

# Contents

<b>Contents</b>	<b>i</b>
<b>1 Orderings and Functions</b>	<b>1</b>
1.1 Basic Notation . . . . .	1
1.2 Orderings . . . . .	1
1.3 Functions . . . . .	3
1.4 Cardinality . . . . .	6
<b>2 Ordered Fields</b>	<b>12</b>
2.1 Ordering of $\mathbb{Z}$ . . . . .	12
2.2 Ordering of $\mathbb{Q}$ . . . . .	12
2.3 Rings and Fields . . . . .	14
<b>3 The Real Numbers</b>	<b>16</b>
3.1 The Completion of $\mathbb{Q}$ . . . . .	16
3.2 Ordering of $\mathbb{R}$ . . . . .	16
3.3 Metrics and Norms on $\mathbb{R}^n$ . . . . .	19
<b>4 Supremum, Infimum, and Completeness</b>	<b>22</b>
4.1 Supremum and Infimum . . . . .	22
4.2 Nested Intervals . . . . .	25
<b>5 Sequences</b>	<b>27</b>
5.1 Basic Definitions and Examples . . . . .	27
5.2 Convergence . . . . .	28

# Orderings and Functions

## 1.1 Basic Notation

### Definition 1.1.1.

- (1) The natural numbers are defined as  $\mathbf{N} = \{1, 2, 3, \dots\}$ ,
- (2) The positive integers are defined as  $\mathbf{N}_0 = \mathbf{Z}^+ = \{0, 1, 2, 3, \dots\}$ ,
- (3) The integers are defined as  $\mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ ,
- (4) The rational numbers are defined as  $\mathbf{Q} = \{\frac{a}{b} \mid a, b \in \mathbf{Z}, b \neq 0\}$ ,
- (5) The real numbers are "defined" (we will get more into this later) as the set  $(-\infty, \infty)$ ,
- (6) The complex numbers are defined as  $\mathbf{C} = \{a + bi \mid a, b \in \mathbf{R}, i^2 = -1\}$ .

**Example 1.1.1.** Note that  $\sqrt{2}, \pi, e \notin \mathbf{Q}$ , as they cannot be expressed as fractions.

**Definition 1.1.2.** Let  $A$  and  $B$  be sets. The cartesian product is defined as  $A \times B = \{(a, b) \mid a \in A, b \in B\}$ .

**Definition 1.1.3.** A relation from  $A$  to  $B$  is a subset  $R \subseteq A \times B$ . Typically, when one says "a relation on  $A$ " that means a relation from  $A$  to  $A$ ; i.e.,  $R \subseteq A \times A$ .

**Definition 1.1.4.** Let  $A$  be a set and  $R$  a relation on  $A$ . Then  $R$  is:

- (1) reflexive if  $(a, a) \in R$  for all  $a \in A$ ,
- (2) transitive if  $(a, b), (b, c) \in R$  implies  $(a, c) \in R$ ,
- (3) symmetric if  $(a, b) \in R$  implies  $(b, a) \in R$ , and
- (4) antisymmetric if  $(a, b), (b, a) \in R$  implies  $a = b$ .

## 1.2 Orderings

**Definition 1.2.1.** Let  $A$  be a set. An ordering of  $A$  is a relation  $R$  on  $A$  that is reflexive, transitive, and antisymmetric. If this is the case, we write  $(a, b) \in R$  as  $a \leq_R b$ . If  $A$  is an ordered set we write it as the ordered pair  $(A, \leq_R)$  (or just  $A$  if the ordering is obvious by context).

**Example 1.2.1.**

- (1) Let  $m, n \in \mathbf{Z}$ . The algebraic ordering  $\leq_a$  is defined as follows:  $m \leq_a n$  if and only if there exists an element  $k \in \mathbf{N}_0$  with  $m + k = n$ .
- (2) The set of natural numbers  $\mathbf{N}$  equipped with the relation of divisibility form an ordering. Let  $m, n \in \mathbf{N}$ . Then  $m \leq_d n$  if and only if  $m \mid n$ .
- (3) Let  $S$  be any set. The subsets of  $S$  (i.e., elements of its power set) equipped with the relation of inclusion form an ordering. Let  $A, B \in \mathcal{P}(S)$ . Then  $A \leq_{\mathcal{P}(S)} B$  if and only if  $A \subseteq B$ .
- (4) The set of rational numbers  $\mathbf{Q}$  form an algebraic ordering as follows: if  $\frac{a}{b}, \frac{c}{d} \in \mathbf{Q}$ , then  $\frac{a}{b} \leq_a \frac{c}{d}$  if and only if  $ad \leq_a bc$  (in  $\mathbf{Z}$ ).

**Definition 1.2.2.** An ordered set  $(A, \leq_R)$  is total (or linear) if for all  $a, b \in A$  we have that  $a \leq_R b$  or  $b \leq_R a$ .

**Example 1.2.2.** The ordered sets  $(\mathbf{Z}, \leq_a)$  and  $(\mathbf{Q}, \leq_a)$  are total orderings, whereas  $(\mathbf{N}, \leq_d)$  and  $(\mathcal{P}(S), \leq_{\mathcal{P}(S)})$  are not total orderings.

**Definition 1.2.3.** Let  $(X, \leq)$  be an ordered set. Let  $A \subseteq X$ .

- (1)  $A$  is called bounded above if there exists an element  $u \in X$  with  $a \leq u$  for all  $a \in A$ . Such a  $u$  (not necessarily unique) is called an upperbound for  $A$ .
- (2)  $A$  is called bounded below if there exists an element  $v \in X$  with  $v \leq a$  for all  $a \in A$ . Such a  $v$  (not necessarily unique) is called a lowerbound for  $A$ .
- (3) If  $A$  admits an upperbound  $u$  with  $u \in A$ , then  $u$  is called the greatest element of  $A$ .
- (4) If  $A$  admits a lowerbound  $v$  with  $v \in A$ , then  $v$  is called the least element of  $A$ .
- (5) Let  $A$  be bounded above. The set of upperbounds of  $A$  is defined as  $\mathcal{U}_A = \{u \in X \mid u \text{ is an upperbound of } A\}$ . If  $l$  is the least element of  $\mathcal{U}_A$ , we write  $l = \sup(A)$  and call it the supremum of  $A$ .
- (6) Let  $A$  be bounded below. The set of lowerbounds of  $A$  is defined as  $\mathcal{L}_A = \{v \in X \mid v \text{ is a lowerbound of } A\}$ . If  $g$  is the greatest element of  $\mathcal{L}_A$ , we write  $g = \inf(A)$  and call it the infimum of  $A$ .
- (7) A maximal element of  $A$  is an element  $m \in A$  such that if  $a \geq m$ , then  $a = m$  (not necessarily unique).
- (8) A minimal element of  $A$  is an element  $n \in A$  such that if  $a \leq n$ , then  $a = n$  (not necessarily unique).
- (9) If  $(A, \leq)$  is a total ordering, then  $A$  is called a chain.

**Proposition 1.2.1.** Let  $(X, \leq)$  be an ordered set and  $A \subseteq X$ .

- (1) If  $A$  admits a greatest element, then it is unique,

- (2) If  $A$  admits a least element, then it is unique,
- (3) If  $A$  admits a least upper bound, then it is unique,
- (4) If  $A$  admits a greatest lower bound, then it is unique.

*Proof.* Suppose  $u, u'$  are greatest elements of  $A$ , then  $u, u' \in A$ . Hence  $u \leq u'$  and  $u' \leq u$ . By antisymmetry,  $u = u'$ , meaning the greatest element is unique. The proof for least elements being unique is identical, which establishes (1) and (2).

Note that  $\mathcal{U}_A \subseteq X$ . By definition the least element of  $\mathcal{U}_A$  is defined to be the supremum of  $A$ , and since least elements are unique the supremum of  $A$  must be unique. Similarly,  $\mathcal{L}_A \subseteq X$ . By definition the greatest element of  $\mathcal{L}_A$  is defined to be the infimum of  $A$ , and since greatest elements are unique the infimum of  $A$  must be unique. This establishes (3) and (4).  $\square$

**Lemma 1.2.1** (Zorn's Lemma). *Let  $X$  be an ordered set with the property that every chain has an upperbound. Then  $X$  contains a maximal element.*

**Example 1.2.3.** Considered the ordered set  $(\mathbb{N}, \leq_d)$  and the subset  $A = \{4, 7, 12, 28, 35\}$ .

- $A$  is bounded above with  $4 \times 7 \times 12 \times 28 \times 35$  as an upperbound.
- The supremum of  $A$  is  $\text{lcm}(4, 7, 12, 28, 35)$ .
- There does not exist a greatest element.
- 12, 28, and 35 are maximal elements (no other element in  $A$  divides them).

**Definition 1.2.4.** Let  $(X, \leq)$  be an ordered set and  $A \subseteq X$ . If  $A$  is bounded above and below, then we say  $A$  is bounded.

**Definition 1.2.5.** Let  $(X, \leq)$  be an ordered set. Then  $(X, \leq)$  is complete if, for every bounded set  $A \subseteq X$ ,  $\sup(A)$  and  $\inf(A)$  exist.

## 1.3 Functions

**Definition 1.3.1.** Let  $X$  and  $Y$  be sets. A function from  $X$  to  $Y$  is a relation  $f \subseteq X \times Y$  such that for all  $x \in X$ , there exists a unique  $y_x \in Y$  with  $(x, y_x) \in f$ .

- (1) The set  $X$  is the domain of  $f$ .
- (2) The set  $Y$  is the codomain of  $f$ .
- (3) The image of  $f$  is defined as  $f(X) = \{f(x) \mid x \in X\} \subseteq Y$  (also sometimes denoted  $\text{im}(f)$ ).
- (4) The preimage of  $f$  is defined as  $f^{-1}(Y) = \{x \in X \mid f(x) \in Y\} \subseteq X$ .
- (5) The graph of  $f$  is defined as  $\text{Graph}(f) = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$ .

If  $f$  is a function, we denote it by  $f : X \rightarrow Y$  or  $X \xrightarrow{f} Y$ .

**Example 1.3.1.** Let  $X$  be a set.

- (1) The *identity map*  $\text{id}_X : X \rightarrow X$  is defined by  $\text{id}_X(x) = x$ .
- (2) If  $X \subseteq Y$ , the *inclusion map*  $\iota : X \rightarrow Y$  is defined by  $\iota(x) = x$ .
- (3) If  $A \subseteq X$  is a set, the *characteristic function* (or *step function*)  $\mathbf{1}_A : X \rightarrow \mathbf{R}$  is defined by

$$\mathbf{1}_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A. \end{cases}$$

**Definition 1.3.2.** Given  $f, g : X \rightarrow \mathbf{R}$  and  $\alpha \in \mathbf{R}$ , the pointwise operations on  $f$  and  $g$  are:

- $(f \pm g)(x) = f(x) \pm g(x)$ ,
- $(\alpha f)(x) = \alpha f(x)$ ,
- $(fg)(x) = f(x)g(x)$ ,
- $(f/g)(x) = f(x)/g(x)$ .

**Definition 1.3.3.** Let  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be maps between sets. The composition of  $f$  and  $g$  is denoted  $g \circ f : X \rightarrow Z$ .

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \\ & \searrow & & \nearrow & \\ & & g \circ f & & \end{array}$$

**Definition 1.3.4.** Let  $f : X \rightarrow Y$  be a map between sets.

- (1)  $f$  is left-invertible if there exists a map  $g : Y \rightarrow X$  with  $g \circ f = \text{id}_X$ .
- (2)  $f$  is right-invertible if there exists a map  $h : Y \rightarrow X$  with  $f \circ h = \text{id}_Y$ .
- (3)  $f$  is invertible if there exists a map  $k : Y \rightarrow X$  with  $k \circ f = \text{id}_X$  and  $f \circ k = \text{id}_Y$ .

