{Q} \mid x = l_1 + l_2 \text{ for some } l_1 \in L_1 \text{ and } l_2 \in L_2\},$$

and

$$Y = \mathbb{Q} \setminus X.$$

**Exercise 1.43**

Show that  $(X, Y)$  is indeed a Dedekind cut.

**Exercise 1.44**

Let  $p, q \in \mathbb{Q}$ . Show:  $\underline{p} + \underline{q} = \underline{p + q}$ .

**Task 1.45**

Show that the Dedekind cuts with the addition defined above form an Abelian group (see p. 10). What is the neutral element? What is the additive inverse of a Dedekind cut?

Note that the previous task makes it, in particular, possible to define the difference of two Dedekind cuts.

Next, we can define an order on Dedekind cuts: We say that  $(L_1, U_1) \leq (L_2, U_2)$ , if  $L_1 \subseteq L_2$ . In particular,  $(L, U)$  is non-negative, if  $(-\infty, 0) \cap \mathbb{Q} \subseteq L$ . We say  $(L_1, U_1) < (L_2, U_2)$ , if  $(L_1, U_1) \leq (L_2, U_2)$  and  $(L_1, U_1) \neq (L_2, U_2)$ .

Clearly  $\leq$  is reflexive, anti-symmetric and transitive (why?). The order is also total:

**Exercise 1.46**

For any two Dedekind cuts  $(L_1, U_1)$  and  $(L_2, U_2)$ ,

$$(L_1, U_1) \leq (L_2, U_2) \text{ or } (L_2, U_2) \leq (L_1, U_1).$$

It is harder to define the multiplication of Dedekind cuts. If both  $(L_1, U_1)$  and  $(L_2, U_2)$  are non-negative, we define their product  $(X, Y)$  as

$$X = \mathbb{Q} \setminus Y,$$

where

$$Y = \{y \in \mathbb{Q} \mid y = u_1 \cdot u_2 \text{ for some } u_1 \in U_1 \text{ and } u_2 \in U_2\}.$$

**Exercise 1.47**

Check that the product defined above is indeed a Dedekind cut.

To define the product of arbitrary Dedekind cuts, we need the following result:

**Exercise 1.48**

Every Dedekind cut is the difference of two non-negative Dedekind cuts.

We then define the product of two arbitrary Dedekind cuts by “multiplying out”:

**Task 1.49**

Define the product of two arbitrary Dedekind cuts formally, and show that the concept is well-defined.

With these definitions one can show with quite a bit more work:

**Theorem.** The real numbers with the addition, multiplication and order defined above form an **ordered Archimedean field**.

The Dedekind cut  $\underline{1} := (\mathbb{Q} \cap (-\infty, 1), \mathbb{Q} \cap [1, \infty))$  is the neutral element with respect to multiplication. The existence of a multiplicative inverse is first shown for positive Dedekind cuts, and then generalized to negative Dedekind cuts.

**Completeness of Dedekind cuts.** Note that a Dedekind cut  $(L', U')$  is an upper bound for a set of Dedekind cuts  $\mathcal{D}$ , if  $L \subseteq L'$  for all  $(L, U) \in \mathcal{D}$ .

**Exercise 1.50**

Let

$$\mathcal{D} = \left\{ \left( \mathbb{Q} \cap \left(-\infty, -\frac{1}{n}\right), \mathbb{Q} \cap \left[-\frac{1}{n}, \infty\right) \right) \mid n \in \mathbb{N} \right\}.$$

Show that  $\mathcal{D}$  is bounded from above, then determine its least upper bound.

Finally we can show that the set of real numbers defined via Dedekind cuts is **complete**:

**Exercise 1.51**

Show that  $\mathbb{R}$ , the set of all Dedekind cuts, satisfies Axiom **(C2)**.

**Exercise 1.52**

Show that  $\mathbb{Q}$  is dense in  $\mathbb{R}$ : Given two Dedekind cuts  $(L_1, U_1) < (L_2, U_2)$ , there is a  $q \in \mathbb{Q}$  such that

$$(L_1, U_1) \leq \underline{q} \leq (L_2, U_2).$$