**Example 1.3.2.** The *shift function* is a map  $s : \mathbf{N} \rightarrow \mathbf{N}$  defined by  $s(n) = n + 1$ . Note that this function is left-invertible: define  $g : \mathbf{N} \rightarrow \mathbf{N}$  by

$$g(n) = \begin{cases} n - 1, & n \geq 2 \\ n_0, & n = 1, \end{cases}$$

where  $n_0$  is an arbitrary natural number, then  $g \circ s = \text{id}_{\mathbf{N}}$ .

Suppose that  $s$  has a right inverse, that is, there exists a function  $h : \mathbf{N} \rightarrow \mathbf{N}$  such that  $s \circ h = \text{id}_{\mathbf{N}}$ . Observe that:

$$(s \circ h)(1) = s(h(1)) = h(1) + 1 = 1.$$

It must be the case that  $h(1) = 0$ , which is a contradiction. Hence  $s$  is not right-invertible.

**Example 1.3.3.** The function  $g$  defined above is right invertible, but not left invertible.

**Proposition 1.3.1.** *Let  $f : X \rightarrow Y$  be a map between sets. The following are equivalent:*

- (1)  $f$  is invertible,
- (2)  $f$  is right-invertible and left-invertible.

*Proof.* Clearly (1) implies (2). Assume  $f$  to be left and right-invertible. Then there exists maps  $h, g : Y \rightarrow X$  with  $g \circ f = \text{id}_X$  and  $f \circ h = \text{id}_Y$ . Observe that:

$$\begin{aligned} h &= \text{id}_X \circ h \\ &= (g \circ f) \circ h \\ &= g \circ (f \circ h) \\ &= g \circ \text{id}_Y \\ &= g, \end{aligned}$$

establishing the proposition. □

**Definition 1.3.5.** Let  $f : X \rightarrow Y$  be a map between sets.

- (1)  $f$  is injective if  $f(x_1) = f(x_2)$  implies  $x_1 = x_2$ ,
- (2)  $f$  is surjective if  $\text{im}(f) = Y$ , and
- (3)  $f$  is bijjective if it is injective and surjective.

**Proposition 1.3.2.** *Let  $f : X \rightarrow Y$  be a map between sets.*

- 1.  $f$  is injective if and only if  $f$  is left-invertible.
- 2.  $f$  is surjective if and only if  $f$  is right-invertible.
- 3.  $f$  is bijective if and only if  $f$  is invertible.

*Proof.* (1) **Do the forward direction yourself!** Now assume  $f : X \rightarrow Y$  is injective. Define  $g : Y \rightarrow X$  by

$$g(y) = \begin{cases} x_0, & y \notin \text{im}(f) \\ x_y, & y \in \text{im}(f), \end{cases}$$

where  $x_y$  is the unique element in  $x$  mapping to  $y$ ; i.e.,  $f(x_y) = y$ . By our construction,  $(g \circ f)(x) = x$  for all  $x \in X$ .

(2) **Do the forward direction yourself!** Now assume  $f : X \rightarrow Y$  is onto. Note that the preimage of  $f$  is nonempty, so we can define  $h : Y \rightarrow X$  by  $h(y) = x_y$ , where  $x_y \in f^{-1}(y)$ . By our construction  $(f \circ h)(y) = f(x_y) = y$  for all  $y \in Y$ .

(3) **Do this yourself its easy!** □

**Corollary 1.3.1.** *Let  $A, B$  be sets. There exists an injection  $A \hookrightarrow B$  if and only if there exists a surjection  $B \twoheadrightarrow A$ .*

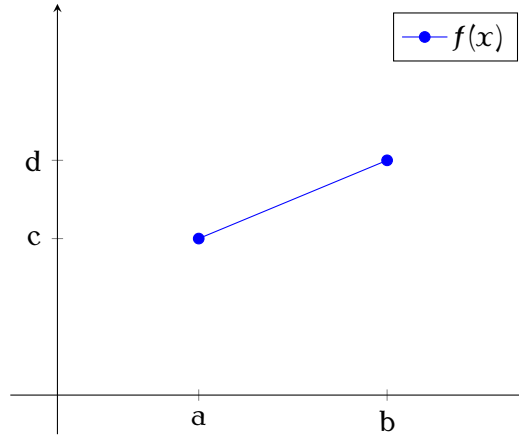
*Proof.* If  $f : A \rightarrow B$  is injective, then  $f$  is left invertible, that is, there exists a function  $g : B \rightarrow A$  with  $g \circ f = \text{id}_A$ . But this means  $g$  is right invertible, so  $g$  is onto. The other direction follows identically. □

## 1.4 Cardinality

**Definition 1.4.1.** Let  $A, B$  be sets. Then  $\text{card}(A) = \text{card}(B)$  if there exists a bijection  $A \hookrightarrow B$ .

**Example 1.4.1.**

- (1) Define  $f : \mathbb{N}_0 \rightarrow \mathbb{N}$  by  $f(n) = n + 1$ . This is a bijection, hence  $\text{card}(\mathbb{N}_0) = \text{card}(\mathbb{N})$ .
- (2) Let  $[a, b]$  and  $[c, d]$  be intervals with  $a < b$  and  $c < d$ . Define  $f : [a, b] \rightarrow [c, d]$  by  $f(x) = \left(\frac{d-c}{b-a}\right)(x - a) + c$ .



This is a bijection, hence  $\text{card}([a, b]) = \text{card}([c, d])$ . The result is the same had the intervals been open.

- (3) Recall that  $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$  is a bijection. Consider the maps  $(0, 1) \xrightarrow{g} (-\frac{\pi}{2}, \frac{\pi}{2}) \xrightarrow{\tan} \mathbb{R}$ . Since  $g$  and  $\tan$  are bijective,  $\tan \circ g$  is bijective, hence  $\text{card}((0, 1)) = \text{card}(\mathbb{R})$ .

**Definition 1.4.2.** A set  $A$  is called finite if there exists an  $N \in \mathbb{N}$  such that  $\text{card}(A) = \text{card}(\{1, \dots, N\})$ . If not, then  $A$  is called infinite.

**Proposition 1.4.1.** Given  $m, n \in \mathbb{N}$ ,  $m \neq n$ , then  $\text{card}(\{1, \dots, m\}) \neq \text{card}(\{1, \dots, n\})$ .

*Proof.* Without loss of generality, let  $m > n$ . By way of contradiction, if there exists a bijection  $f : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ , then there exists  $i, j \in \{1, \dots, m\}$  with  $i \neq j$  and  $f(i) = f(j)$ . This is a contradiction ( $f$  is not injective).  $\square$

**Proposition 1.4.2.**  $\mathbb{N}$  is infinite.

*Proof.* Suppose towards contradiction there exists an  $N \in \mathbb{N}$  and a bijection  $f : \mathbb{N} \rightarrow \{1, \dots, N\}$ . Note that the inclusion map  $\iota : \{1, \dots, N, N+1\} \rightarrow \mathbb{N}$  is injective. Now consider the maps  $\{1, \dots, N, N+1\} \xrightarrow{\iota} \mathbb{N} \xrightarrow{f} \{1, \dots, N\}$ . Then  $f \circ \iota : \{1, \dots, N, N+1\} \rightarrow \{1, \dots, N\}$ . But by the previous example this cannot be true, thus  $\mathbb{N}$  is infinite.  $\square$

**Exercise 1.4.1.** If  $A$  is infinite, there exists an injection  $\mathbb{N} \hookrightarrow A$ .

*Proof.* Let  $\pi : \mathbf{N} \rightarrow A$  be a map. Let  $a_1 \in A$ . Define  $\pi(1) = a_1$ . Since  $A$  is infinite,  $A - \{a_1\}$  is also infinite. Pick  $a_2 \in A$  and let  $\pi(2) = a_2$ . Inductively, we have that an injection  $\mathbf{N} \hookrightarrow A$ .  $\square$

**Example 1.4.2.**

- (1) Define  $k : \mathbf{Z} \rightarrow \mathbf{N}$  by  $k(n) = (-1)^{n-1} \lfloor \frac{n}{2} \rfloor$ . This is a bijection, hence  $\text{card}(\mathbf{Z}) = \text{card}(\mathbf{N})$ .
- (2) Let  $X$  be any set. Recall that the *power set of  $X$*  is defined as  $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ . Define  $2^X = \{f \mid f : X \rightarrow \{0, 1\}\}$ . Let  $A \subseteq X$ . Define  $\varphi : \mathcal{P}(X) \rightarrow 2^X$  by  $\varphi(A) = \mathbf{1}_A$ , where  $\mathbf{1}_A$  is the *characteristic function* defined in Example 1.3.1. Note that  $\varphi(A) = \varphi(B)$  if and only if  $\mathbf{1}_A = \mathbf{1}_B$ . Recall that functions are equal if and only if  $\mathbf{1}_A(x) = \mathbf{1}_B(x)$  for all  $x \in X$ .  $x \in A$  if and only if  $\mathbf{1}_A(x) = 1$  if and only if  $\mathbf{1}_B(x) = 1$ , giving  $x \in B$ . Thus  $A = B$  which means  $\varphi$  is injective. Now let  $f \in 2^X$ . Let  $A = \{x \in X \mid f(x) = 1\}$ . Then  $\mathbf{1}_A = f$ . Thus  $\varphi$  is bijective and so  $\text{card}(\mathcal{P}(X)) = \text{card}(2^X)$ .

**Exercise 1.4.2.** Show that  $\text{card}(\mathcal{P}(\{1, \dots, N\})) = 2^N$ .

*Proof.* **do this**  $\square$

**Theorem 1.4.1** (Cantor's Diagonal Argument).  $\text{card}(\mathbf{N}) < \text{card}((0, 1))$ .

*Proof.* Recall that every  $\sigma \in (0, 1)$  has a decimal expansion  $\sigma = 0.\sigma_1\sigma_2\dots = \sum_{k=1}^{\infty} \frac{\sigma_k}{10^k}$ , where  $\sigma_j \in \{0, 1, 2, \dots, 9\}$  which does not terminate in 9's. By way of contradiction, suppose there exists a surjection  $r : \mathbf{N} \rightarrow (0, 1)$  defined by  $r(n) = 0.\sigma_1(n)\sigma_2(n)\sigma_3(n)\dots$ , where  $\sigma_j(n) \in \{0, 1, 2, \dots, 9\}$  is the  $j^{\text{th}}$  digit in the decimal expansion.

Consider the map  $\tau : \mathbf{N} \rightarrow \{0, 1, \dots, 9\}$  defined by:

$$\tau(n) = \begin{cases} 3, & \sigma_n(n) = 2 \\ 2, & \sigma_n(n) = 3, \end{cases}$$

and let  $t = 0.\tau(1)\tau(2)\tau(3)\dots$ . Observe the following:

$$\begin{aligned} r(1) &= 0.\sigma_1(1)\sigma_2(1)\sigma_3(1)\sigma_4(1)\dots \\ r(2) &= 0.\sigma_1(2)\sigma_2(2)\sigma_3(2)\sigma_4(2)\dots \\ r(3) &= 0.\sigma_1(3)\sigma_2(3)\sigma_3(3)\sigma_4(3)\dots \\ r(4) &= 0.\sigma_1(4)\sigma_2(4)\sigma_3(4)\sigma_4(4)\dots \\ &\vdots \\ r(n) &= 0.\sigma_1(n)\sigma_2(n)\sigma_3(n)\sigma_4(n) \dots \sigma_n(n). \end{aligned}$$

Since  $r$  is surjective, there is an  $m \in \mathbf{N}$  with  $r(m) = t$ . It follows that:

$$\begin{aligned} r(m) &= 0.\sigma_1(m)\sigma_2(m)\sigma_3(m)\dots\sigma_m(m)\dots \\ &= 0.\tau(1)\tau(2)\tau(3)\dots\tau(m)\dots \end{aligned}$$

which implies that  $\sigma_m(m) = \tau(m)$ . But recall how we defined  $\tau(n)$ —if  $\sigma_m(m) = 2$ , then  $\tau(2) = 3$  and if  $\sigma_m(m) \neq 2$ , then  $\tau(2) = 2$ . This is a contradiction, hence there does not exist a surjection  $\mathbf{N} \xrightarrow{r} (0, 1)$ .  $\square$



**Corollary 1.4.1.**  $\text{card}(\mathbf{N}) \neq \text{card}(\mathbf{R})$

*Proof.* It follows from Example 1.4.1 that  $\text{card}(\mathbf{N}) < \text{card}((0, 1)) = \text{card}(\mathbf{R})$ .  $\square$

**Definition 1.4.3.** Let  $A$  and  $B$  be sets.

- (1) We write  $\text{card}(A) \leq \text{card}(B)$  if there exists an injection  $A \hookrightarrow B$ .
- (2) We write  $\text{card}(A) < \text{card}(B)$  if  $\text{card}(A) \leq \text{card}(B)$  and  $\text{card}(A) \neq \text{card}(B)$

**Example 1.4.3.**

- (1) If  $A \subseteq B$ , then the inclusion map  $\iota : A \rightarrow B$  gives  $\text{card}(A) \leq \text{card}(B)$ .
- (2) If  $m > n$ , then  $\text{card}\{1, \dots, n\} < \text{card}\{1, \dots, m\}$

**Proposition 1.4.3.** Let  $A$  be a set. Then  $\text{card}(A) < \text{card}(\mathcal{P}(A))$ .

*Proof.* Define  $f : A \rightarrow \mathcal{P}(A)$  by  $a \mapsto \{a\}$ . This is clearly an injective map. Now suppose towards contradiction that there exists a surjection  $g : A \rightarrow \mathcal{P}(A)$  defined by  $a \mapsto g(a)$ . Then  $g(a) \subseteq A$  (by the definition of a power set).

Let  $S = \{a \in A \mid a \notin g(a)\}$ . Then  $S \subseteq A$ . Since  $g$  is onto, there exists an element  $x \in A$  with  $g(x) = S$ . Case 1:  $x \in S$ . This implies that  $x \notin g(x)$ . But  $g(x) = S$ , so  $x \notin S$ , a contradiction. Case 2:  $x \notin S$ . This implies that  $x \in g(x)$ . But by definition this means  $x \in S$ , a contradiction. Since we have exhausted all the necessary cases, it must be that there does not exist a surjection from  $A \rightarrow \mathcal{P}(A)$ . Hence  $\text{card}(A) < \text{card}(\mathcal{P}(A))$ .  $\square$

**Lemma 1.4.1.** Let  $A$  and  $B$  be sets. The following are equivalent:

- (1)  $\text{card}(A) \leq \text{card}(B)$ ;
- (2) there exists an injection  $A \hookrightarrow B$ ;
- (3) there exists a surjection  $B \twoheadrightarrow A$ .

**Example 1.4.4.**

- (1) Define  $\mathbf{N} \times \mathbf{Z} \rightarrow \mathbf{Q}$  by  $(n, m) \mapsto \frac{m}{n}$ . This is surjective, so  $\text{card}(\mathbf{Q}) \leq \text{card}(\mathbf{N} \times \mathbf{Z})$ .
- (2) Define  $\mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$  by  $(m, n) \mapsto 2^m \cdot 3^n$ . Then  $g$  is injective by the fundamental theorem of arithmetic. So  $\text{card}(\mathbf{N} \times \mathbf{N}) \leq \text{card}(\mathbf{N})$ .
- (3) Recall from Example 1.4.2 that  $k : \mathbf{N} \rightarrow \mathbf{Z}$  defined by  $k(n) = (-1)^{n-1} \lfloor \frac{n}{2} \rfloor$  is a bijection. Define  $K : \mathbf{Z} \times \mathbf{N} \rightarrow \mathbf{N} \times \mathbf{N}$  by  $(m, n) \mapsto (k^{-1}(m), n)$ . This is a bijection, so  $\text{card}(\mathbf{Z} \times \mathbf{N}) = \text{card}(\mathbf{N} \times \mathbf{N})$ .
- (4) From the previous examples, we've established that:

$$\text{card}(\mathbf{N}) \leq \text{card}(\mathbf{Q}) \leq \text{card}(\mathbf{Z} \times \mathbf{N}) = \text{card}(\mathbf{N} \times \mathbf{N}) \leq \text{card}(\mathbf{N})$$

**Theorem 1.4.2.** Let  $\aleph$  denote the class of cardinals. The pair  $(\aleph, \leq)$  forms a total ordering—where  $\leq$  is defined by  $\text{card}(A) \leq \text{card}(B)$  if and only if  $A \hookrightarrow B$ . In particular, if  $A, B, C$  are sets with  $\text{card}(A), \text{card}(B), \text{card}(C) \in \text{obj}(\aleph)$ , then we have the following:

- (1)  $\text{card}(A) \leq \text{card}(A)$  (reflexive).
- (2) If  $\text{card}(A) \leq \text{card}(B) \leq \text{card}(C)$ , then  $\text{card}(A) \leq \text{card}(C)$  (transitive).
- (3) If  $\text{card}(A) \leq \text{card}(B)$  and  $\text{card}(B) \leq \text{card}(A)$ , then  $\text{card}(A) = \text{card}(B)$  (antisymmetric).
- (4) Either  $\text{card}(A) \leq \text{card}(B)$  or  $\text{card}(B) \leq \text{card}(A)$  (total).

*Proof.* (1) and (2) follow by simply applying definitions. Note that any set bijects into itself, hence  $A \hookrightarrow A$  implies  $A \hookrightarrow A$ , establishing  $\text{card}(A) \leq \text{card}(A)$ . Similarly, if there are bijections  $A \hookrightarrow B \hookrightarrow C$ , then clearly there is a bijection  $A \hookrightarrow C$ . Hence  $\text{card}(A) = \text{card}(C)$ .

(3) (Cantor-Schröder-Bernstein Theorem) We have injections  $A \xhookrightarrow{f}$  and  $B \xhookrightarrow{g} A$ . Let:

$$\begin{aligned} A_0 &= \text{im}(g)^c \\ A_1 &= (g \circ f)(A_0) \\ A_2 &= (g \circ f)(A_1) \\ &\vdots \\ A_n &= (g \circ f)(A_{n-1}). \end{aligned}$$

Note that  $A_1 \cap A_0 = \emptyset$  because  $A_1 \subseteq \text{im}(g)$  and  $A_0 = \text{im}(g)^c$ . We similarly have that  $A_2 \cap A_0 = \emptyset$ . Claim:  $A_1 \cap A_2 = \emptyset$ . **finish this**

(4) Let  $A \rightarrow B$  be a map. Let  $\mathcal{F} = \{(D, f) \mid D \subseteq A, f : D \hookrightarrow B, f \text{ is injective}\}$ . Note that  $\mathcal{F} \neq \emptyset$  because  $(\emptyset, k) \in \mathcal{F}$  for some map  $k$ . Define an ordering on  $\mathcal{F}$  as follows:  $(D, f) \leq_{\mathcal{F}} (E, g)$  if and only if  $D \subseteq E$  and  $g|_D = f$ . Then  $\mathcal{F}$  admits an upperbound of  $A$ . By **Zorn's Lemma**, there exists a maximal element  $(M, h) \in \mathcal{F}$ . Suppose towards contradiction there are elements  $a \in A$ ,  $a \notin M$  and  $b \in B$ ,  $b \notin h(M)$ . Consider the map:

$$h' : M \cup \{a\} \rightarrow B \text{ defined by } \begin{cases} h'(M) = h(M) \\ h'(a) = b \end{cases}.$$

This set is clearly injective, and furthermore we have that  $(M, h) \leq (M \cup \{a\}, h')$ . This is a contradiction, hence  $M = A$  or  $h(M) = B$ . If  $M = A$ , then the injection  $A \xhookrightarrow{h} B$  implies  $\text{card}(A) \leq \text{card}(B)$ . If  $h(M) = B$ , then the map  $B \hookrightarrow M \xhookrightarrow{h} A$  implies  $\text{card}(B) \leq \text{card}(A)$ .  $\square$

**Corollary 1.4.2.**  $\text{card}(\mathbb{Q}) = \text{card}(\mathbb{N})$ .

*Proof.* This follows directly from Example 1.4.4 and Theorem 1.4.2  $\square$

**Definition 1.4.4.** A set  $A$  is countable if  $\text{card}(A) \leq \text{card}(\mathbb{N})$ . Equivalently, there exists an injection  $A \hookrightarrow \mathbb{N}$  and a surjection  $\mathbb{N} \twoheadrightarrow A$ . If  $A$  is countable and infinite,  $A$  is called denumerable (or more commonly referred to as countably infinity).

**Definition 1.4.5.** We say  $\text{card}(\mathbf{N}) = \text{card}(\mathbf{Z}) = \text{card}(\mathbf{Q}) := \aleph_0$ , called aleph naught. We also define  $\text{card}(\mathbf{R}) = \mathfrak{c}$ , called the continuum.

**Example 1.4.5.** By Theorem 1.4.1,  $\aleph_0 < \mathfrak{c}$ .

**Corollary 1.4.3.** *There does not exist an infinite set  $A$  with  $\text{card}(A) < \aleph_0$ . In particular, if  $A$  is infinite and countable, then  $\text{card}(A) = \aleph_0$ .*

*Proof.* By Exercise 1.4.1,  $\text{card}(\mathbf{N}) \leq \text{card}(A)$ , and by definition (since  $A$  is countable),  $\text{card}(A) \leq \text{card}(\mathbf{N})$ . So by Theorem 1.4.2,  $\text{card}(A) = \text{card}(\mathbf{N}) = \aleph_0$ .  $\square$

**Example 1.4.6.**  $\text{card}(\mathcal{P}(\mathbf{N})) > \text{card}(\mathbf{N}) = \aleph_0$ .

**Proposition 1.4.4.** *The countable union of countable sets is countable. More precisely, if  $A_i$  is countable for all  $i \in \mathbf{N}$ , then  $\bigcup_{i=1}^{\infty} A_i$  is countable.*

*Proof.* By definition, there exist surjections  $\pi_i : \mathbf{N} \rightarrow A_i$ . Define  $\pi : \mathbf{N} \times \mathbf{N} \rightarrow \bigcup_{i=1}^{\infty} A_i$  by  $\pi(i, j) = \pi_i(j)$ . Claim:  $\pi$  is onto. Let  $x \in \bigcup_{i=1}^{\infty} A_i$ , then there exists an  $i_0$  with  $x \in A_{i_0}$ . Since  $\pi_{i_0}$  is onto, there exists a  $j_0 \in \mathbf{N}$  with  $\pi_{i_0}(j_0) = x$ . So  $\pi(i_0, j_0) = x$ , establishing that  $\pi$  is surjective as well. Therefore  $\text{card}(\bigcup_{i=1}^{\infty} A_i) \leq \text{card}(\mathbf{N} \times \mathbf{N}) = \text{card}(\mathbf{N})$ .  $\square$

**Lemma 1.4.2.**  $\text{card}([0, 1]) \leq \text{card}(2^{\mathbf{N}})$ .

*Proof.* Recall that every  $\sigma \in [0, 1]$  has a binary expansion  $\sigma = \sum_{k=1}^{\infty} \frac{\sigma_k}{2^k}$ , where  $\sigma_k \in \{0, 1\}$ . Consider the map  $\varphi : 2^{\mathbf{N}} \rightarrow [0, 1]$  defined by  $\varphi(f) = \sum_{k=1}^{\infty} \frac{f(k)}{2^k}$ . Letting  $f(k) = \sigma_k$  gives  $\varphi$  is surjective.  $\square$

**Lemma 1.4.3.**  $\text{card}(\mathbf{R}) = \text{card}([0, 1])$ .

*Proof.* By inclusion  $[0, 1] \hookrightarrow \mathbf{R}$ , which implies that  $\text{card}([0, 1]) \leq \text{card}(\mathbf{R})$ . Recall that  $\mathbf{R} \xrightarrow{\tan} (0, 1) \hookrightarrow [0, 1]$ , which implies that  $\text{card}(\mathbf{R}) \leq \text{card}([0, 1])$ . Then Theorem 1.4.2 gives the desired result.  $\square$

**Lemma 1.4.4.**  $\text{card}(2^{\mathbf{N}}) \leq \text{card}([0, 1])$ .

*Proof.* Consider the map  $\lambda : 2^{\mathbf{N}} \rightarrow [0, 1]$  defined by  $\lambda(f) = \sum_{k=1}^{\infty} \frac{f(k)}{3^k}$ . Claim:  $\lambda$  is injective. Let  $f, g \in 2^{\mathbf{N}}$  with  $f \neq g$ . Let  $k_0$  be the smallest point  $k$  where  $f$  and  $g$  are different. So in particular:

$$\begin{aligned} f(1) &= g(1) \\ f(2) &= g(2) \\ &\vdots \\ f(k_0 - 1) &= g(k_0 - 1) \\ f(k_0) &\neq g(k_0). \end{aligned}$$

Let:

$$\begin{aligned}
 t_1 &= \sum_{k > k_0} \frac{f(k)}{3^k} && \text{sum past } k_0 \\
 t_2 &= \sum_{k > k_0} \frac{g(k)}{3^k} && \text{sum past } k_0 \\
 s_1 &= \sum_{k=1}^{k_0-1} \frac{f(k)}{3^k} && \text{sum before } k_0 \\
 s_2 &= \sum_{k=1}^{k_0-1} \frac{g(k)}{3^k} && \text{sum before } k_0
 \end{aligned}$$

We have that:

$$\begin{aligned}
 \lambda(f) &= s_1 + \frac{f(k_0)}{3^{k_0}} + t_1 \\
 \lambda(g) &= s_2 + \frac{g(k_0)}{3^{k_0}} + t_2
 \end{aligned}$$

Because  $f$  and  $g$  differ at  $k_0$ , without loss of generality let  $f(k_0) = 0$  and  $g(k_0) = 1$ . Then  $\lambda(g) - \lambda(f) = \frac{1}{3^{k_0}} + t_2 - t_1$ . Observe that:

$$\begin{aligned}
 |t_2 - t_1| &= \left| \sum_{k > k_0} \frac{g(k) - f(k)}{3^k} \right| \\
 &\leq \sum_{k > k_0} \frac{|g(k) - f(k)|}{3^k} && \text{By triangle inequality} \\
 &\leq \sum_{k > k_0} \frac{1}{3^k} && \text{By comparison test} \\
 &= \frac{1}{3^{k_0+1}} \sum_{k \geq 0} \frac{1}{3^k} \\
 &= \frac{1}{3^{k_0+1}} \cdot \frac{1}{1 - \frac{1}{3}} \\
 &= \frac{3}{2 \cdot 3^{k_0+1}} \\
 &= \frac{1}{2 \cdot 3^{k_0}} \\
 &< \frac{1}{3^{k_0}}.
 \end{aligned}$$

Since  $|t_2 - t_1| < \frac{1}{3^{k_0}}$ ,  $\lambda(g) - \lambda(f) \neq 0$ , establishing  $\lambda$  as an injection. Thus  $\text{card}(2^{\mathbb{N}}) \leq \text{card}([0, 1])$ .  $\square$

**Theorem 1.4.3.**  $\text{card}(2^{\mathbb{N}}) = \text{card}(\mathcal{P}(\mathbb{N})) = \text{card}(\mathbb{R})$ .

*Proof.* This follows from Lemma 1.4.2, Lemma 1.4.3, and Lemma 1.4.4.  $\square$

# 2

## Ordered Fields

### 2.1 Ordering of $\mathbb{Z}$

**Definition 2.1.1.** Define  $\mathbf{Z}^+ = \{n \in \mathbf{Z} \mid n \geq_a 0\}$ , where  $\geq_a$  is the *algebraic ordering* from Example 1.2.1. We call  $\mathbf{Z}^+$  the cone of positive integers, and they admit the following axioms:

- (1) If  $m, n \in \mathbf{Z}^+$ , then  $m + n \in \mathbf{Z}^+$  and  $mn \in \mathbf{Z}^+$ .
- (2) For all  $m \in \mathbf{Z}$ ,  $m \in \mathbf{Z}^+$  or  $-m \in \mathbf{Z}^+$ .
- (3) If  $m \in \mathbf{Z}^+$  and  $-m \in \mathbf{Z}^+$ , then  $m = 0$ .

**Proposition 2.1.1** (Properties of  $\leq_a$ ).

- (1)  $m \leq_a n$  if and only if  $n - m \in \mathbf{Z}^+$ .
- (2) If  $m \leq_a n$  and  $p \leq_a q$ , then  $m + p \leq_a n + q$ .
- (3) If  $m \leq_a n$  and  $p \in \mathbf{Z}^+$ , then  $pm \leq_a pn$ .
- (4) If  $m \leq_a n$  then  $-n \leq_a -m$ .
- (5)  $(\mathbf{Z}, \leq_a)$  forms a total ordering.
- (6) If  $m >_a 0$  and  $mn >_a 0$ , then  $n >_a 0$ .
- (7) If  $m >_a 0$  and  $mn \geq_a mp$ , then  $n \geq_a p$ .

*Proof.* (5) Let  $m, n \in \mathbf{Z}$ , since  $\mathbf{Z}$  is closed under subtraction  $m - n \in \mathbf{Z}$ . So either  $m - n \in \mathbf{Z}^+$  or  $n - m \in \mathbf{Z}^+$ . Then by (1)  $n \leq_a m$  or  $m \leq_a n$ . Thus  $(\mathbf{Z}, \leq_a)$  is a total ordering.

(6) We have  $mn >_a 0$  with  $m >_a 0$ . If  $n = 0$ , we are done. So now assume  $n \neq 0$ . Then either  $n \in \mathbf{Z}^+$  or  $-n \in \mathbf{Z}^+$ . If  $-n \in \mathbf{Z}^+$ , then  $m(-n) = -(mn) \in \mathbf{Z}^+$ . But we had assumed  $mn >_a 0$ ; i.e.,  $mn \in \mathbf{Z}^+$ , hence it must be the case that  $mn = 0$ , a contradiction. Therefore it must be that  $n \in \mathbf{Z}^+$ .  $\square$

### 2.2 Ordering of $\mathbb{Q}$

**Proposition 2.2.1.** Define  $Q := \mathbf{Z} \times \mathbf{N}$ . Show that  $\sim$  forms an equivalence relation, where  $(a, b) \sim (c, d)$  if and only if  $ad = bc$ .

*Proof.* I dont wanna do this  $\square$

**Definition 2.2.1.** The set of equivalence classes of  $Q$  is  $\mathbf{Q} = Q / \sim = \{[(a, b)] \mid (a, b) \in Q\}$ . We call this set the rational numbers, and denote the equivalence classes  $[(a, b)]$  as  $\frac{a}{b}$ .

**Proposition 2.2.2.** *The operations*

$$\begin{aligned} + : \mathbf{Q} \times \mathbf{Q} &\rightarrow \mathbf{Q} \text{ defined by } [(a, b)] + [(c, d)] = [(ad + bc, bd)] \\ \cdot : \mathbf{Q} \times \mathbf{Q} &\rightarrow \mathbf{Q} \text{ defined by } [(a, b)] \cdot [(c, d)] = [(ac, bd)] \end{aligned}$$

are well-defined. Furthermore,  $(\mathbf{Q}, +, \cdot)$  forms a field.

*Proof.* I dont wana □

**Lemma 2.2.1.** *There is an injective map  $\mathbf{Z} \xrightarrow{j} \mathbf{Q}$  defined by  $j(n) = \frac{n}{1}$  satisfying the properties*

$$\begin{aligned} j(n + m) &= j(n) + j(m) \\ j(nm) &= j(n)j(m). \end{aligned}$$

*Proof.* Note that  $j(n) = j(m)$  if and only if  $\frac{n}{1} = \frac{m}{1}$ . By definition this is equivalent to  $n = m$ , hence  $j$  is injective.

Observe that  $j(n + m) = \frac{n+m}{1} = \frac{n}{1} + \frac{m}{1} = j(n) + j(m)$  and  $j(nm) = \frac{nm}{1} = \frac{n}{1} \cdot \frac{m}{1} = j(n)j(m)$ . □

**Theorem 2.2.1.**  $(\mathbf{Q}, \leq_Q)$  is a total ordering, where  $\leq_Q$  is a well-defined ordering defined by  $\frac{a}{b} \leq_Q \frac{c}{d}$  if and only if  $ad \leq_a bc$  in  $(\mathbf{Z}, \leq_a)$ . Furthermore, the map  $j : \mathbf{Z} \hookrightarrow \mathbf{Q}$  is order preserving, that is, if  $n \leq_a m$  in  $(\mathbf{Z}, \leq_a)$ , then  $j(n) \leq_Q j(m)$  in  $(\mathbf{Q}, \leq_Q)$ .

*Proof.* i REALLY dont □

**Definition 2.2.2.** Define  $\mathbf{Q}_+ := \{q \in \mathbf{Q} \mid q \geq_Q 0\}$  as the cone of positive rationals, and they admit the following axioms:

- (1) If  $q_1, q_2 \in \mathbf{Q}^+$ , then  $q_1 + q_2 \in \mathbf{Q}^+$  and  $q_1 q_2 \in \mathbf{Q}^+$ .
- (2) For all  $q \in \mathbf{Q}$ ,  $q \in \mathbf{Q}^+$  or  $-q \in \mathbf{Q}^+$ .
- (3) If  $q \in \mathbf{Q}^+$  and  $-q \in \mathbf{Q}^+$ , then  $q = 0$ .
- (4)  $q_1 \leq_Q q_2$  if and only if  $q_2 - q_1 \in \mathbf{Q}^+$ .

**Proposition 2.2.3.** *Let  $r, s, t, u \in \mathbf{Q}$*

- (1) *If  $r \leq_Q s$  and  $t \leq_Q u$ , then  $r + t \leq_Q s + u$ .*
- (2) *If  $r \leq_Q s$  and  $t \geq_Q 0$ , then  $tr \leq_Q ts$ .*

*Proof.* do this shi later □

## 2.3 Rings and Fields

**Definition 2.3.1.** A ring is a non-empty set  $R$  equipped with two binary operations:

$$R \times R \xrightarrow{a} R \text{ defined by } a(r, s) = r + s$$

$$R \times R \xrightarrow{m} R \text{ defined by } m(r, s) = rs,$$

such that they admit the following axioms:

(1)  $R$  is an *abelian group* under addition:

- (i)  $r + (s + t) = (r + s) + t$  for all  $r, s, t \in R$ ,
- (ii) there exists an element  $0_R \in R$  with  $r + 0_R = r = 0_R + r$  for all  $r \in R$ ,
- (iii) For all  $r \in R$  there exists an  $s \in R$  such that  $r + s = 0_R = s + r$  (such an  $s$  is unique, and is denoted  $-r$ ),
- (iv)  $r + s = s + r$  for all  $r, s \in R$ .

(2)  $r(st) = (rs)t$  for all  $r, s, t \in R$ ,

(3)  $(r + s)t = rt + rs$  and  $r(s + t) = rs + rt$  for all  $r, s, t \in R$ .

If  $R$  contains an element  $1_R$  such that  $1_R r = r = r 1_R$ , then we say  $R$  is unital. If  $rs = sr$  for all  $r, s \in R$ , then we say  $R$  is commutative. If  $R$  is a unital ring such that  $1_R \neq 0_R$  and for all  $r \in R$  there exists an  $s \in R$  such that  $rs = 1_R = sr$  (such an  $s$  is unique, and denoted  $r^{-1}$ ), then we say  $R$  is a division ring.

**Definition 2.3.2.** A field is a commutative division ring.

**Example 2.3.1.**

(1)  $\mathbf{Q}$  is a field.

(2)  $\mathbf{Z}/p\mathbf{Z}$  is a field.

(3)  $\mathbf{C}_{\mathbf{Q}} = \{r + si \mid r, s \in \mathbf{Q}, i^2 = -1\}$  with addition and multiplication defined by

$$\begin{aligned} (r + si) + (t + ui) &:= (r + t) + (s + u)i \\ (r + si)(t + ui) &:= (rt - su) + (ru + st)i \end{aligned}$$

is a field. We call this set the *complex rationals*.

**Definition 2.3.3.** An ordered field is a field  $F$  equipped with a total ordering  $\leq_F$  such that:

(1) If  $x \leq_F y$  and  $u \leq_F v$ , then  $x + u \leq_F y + v$ .

(2) If  $x \leq_F y$  and  $z \geq_F 0$ , then  $xz \leq_F zy$ .

We similarly define  $F^+ = \{x \in F \mid x \geq_F 0\}$  as the cone of positive elements.

**Proposition 2.3.1.** *Let  $(F, \leq_F)$  be an ordered field.*

- (1) *If  $x, y \in F^+$ , then  $x + y \in F^+$  and  $xy \in F^+$ .*
- (2) *If  $x \in F$ , then  $-x \in F^+$  or  $x \in F^+$ .*
- (3) *If  $x, -x \in F^+$ , then  $x = 0$ .*

*Proof. need to do*

□

**Example 2.3.2.**

- (1)  $\mathbf{Q}$  is an ordered field.
- (2) Is  $\mathbf{C}_{\mathbf{Q}}$  an ordered field?

**Proposition 2.3.2.** *Let  $(F, \leq)$  be an ordered field with  $1_F \neq 0_F$ .*

- (1) *For all  $a \in F$ ,  $a^2 \in F^+$ .*
- (2)  *$0, 1 \in F^+$ .*
- (3) *If  $n \in \mathbf{N}$ , then  $n \cdot 1_F := \underbrace{1_F + 1_F + \dots + 1_F}_{n \text{ times}}$ , implying  $n \cdot 1_F \in F^+$ .*
- (4) *If  $x \in F^+$  and  $x \neq 0$ , then  $x^{-1} \in F^+$ .*
- (5) *If  $xy \in F^+$  and  $xy \neq 0$ , then  $x, y \in F^+$  or  $-x, -y \in F^+$ .*
- (6) *If  $0 < x \leq y$ , then  $y^{-1} \leq x^{-1}$ .*
- (7) *If  $x \leq y$ , then  $-y \leq -x$ .*
- (8) *If  $x \geq 1_F$ , then  $x^2 \geq x$ .*
- (9) *If  $x \leq 1_F$ , then  $x^2 \leq x$ .*

*Proof.* (1) If  $a \in F^+$ , then  $a \cdot a = a^2 \in F^+$ . If  $-a \in F^+$ , then  $(-a) \cdot (-a) = a^2 \in F^+$ .

(2) From part (1) we have that  $0 = 0 \cdot 0 \in F^+$ . Similarly,  $1 = 1 \cdot 1 \in F^+$  and  $(-1) \cdot (-1) \in F^+$ .

(3) Since  $F^+$  is closed under addition, we can inductively show that  $n \cdot 1 = 1 + 1 + \dots + 1 \in F^+$ .

(4) Suppose towards contradiction  $x^{-1} \notin F^+$ . Then  $-(x^{-1}) \in F^+$ , so  $(-(x^{-1})) \cdot x = -1(x^{-1} \cdot x) = -1 \in F^+$ . But  $-1, 1 \in F^+$  implies  $1 = 0$ , a contradiction. Thus  $x^{-1} \in F^+$ .

(6)  $y \geq x > 0$  implies  $x, y \in F^+$ . So  $x^{-1}, y^{-1} \in F^+$ . Then  $y^{-1}xx^{-1} \leq y^{-1}yx^{-1}$ , and simplifying yields  $y^{-1} \leq x^{-1}$ . *finish the rest (i'm not going to)* □



# 3

## The Real Numbers

### 3.1 The Completion of $\mathbb{Q}$

**Definition 3.1.1.** A Dedekind cut is a nonempty subset  $D$  of  $\mathbb{Q}$  with the following properties:

- (1)  $D \neq \mathbb{Q}$ ;
- (2) If  $b \in D$ , then  $a \in D$  for all  $a \in \mathbb{Q}$  with  $a < b$ ;
- (3)  $D$  does not contain a largest element.

**Example 3.1.1.** The following examples are Dedekind cuts:

- (1)  $\{a \in \mathbb{Q} \mid a < 3\}$  (the set of all rational numbers less than 3).
- (2)  $\{a \in \mathbb{Q} \mid a < 0 \text{ or } a^2 < 2\}$  (the set of all rational numbers less than  $\sqrt{2}$ ).
- (3)  $\{a \in \mathbb{Q} \mid a < 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} \text{ for some } n \in \mathbb{Z}^+\}$  (the set of all rational numbers less than  $e$ ).

**Definition 3.1.2.** Let  $C$  and  $D$  be Dedekind cuts.

will probably not finish this

### 3.2 Ordering of $\mathbb{R}$

**Axiom 1.**  $\mathbb{R}$  is an ordered field.

**Proposition 3.2.1.**  $\mathbb{Q}^+ \subseteq \mathbb{R}^+$ .

*Proof.* If  $x \in \mathbb{Q}^+$ , then  $x = \frac{p}{q}$  with  $p \in \mathbb{Z}^+$  and  $q \in \mathbb{N}$ . Write  $p = \underbrace{1 + 1 + \dots + 1}_{p \text{ times}}$ , then  $p \in \mathbb{R}^+$ . Similarly, write  $q = \underbrace{1 + 1 + \dots + 1}_{q \text{ times}}$ . Then  $q \in \mathbb{R}^+$ , which implies that  $q^{-1} \in \mathbb{R}^+$ . Hence  $\frac{p}{q} \in \mathbb{R}^+$ , establishing  $\mathbb{Q}^+ \subseteq \mathbb{R}^+$ . □

**Proposition 3.2.2.** The maps  $\mathbb{Z} \xrightarrow{j} \mathbb{Q} \xrightarrow{i} \mathbb{R}$  are order embeddings (defined in Lemma 2.2.1 and Theorem 2.2.1).

*Proof.* Suppose  $i(q_1) \leq_{\mathbb{Q}} i(q_2)$ . Then  $q_1 \leq_{\mathbb{R}} q_2$ , hence  $q_2 - q_1 \in \mathbb{R}^+$ . Now If  $q_2 - q_2 \in \mathbb{Q}^+$ , then  $q_2 - q_1 \in \mathbb{R}^+$ . Hence  $q_1 \leq_{\mathbb{R}} q_2$ . wtf is this saying? □

**Proposition 3.2.3.** Let  $a, b \in \mathbb{R}$ . If  $a \leq b$  (or  $a < b$ ), then  $a \leq \frac{1}{2}(a + b) \leq b$  (or  $a < \frac{1}{2}(a + b) < b$ ).

*Proof.* By the order axioms,  $a \leq b$  implies  $a + a \leq a + b$ . So  $2a \leq a + b$ , which is equivalent to  $a \leq \frac{1}{2}(a + b)$ . Similarly,  $a + b \leq b + b$ , which similarly gives  $\frac{1}{2}(a + b) \leq b$ , establishing the proposition.  $\square$

**Corollary 3.2.1.** Given  $b > 0$ , we have  $0 < \frac{1}{2}b < b$ .

*Proof.* From Proposition 3.2.3, setting  $a = 0$  yields the desired result.  $\square$

**Proposition 3.2.4.** Suppose  $a \in \mathbb{R}$ . For all  $\epsilon > 0$ , if  $0 \leq a \leq \epsilon$ , then  $a = 0$ .

*Proof.* If  $a = 0$  we are done. If  $a > 0$ , by Corollary 3.2.1  $0 \leq \frac{1}{2}a \leq a$ . Pick  $\epsilon = \frac{1}{2}a$ , then  $a \leq \frac{1}{2}a$ , a contradiction. Thus  $a = 0$ .  $\square$

**Definition 3.2.1.** Let  $a_1, a_2, \dots, a_n > 0$ . The arithmetic mean is  $\frac{1}{n} \left( \sum_{j=1}^n a_j \right)$ . The geometric mean is  $\left( \prod_{j=1}^n a_j \right)^{\frac{1}{n}}$ .

**Proposition 3.2.5** (AM-GM Inequality). For all  $a_1, a_2, \dots, a_n \geq 0$ , then  $\left( \prod_{j=1}^n a_j \right)^{\frac{1}{n}} \leq \frac{1}{n} \left( \sum_{j=1}^n a_j \right)$ .

*Proof.* We will only prove the  $n = 2$  case. Consider the fact that  $(a_1 - a_2)^2 \geq 0$ , and expanding gives  $a_1^2 - 2a_1a_2 + a_2^2$ . So  $2a_1a_2 \leq a_1^2 + a_2^2$ . Adding  $2a_1a_2$  to both sides yields  $4a_1a_2 \leq a_1^2 + 2a_1a_2 + a_2^2$ , which is equivalent to  $4a_1a_2 \leq (a_1 + a_2)^2$ . Then simplifying yields the desired result of  $(a_1a_2)^{\frac{1}{2}} \leq \frac{1}{2}(a_1 + a_2)$ .  $\square$

**Proposition 3.2.6** (Bernoulli's Inequality). If  $x > -1$ , then  $(1 + x)^n \geq 1 + nx$  for all  $n \in \mathbb{N}_0$ .

*Proof.* We proceed with induction with base case  $n = 0$  and  $n = 1$ ; these hold by inspection. Assume the inequality holds true for  $n = k$ . For  $n = k + 1$ :

$$\begin{aligned} (1 + x)^{k+1} &= (1 + x)^k(1 + x) \\ &\geq (1 + nx)(1 + x)^1 \\ &= 1 + (n + 1)x + nx^2 \\ &\geq 1 + (n + 1)x. \end{aligned}$$

$\square$

**Proposition 3.2.7** (Cauchy-Schwartz Inequality). Let  $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}^n$ . Then:

$$\left| \sum_{j=1}^n a_j b_j \right| \leq \left( \sum_{j=1}^n a_j^2 \right)^{\frac{1}{2}} \left( \sum_{j=1}^n b_j^2 \right)^{\frac{1}{2}}.$$

---

<sup>1</sup>Because order is preserved under multiplication by positive elements.

*Proof.* Consider the map  $F : \mathbb{R}^n \rightarrow \mathbb{R}^n$  defined by  $F(t) = \sum_{j=1}^n (a_j - b_j t)^2$ . Note that  $\sum_{j=1}^n (a_j - b_j t)^2 \geq 0$ . Observe that:

$$\begin{aligned} \sum_{j=1}^n (a_j - b_j t)^2 &= \sum_{j=1}^n (a_j^2 - 2a_j b_j t + b_j^2 t^2) \\ &= \sum_{j=1}^n a_j^2 - \sum_{j=1}^n 2a_j b_j t + \sum_{j=1}^n b_j^2 t^2. \end{aligned}$$

This is a quadratic equation, and since  $F(t) \geq 0$ , the discriminant will be less than or equal to 0. Hence:

$$\Delta = \left( \sum_{j=1}^n 2a_j b_j \right)^2 - 4 \left( \sum_{j=1}^n b_j^2 \right) \left( \sum_{j=1}^n a_j^2 \right) \leq 0.$$

Simplifying gives:

$$\left( \sum_{j=1}^n 2a_j b_j \right)^2 \leq 4 \left( \sum_{j=1}^n b_j^2 \right) \left( \sum_{j=1}^n a_j^2 \right).$$

Pulling 2 out from the left-hand side, dividing both sides by 4, and then square-rooting gives the desired result.  $\square$

**Question.** When do we have equality?

*Answer.* When  $\Delta = 0$ , there exists a  $t_0 \in \mathbb{R}$  with  $F(t_0) = 0$ . So  $\sum_{j=1}^n (a_j - b_j t_0) = 0$  implies  $a_j - b_j t_0 = 0$  for all  $j$ . Hence there is equality only when  $a_j = b_j t_0$  for all  $j$ .

**Proposition 3.2.8** (Triangle Inequality). *Let  $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}^n$ . Then:*

$$\left( \sum_{j=1}^n (a_j + b_j)^2 \right)^{\frac{1}{2}} \leq \left( \sum_{j=1}^n a_j^2 \right)^{\frac{1}{2}} + \left( \sum_{j=1}^n b_j^2 \right)^{\frac{1}{2}}.$$

*Proof.* Observe that:

$$\begin{aligned} \sum_{j=1}^n (a_j + b_j)^2 &= \sum_{j=1}^n (a_j^2 + 2a_j b_j + b_j^2) \\ &= \sum_{j=1}^n a_j^2 + \sum_{j=1}^n 2a_j b_j + \sum_{j=1}^n b_j^2 \\ &\leq \sum_{j=1}^n a_j^2 + 2 \left( \sum_{j=1}^n a_j^2 \right)^{\frac{1}{2}} \left( \sum_{j=1}^n b_j^2 \right)^{\frac{1}{2}} + \sum_{j=1}^n b_j^2 \\ &= \left( \left( \sum_{j=1}^n a_j^2 \right)^{\frac{1}{2}} + \left( \sum_{j=1}^n b_j^2 \right)^{\frac{1}{2}} \right)^2. \end{aligned}$$

Squaring both sides gives the desired result.  $\square$

### 3.3 Metrics and Norms on $\mathbb{R}^n$

**Definition 3.3.1.** The absolute value is a function  $|\cdot| : \mathbb{R} \rightarrow \mathbb{R}$  defined by:

$$|x| = \begin{cases} x, & x \in \mathbb{R}^+ \\ -x, & -x \in \mathbb{R}^+. \end{cases}$$

**Proposition 3.3.1.** Let  $a, b \in \mathbb{R}$  and  $\delta > 0$ .

- (1)  $|ab| = |a||b|$ .
- (2)  $|a|^2 = |a^2|$ .
- (3)  $|-a| = |a|$ .
- (4)  $|a| \in \mathbb{R}^+$ .
- (5)  $-|a| \leq a \leq |a|$ .
- (6)  $|a| \leq \delta$  if and only if  $-\delta \leq a \leq \delta$ .
- (7)  $|a + b| \leq |a| + |b|$ .
- (8)  $|a - b| \leq |a| + |b|$ .
- (9)  $||a| - |b|| \leq |a - b|$ .

*Proof.* **do later** □

**Lemma 3.3.1.**  $\pm x \leq \delta$  if and only if  $|x| \leq \delta$ .

*Proof.* **do later** □

**Lemma 3.3.2.**  $A \subseteq \mathbb{R}$  is bounded if and only if there exists an  $r > 0$  such that  $|a| < r$  for all  $a \in A$ .

*Proof.* Suppose  $A \subseteq \mathbb{R}$  is bounded. Then there exists an  $l, u \in \mathbb{R}$  with  $l \leq a \leq u$  for all  $a \in A$ . We have that:

$$-|l| \leq l \leq a \leq u \leq |u|.$$

Let  $r = \max \{|l|, |u|\} \geq 0$ . So  $-r \leq |l| \leq a \leq |u| \leq r$ . Thus  $|a| \leq r$ .

Conversely, suppose there exists an  $r > 0$  with  $|a| \leq r$  for all  $a \in A$ . Then  $-r \leq a \leq r$  for all  $a \in A$ , hence  $A$  is bounded. □

**Definition 3.3.2.** A function  $f : D \rightarrow \mathbb{R}$  is bounded if  $\text{im}(f) \subseteq \mathbb{R}$  is a bounded subset. Equivalently, there exists a  $c > 0$  such that  $|f(x)| < c$  for all  $x \in D$ .

**Example 3.3.1.** Consider the function  $f : [3, 7] \rightarrow \mathbf{R}$  defined by  $f(x) = \frac{x^2+2x+1}{x-1}$ . Since  $3 \leq x \leq 7$ , observe that:

$$\begin{aligned} |x^2 + 2x + 1| &\leq |x^2| + |2x| + 1 \\ &= |x|^2 + 2|x| + 1 \quad \text{Evaluate at 7} \\ &= 64 \end{aligned}$$

Likewise,  $3 \leq x \leq 7$  implies  $|x - 1| \geq 2$ , hence  $\frac{1}{|x-1|} \leq \frac{1}{2}$ . Together, we have that:

$$\left| \frac{x^2 + 2x + 1}{x - 1} \right| \leq \frac{64}{2} = 32.$$

**Definition 3.3.3.** Let  $s, t \in \mathbf{R}$ . We define the distance between  $s$  and  $t$  as  $d(s, t) = |s - t|$ .

**Definition 3.3.4.** Let  $X$  be a nonempty set equipped with a map  $d : X \times X \rightarrow \mathbf{R}^+$ . We say  $(X, d)$  is a semi-metric if for all  $x, y, z \in X$ ,

- (1)  $d(x, y) = d(y, x)$ ,
- (2)  $d(x, z) \leq d(x, y) + d(y, z)$ , and
- (3)  $d(x, x) = 0$ .

We say  $(X, d)$  is a metric space if it satisfies the additional axiom:

- (4)  $d(x, y) = 0$  implies  $x = y$ .

**Proposition 3.3.2.**

- (1)  $(\mathbf{R}, d_1(s, t) = |s - t|)$  is a metric space.
- (2)  $(\mathbf{R}^n, d_1(\vec{x}, \vec{y}) = \sum_{j=1}^n |y_j - x_j|)$  is a metric space.
- (3)  $(\mathbf{R}^n, d_\infty(\vec{x}, \vec{y}) = \max_{j=1}^n \{|y_j - x_j|\})$  is a metric space.
- (4)  $(\mathbf{R}^n, d_2(\vec{x}, \vec{y}) = \left( \sum_{j=1}^n |y_j - x_j|^2 \right)^{\frac{1}{2}})$  is a metric space.
- (5)  $(\mathbf{R}^n, d_p(\vec{x}, \vec{y}) = \left( \sum_{j=1}^n |y_j - x_j|^p \right)^{\frac{1}{p}})$  for some  $p \in \mathbf{Q}$  is a metric space.

*Proof.* (1) We have  $d(s, t) = |s - t| = |t - s| = d(t, s)$ . Similarly,  $d(s, r) = |s - r| = |s - t + t - r| \leq |s - t| + |t - r| = d(s, t) + d(t, r)$ . Clearly  $d(s, s) = |s - s| = 0$ . Lastly, if  $d(s, t) = 0$ , then  $|s - t| = 0$ , which is equivalent to  $s - t = 0$ ; i.e.,  $s = t$ . Thus  $(\mathbf{R}, d_1)$  is a metric space.

(4) Axioms 2 and 3 of metric spaces are clearly satisfied. If  $d_2(\vec{x}, \vec{y}) = 0$  then  $|y_j - x_j|^2 = 0$  for all  $j$ . Hence  $y_j - x_j = 0$ ; i.e.,  $y_j = x_j$  for all  $j$ , establishing axiom 4. Observe that:

$$\begin{aligned}
 d_2(\vec{x}, \vec{z}) &= \left( \sum_{j=1}^n |z_j - x_j|^2 \right)^{\frac{1}{2}} \\
 &= \left( \sum_{j=1}^n |z_j - y_j + y_j - x_j|^2 \right)^{\frac{1}{2}} \\
 &= \left( \sum_{j=1}^n (z_j - y_j + y_j - x_j)^2 \right)^{\frac{1}{2}} \\
 &\leq \left( \sum_{j=1}^n (z_j - y_j)^2 \right)^{\frac{1}{2}} + \left( \sum_{j=1}^n (y_j - x_j)^2 \right)^{\frac{1}{2}} \\
 &= \left( \sum_{j=1}^n |z_j - y_j|^2 \right)^{\frac{1}{2}} + \left( \sum_{j=1}^n |y_j - x_j|^2 \right)^{\frac{1}{2}} \\
 &= d_2(\vec{x}, \vec{y}) + d_2(\vec{y}, \vec{z}).
 \end{aligned}$$

Thus  $(\mathbb{R}^n, d_2)$  is a metric space. □

**Definition 3.3.5.** Let  $(X, d)$  be a metric space.

- (1) The open ball centered at  $x_0$  with radius  $\delta > 0$  is  $U(x_0, \delta) = \{y \in X \mid d(y, x_0) < \delta\}$ .
- (2) The closed ball centered at  $x_0$  with radius  $\delta > 0$  is  $B(x_0, \delta) = \{y \in X \mid d(y, x_0) \leq \delta\}$ .
- (3) A subset  $A \subseteq X$  is called open if for all  $a \in A$ , there exists a  $\delta > 0$  such that  $U(a, \delta) \subseteq A$ .
- (4) A subset  $C \subseteq X$  is called closed if  $\text{compl}(C) = X \setminus C$  is open.

**Example 3.3.2.** Consider  $X = \mathbb{R}$  and  $d(s, t) = |s - t|$ . Observe that:

$$\begin{aligned}
 U(t, \delta) &= \{s \in \mathbb{R} \mid d(s, t) < \delta\} \\
 &= \{s \in \mathbb{R} \mid |s - t| < \delta\} \\
 &= \{s \in \mathbb{R} \mid -\delta < s - t < \delta\} \\
 &= \{s \in \mathbb{R} \mid -\delta + t < s < \delta + t\} \\
 &= (t - \delta, t + \delta).
 \end{aligned}$$

It follows similarly that  $B(t, \delta) = [t - \delta, t + \delta]$ .

**Proposition 3.3.3.** If  $I$  is an open interval, then  $I$  is open.

*Proof.* Let  $I = (a, b)$ . Let  $x \in I$ . Let  $\delta_x = \min\{x - a, b - x\} > 0$ . Now let  $t \in V_{\delta}(x)$ . Then  $t \in (x - \delta, x + \delta)$ . Case 1:  $\min\{x - a, b - x\} = x - a$ . Then  $x - (x - a) < t < x + x - a$ , **idk how to do this** □

# 4

## Supremum, Infimum, and Completeness

### 4.1 Supremum and Infimum

**Theorem 4.1.1.** Let  $\emptyset \neq A \subseteq \mathbf{R}$ . Let  $u$  be an upperbound for  $A$ . The following are equivalent:

- (1)  $u = \sup(A)$ .
- (2) If  $t < u$ , then there exists an  $a_t \in A$  with  $t < a_t$ .
- (3) For all  $\epsilon > 0$ , there exists an  $a_\epsilon \in A$  such that  $u - \epsilon < a_\epsilon$ .

*Proof.* [(1)  $\implies$  (2)] Assume  $u = \sup(A)$ . Let  $t < u$ . Suppose towards contradiction there does not exist an  $a \in A$  with  $a > t$ . Then  $a \leq t$  for all  $a \in A$ . But this implies  $t$  is an upperbound of  $A$  less than  $u$ , which is a contradiction because  $u$  is the least upper bound. [(2)  $\implies$  (3)] Given  $\epsilon > 0$ , let  $t = u - \epsilon$ . Then applying (2) gives the desired result. [(3)  $\implies$  (1)] We know  $u$  is an upperbound of  $A$ , we aim to show that it is the least upperbound. Let  $v$  be an upperbound for  $A$  with  $v < u$ . Pick  $\epsilon = u - v > 0$ . By (3), there exists an  $a_\epsilon \in A$  such that  $u - (u - v) < a_\epsilon$ . So  $v < a_\epsilon$ , which is a contradiction ( $v$  is an upperbound, how can it be smaller than an element of  $A$ ?).  $\square$

**Example 4.1.1.** Claim:  $\sup([0, 1)) = 1$ . If  $s \in [0, 1)$ , by definition  $s < 1$ , so 1 is an upper bound for  $[0, 1)$ . Given  $t < 1$ , set  $\delta = 1 - t > 0$ . Then  $0 < \frac{\delta}{2} < \delta$  **this is not trivial, have to show  $\delta - \delta/2$  is positive**. This gives:

$$t < t + \frac{\delta}{2} < t + \delta = 1.$$

Pick  $a_t = t + \frac{\delta}{2}$ . By (2) of Theorem 4.1.1,  $a_t \in [0, 1)$ , hence  $1 = \sup([0, 1))$ .

**Proposition 4.1.1.** Let  $A, B \subseteq \mathbf{R}$  and  $a \leq b$  for all  $a \in A$  and  $b \in B$ . Then  $\sup(A) \leq \inf(B)$ .

*Proof.* Fix a point  $b_0 \in B$ . Then  $a \leq b_0$  for all  $a \in A$ . Then  $b_0$  is an upperbound for  $A$ . This gives  $u := \sup(A) \leq b_0$ . But since  $b_0$  was arbitrary, we have  $u \leq b$  for all  $b \in B$ . So  $u$  is a lower bound for  $B$ , therefore  $u \leq \inf(B)$ .  $\square$

**Axiom 2** (Completeness of  $\mathbf{R}$ ). Given any nonempty subset  $A \subseteq \mathbf{R}$  which is bounded above,  $\sup(A)$  exists.

**Lemma 4.1.1.** For  $A \subseteq \mathbf{R}$  which is bounded below,  $\sup(-A) = -\inf(A)$ .

*Proof.* If  $A$  is bounded below, then  $-A$  is bounded above. Then  $\sup(-A)$  exists, define it as  $u$ . So for all  $a \in A$ ,  $-a \leq u$ . Hence  $-u$  is a lower bound for  $A$ . Suppose  $v$  is another lower bound for  $A$ . Then  $v \leq a$  for all  $a \in A$ . So  $-v \geq -a$  for all  $a \in A$ . Thus  $-v$  is an upper bound of  $-A$ . Therefore, since  $u$  is the least upper bound,  $-v \geq u$ ; i.e.,  $-u \geq v$ . Thus  $-u = \inf(A)$ .  $\square$

**Axiom 3** (Well-Ordering Principle). *Every nonempty subset  $A \subseteq \mathbf{N}$  contains a least element.*

**Proposition 4.1.2** (Arcimedean Property 1). *If  $x \in \mathbf{R}$ , then there exists  $n_x \in \mathbf{N}$  with  $x < n_x$ .*

*Proof.* Suppose not. That is, suppose  $n \leq x$  for all  $n \in \mathbf{N}$ . Then  $x$  is an upper bound for  $\mathbf{N}$ . Thus  $\sup(\mathbf{N}) := u$  exists. From part (3) of Theorem 4.1.1, take  $\epsilon = 1$ . Then there exists an  $n \in \mathbf{N}$  such that  $u - 1 < n$ . So  $u < n + 1 \in \mathbf{N}$ , which is a contradiction.  $\square$

**Proposition 4.1.3** (Archimedean Property 2). *If  $t > 0$ , there exists  $n_t \in \mathbf{N}$  with  $\frac{1}{n_t} < t$ .*

*Proof.* From Arcimedean Property 1, pick  $x = \frac{1}{t}$ .  $\square$

**Corollary 4.1.1.** *Given  $t > 0$ , there exists  $m \in \mathbf{N}$  with  $\frac{1}{2^m} < t$ .*

*Proof.* By Archimedean Property 2 there exists an  $n \in \mathbf{N}$  with  $\frac{1}{n} < t$ . Claim:  $\frac{1}{2^n} < \frac{1}{n}$ . It suffices to show that  $2^n > n$ . Proposition 1.4.3 gives  $\text{card}(\{1, 2, \dots, n\}) < \text{card}(\mathcal{P}(\{1, 2, \dots, n\}))$ . Then Exercise 1.4.2 gives:

$$n = \text{card}(\{1, 2, \dots, n\}) < \text{card}(\mathcal{P}(\{1, 2, \dots, n\})) = 2^n.$$

Alternatively, Bernoulli's Inequality gives  $(1 + 1)^n \geq 1 + n$ . Hence  $2^n > n$ .  $\square$

**Example 4.1.2.**

- (1) Claim:  $\inf \left\{ \frac{1}{n} \mid n \in \mathbf{N} \right\} = 0$ . Note that 0 is indeed a lower bound because  $0 < \frac{1}{n}$  for all  $n \in \mathbf{N}$ . Suppose  $t$  is another lower bound. If  $t \leq 0$ , then we are done. If  $t > 0$ , by the Archimedean Property there exists an  $n_t \in \mathbf{N}$  such that  $\frac{1}{n_t} < t$ , which is a contradiction (because we asserted that  $t$  is a lower bound, and  $\frac{1}{n_t} \in \inf \left\{ \frac{1}{n} \mid n \in \mathbf{N} \right\}$ ). Thus  $\inf \left\{ \frac{1}{n} \mid n \in \mathbf{N} \right\} = 0$ .
- (2) Claim:  $\inf \left\{ \frac{1}{2^m} \mid m \in \mathbf{N} \right\} = 0$ . This follows from the above example and previous corollary.

**Corollary 4.1.2.** *Let  $x \in \mathbf{R}$ . Then there exists  $n_x \in \mathbf{Z}$  with  $n_x - 1 \leq x < n_x$ .*

*Proof.* Case 1:  $x \geq 0$ . Let  $S_x = \{n \in \mathbf{N} \mid x < n\}$ . By Arcimedean Property 1  $S_x \neq \emptyset$ . By the Well-Ordering Principle, there exists a least element in this set, call it  $n_x$ . Since  $n_x \in S_x$ , it must be the case that  $x < n_x$ . But since  $n_x$  is the least element,  $n_x - 1 \notin S_x$ . Since  $S_x$  is the set of all natural numbers with lower bound  $x$ ,  $n_x - 1$  is not bounded below by  $x$ . Whence  $n_x - 1 \leq x$ .

Case 2:  $x < 0$ . Define  $S_{-x} = \{n \in \mathbf{N} \mid n < -x\}$ . As a consequence of the Well-Ordering Principle, any subset of the integers which is bounded above admits a greatest element, define it to be  $n_{-x} \in \mathbf{Z}$ . Then  $n_{-x} + 1 \notin S_{-x}$ , hence  $n_{-x} < -x \leq n_{-x} + 1$ . This establishes  $-n_{-x} - 1 \leq x < -n_{-x}$ .  $\square$

**Definition 4.1.1.** Let  $I$  be an open interval. A subset  $D \subseteq \mathbf{R}$  is dense if  $I \cap D \neq \emptyset$ .

**Theorem 4.1.2.**  $\mathbf{Q} \subseteq \mathbf{R}$  is dense.

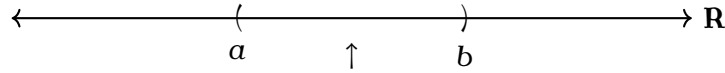


*Proof.* Let  $I$  be an open interval. Then there exists  $a, b \in \mathbf{R}$  with  $(a, b) \subseteq I$ . We have that  $b - a > 0$ . By **Archimedean Property 2** there exists  $n \in \mathbf{N}$  with  $\frac{1}{n} < b - a$ . So  $1 + na < nb$ . By Corollary 4.1.2, there exists  $m \in \mathbf{Z}$  with  $m - 1 \leq na < m$ . Equivalently, we have that  $a < \frac{m}{n}$ . We also have that  $m \leq na + 1 < nb$ , which yields  $\frac{m}{n} < b$ . Thus  $\frac{m}{n} \in (a, b) \cap \mathbf{Q}$ .  $\square$

**Corollary 4.1.3.**  $\mathbf{R} \setminus \mathbf{Q} \subseteq \mathbf{R}$  is dense.

*Proof.* Let  $a < b$ . Consider  $a' = a\sqrt{2}$  and  $b' = b\sqrt{2}$ . Then  $a' < b'$ . By Theorem 4.1.2, there exists a  $q \in \mathbf{Q}$  with  $a' < q < b'$ . Thus  $a < \frac{q}{\sqrt{2}} < b$ . Since  $\frac{q}{\sqrt{2}} \notin \mathbf{Q}$ , the corollary is established.

Alternatively, observe the following picture:



If there is not an irrational number between  $(a, b)$ , then  $(a, b) \subseteq \mathbf{Q}$ , which is a contradiction.  $\square$

**Theorem 4.1.3.** There exists a unique positive number  $x$  with  $x^2 = 2$ .

*Proof.* Consider the set  $S = \{t \in \mathbf{R} \mid t > 0, t^2 < 2\}$ . Note that  $S \neq \emptyset$  because  $1 \in S$ . If  $t \geq 2$ , then  $t^2 \geq 2t > 4$ , meaning it would not be an element of  $S$ . So  $S$  is bounded above by 2. Hence there exists  $u := \sup(S)$ .

Scratchwork: Assume  $u^2 < 2$ . Find a sufficiently small  $n$  so that  $(u + \frac{1}{n})^2 \in S$ ; i.e.,  $(u + \frac{1}{n})^2 < 2$ . Solving for  $n$  yields:

$$\begin{aligned}
 & \text{—————/—————} \\
 & u^2 + \frac{2u}{n} + \frac{1}{n^2} < 2 \\
 & \iff \\
 & \frac{2u}{n} + \frac{1}{n^2} < 2 - u^2 \\
 & \iff \\
 & \frac{1}{n} \left( 2u + \frac{1}{n} \right) < 2 - u^2 \\
 & \iff \\
 & \frac{1}{n} (2u + 1) < 2 - u^2 \\
 & \iff \\
 & \frac{1}{n} < \frac{2 - u^2}{2u + 1} \in \mathbf{R}^+ \setminus \{0\} \\
 & \text{—————/—————}
 \end{aligned}$$

If  $u^2 < 2$ , then  $\frac{2-u^2}{2u+1} > 0$ . By **Archimedean Property 2**, there exists an  $n \in \mathbf{N}$  with  $\frac{1}{n} < \frac{2-u^2}{2u+1}$ . Simplifying yields  $(u + \frac{1}{n})^2 < 2$ , or equivalently  $u + \frac{1}{n} \in S$ , which is a contradiction. It must be the case that  $u^2 \geq 2$ ; i.e.,  $u^2 - 2 \geq 0$ . Now since  $u = \sup(S)$ , for all  $m \in \mathbf{N}$ , there exists  $t_m \in S$  with  $u - \frac{1}{m} < t_m$ . We have that  $(u - \frac{1}{m})^2 < t_m^2 < 2$ . This simplifies to  $u^2 - 2 < \frac{2u}{m} - \frac{1}{m^2} < \frac{2u}{m}$ , or equivalently  $\frac{u^2-2}{2u} < \frac{1}{m}$ . But if  $\frac{u^2-2}{2u} < \frac{1}{m}$  for all  $m \in \mathbf{N}$ , it must be that  $\frac{u^2-2}{2u} = 0$ , hence  $u^2 = 2$ .

Lastly we show that  $u^2$  is unique. Suppose  $u^2 = 2 = v^2$ . Since  $u, v \geq 0$ ,  $(u^2 - v^2) = 0$ . Then  $(u - v)(u + v) = 0$ . If  $u + v = 0$ , then  $u = 0$  and  $v = 0$ , which is a contradiction. So  $u - v = 0$  implies  $u = v$ .  $\square$

*Remark.* Picking 2 was completely arbitrary, we could have showed  $x^2 = a$  for any  $a \geq 0$ .

*Remark.* Using the same argument, we have that for all  $a > 0$ , there exists a unique  $b > 0$  with  $b^2 = a$ . So we have a map:

$$\mathbf{R}^+ \xrightarrow{\sqrt{\cdot}} \mathbf{R}^+,$$

where  $\sqrt{x}$  is the unique positive number with  $(\sqrt{x})^2 = x$ .

*Remark.* We could have similarly defined  $S$  as:

$$S' = \{t \in \mathbf{Q} \mid t > 0, t^2 < 2\},$$

and the proof would not have changed. However,  $\sup(S') = \sqrt{2} \notin \mathbf{Q}$ , meaning  $\mathbf{Q}$  is *not* complete.

## 4.2 Nested Intervals

**Axiom 4.** Given any interval  $I$ , if  $x, y \in I$  with  $x < y$ , then  $[x, y] \in I$ .

**Theorem 4.2.1.** Let  $S \subseteq \mathbf{R}$  be any subset containing at least two points. If  $S$  satisfies Axiom 4, then  $S$  is an interval.

*Proof.* We proceed with cases. Case 1:  $S$  is bounded. Write  $a = \inf(S)$  and  $b = \sup(S)$ . Therefore  $S \subseteq [a, b]$ . If we show  $(a, b) \subseteq S$ , then it follows that  $S = (a, b)$ , or  $[a, b)$ , or  $(a, b]$  or  $[a, b]$ . We must use that  $S$  satisfies Axiom 4 and  $a = \inf(S)$  and  $b = \sup(S)$ . Let  $x \in (a, b)$ . Since  $x > a$ , there exists  $s_1 \in S$  with  $s_1 < x$ . Since  $x < b$ , there exists an  $s_2 \in S$  with  $x < s_2$ . Thus  $s_1, s_2 \in S$  and  $s_1 < s_2$ . By Axiom 4  $[s_1, s_2] \subseteq S$ . But  $x \in [s_1, s_2]$  implies  $x \in S$ . Thus  $(a, b) \subseteq S$ .

Case 2:  $S$  is bounded above **do this**.

Case 3:  $S$  is bounded below **need to do**. □

**Definition 4.2.1.** A sequence of intervals  $(I_n)_{n \geq 1}$  is said to be nested if  $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$

**Proposition 4.2.1.**  $\bigcap_{n \geq 1} [0, \frac{1}{n}) = \{0\}$ .

*Proof.* Note that  $0 \in [0, \frac{1}{n})$  for all  $n \geq 1$ . So  $0 \in \bigcap_{n \geq 1} [0, \frac{1}{n})$ . Let  $a \in \bigcap_{n \geq 1} [0, \frac{1}{n})$ . Then  $0 \leq a < \frac{1}{n}$  for all  $n \geq 1$ . Hence  $a = 0$ . □

**Proposition 4.2.2.**  $\bigcap_{n \geq 1} [n, \infty) = \emptyset$ .

*Proof.* Suppose towards contradiction there exists a  $t \in \bigcap_{n \geq 1} [n, \infty) = \emptyset$ . Then  $t \in [n, \infty)$  for all  $n \geq 1$ . So  $t \geq n$  for all  $n \geq 1$ . Hence  $\mathbf{N}$  is bounded above, which is a contradiction. □

**Theorem 4.2.2 (Nested Intervals).** Let  $(I_n)_{n \geq 1}$  be a sequence of closed and bounded nested intervals. Then  $\bigcap_{n \geq 1} I_n \neq \emptyset$ . Furthermore, if  $\inf \{\text{length}(I_n) \mid n \geq 1\} = 0$ , then  $\bigcap_{n \geq 1} I_n = \{\xi\}$ .

*Proof.* Let  $I_n = [a_n, b_n]$ . Note that:

$$\begin{aligned} a_1 &\leq a_2 \leq a_3 \leq \dots \\ b_1 &\geq b_2 \geq b_3 \geq \dots \end{aligned}$$

We have that  $a_1 \leq a_n \leq b_n \leq b_1$  for all  $n \geq 1$ . So the set  $\{a_n \mid n \geq 1\}$  is bounded above, and similarly  $\{b_n \mid n \geq 1\}$  is bounded below. Let

$$\xi = \sup_{n \geq 1} \{a_n\}$$

$$\eta = \inf_{n \geq 1} \{b_n\}.$$

Claim:  $\xi \leq b_n$  for all  $n \geq 1$ . Assume towards contradiction  $\xi > b_m$  for some  $m \geq 1$ . Since  $\xi = \sup_{n \geq 1} \{a_n\}$ , there exists an  $a_k$  with  $b_m < a_k \leq \xi$ . If  $k \geq m$ , then  $b_m < a_k \leq b_k \leq b_m$ , which is a contradiction. If  $k < m$ , then  $a_k \leq a_m \leq b_m < a_k$ , which is a contradiction.

Claim:  $a_n \leq \xi$  for all  $n \geq 1$ . Then  $\xi \leq \eta$  since  $\sup_{n \geq 1} \{a_n\} = \xi$ . We have  $[\xi, \eta] \subseteq [a_n, b_n]$  for all  $n \in \mathbf{N}$ . Let  $x \in [\xi, \eta]$ . Then:

$$a_n \leq \xi \leq x \leq \eta \leq b_n,$$

hence  $x \in [a_n, b_n]$ ; i.e.,  $[\xi, \eta] \subseteq [a_n, b_n]$  for all  $n \geq 1$ . Thus  $[\xi, \eta] \subseteq \bigcap_{n \geq 1} [a_n, b_n]$ . Conversely, let  $t \in [a_n, b_n]$  for all  $n \geq 1$ . Then  $a_n \leq t \leq b_n$ . This implies  $t$  is both an upper bound for  $\{a_n\}_{n \geq 1}$  and a lower bound for  $\{b_n\}_{n \geq 1}$ . Hence  $\xi \leq t \leq \eta$ , implying  $t \in [\xi, \eta]$ . This establishes  $[\xi, \eta] = \bigcap_{n \geq 1} [a_n, b_n]$ .

Now suppose  $\inf \{\text{length}(I_n) \mid n \geq 1\} = 0$ . Then:

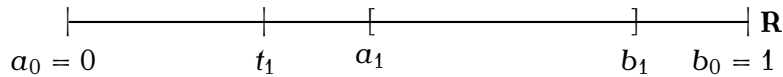
$$\begin{aligned} 0 &= \inf_{n \geq 1} (b_n - a_n) \\ &= \inf_{n \geq 1} b_n - \inf_{n \geq 1} a_n \\ &= \eta - \xi. \end{aligned}$$

Hence  $\xi = \eta$ , which establishes the theorem.

Alternatively, had we assumed  $\xi \neq \eta$ , then  $\eta - \xi > 0$ . So there exists an  $m$  such that  $b_m - a_m < \eta - \xi$ , which is a contradiction since  $[\xi, \eta] \subseteq [a_m, b_m]$ .  $\square$

**Corollary 4.2.1.**  $[0, 1]$  is uncountable.

*Proof.* By way of contradiction, suppose  $[0, 1] = \{t_1, t_2, t_3, \dots\}$ . Consider the following picture:



Find  $[a_1, b_1] \subseteq [0, 1]$  with  $t_1 \notin [a_1, b_1]$ . Find  $[a_2, b_2] \subseteq [a_1, b_1]$  with  $t_2 \notin [a_2, b_2]$ . Inductively, find  $[a_n, b_n] \subseteq [a_{n-1}, b_{n-1}]$  with  $t_n \notin [a_n, b_n]$ . Thus  $[a_n, b_n]$  is nested. Now let  $\xi \in \bigcap_{n \geq 1} [a_n, b_n]$ . Then  $\xi \in [0, 1]$ . But  $\xi \neq t_n$  for all  $n$ , which is a contradiction.  $\square$

# 5

## Sequences

### 5.1 Basic Definitions and Examples

**Definition 5.1.1.** A sequence in a metric space  $X$  is a map  $x : \mathbb{N} \rightarrow X$ . We often write  $x = (x_n)_{n \geq 1} = (x_1, x_2, x_3, \dots)$ , where  $x_n = x(n)$ . If  $X = \mathbb{R}$ , we call  $x$  a real sequence.

**Example 5.1.1** (Sequences Defined Explicitly).

- (1) A constant sequence:  $x_n = t$ ,  $(x_n)_{n \geq 1} = (t, t, t, \dots)$ .
- (2) Sequences defined by a function:  $d_n = (1 + \frac{1}{n})^n$ .
- (3) Geometric sequences<sup>1</sup>: fix  $b \in \mathbb{R}$ ,  $x_n = b^n$ . Then  $(x_n)_{n \geq 1} = (1, b, b^2, b^3, \dots)$ .

**Example 5.1.2** (Sequences Defined Recursively).

- (1) Let  $a_1 = 1$ ,  $a_{n+1} = 2a_n + 1$ . Then  $(a_n)_{n \geq 1} = (1, 3, 7, 15, \dots)$ .
- (2) Let  $f_1 = 1$ ,  $f_2 = 1$ ,  $f_{n+1} = f_n + f_{n-1}$ . Then  $(f_n)_{n=1}^\infty = (1, 1, 2, 3, 5, 8, \dots)$ . This is the *Fibonacci sequence*.
- (3) Let  $X$  be a metric space and  $f : X \rightarrow X$  be an endomorphism. Fix  $x_0 \in X$ . Then define:

$$\begin{aligned} x_1 &= f(x_0) \\ x_2 &= f(x_1) \\ &\vdots \\ x_n &= f(x_{n-1}). \end{aligned}$$

**Example 5.1.3** (New Sequences from Old).

- (1) Let  $(a_n)_{n \geq 1}$  and  $(b_n)_{n \geq 1}$  be sequences. Then define:

$$\begin{aligned} (a_n)_{n \geq 1} \pm (b_n)_{n \geq 1} &= (a_n \pm b_n)_{n \geq 1}, \\ t(a_n)_{n \geq 1} &= (ta_n)_{n \geq 1}, \\ (a_n)_{n \geq 1} \cdot (b_n)_{n \geq 1} &= (a_n \cdot b_n)_{n \geq 1}. \end{aligned}$$

If  $(b_n)_{n \geq 1} \neq 0$  for all  $n$ , then:

$$\frac{(a_n)_{n \geq 1}}{(b_n)_{n \geq 1}} = \left( \frac{a_n}{b_n} \right)_{n \geq 1}.$$

---

<sup>1</sup>These are called geometric because the ratio between each  $x_n$  is constant:  $x_{n+1}/x_n = b^{n+1}/b^n = b$ .

(2) Given  $(x_n)_{n \geq 1}$  and  $k \in \mathbf{N}$ , consider  $(x_{n+k})_{n=0}^\infty = (x_k, x_{k+1}, x_{k+1}, \dots)$ . This is called a *shift* or the  $k^{\text{th}}$  *tail* of  $(x_n)_{n \geq 1}$ .

(3) If  $(a_n)_{n \geq 1}$  is a sequence,  $a_n \neq 0$  for all  $n$ , consider:

$$r_n = \frac{a_{n+1}}{a_n}.$$

So  $(r_n)_{n \geq 1} = \left( \frac{a_2}{a_1}, \frac{a_3}{a_2}, \frac{a_4}{a_3}, \dots \right)$ . These are called sequences of *ratios*.

(4) Given a real sequence  $(x_k)_{k=1}^\infty$ , consider the sequence  $(s_n)_{n=1}^\infty$  where:

$$s_1 = x_1$$

$$s_2 = x_1 + x_2 = s_1 + x_2$$

$$s_3 = x_1 + x_2 + x_3 = s_2 + x_3$$

$$\vdots$$

$$s_n = \sum_{k=1}^n x_k = s_{n-1} + x_n.$$

We call these  $n^{\text{th}}$  *partial sums*. An example of these are geometric sequences and telescoping sequences.

## 5.2 Convergence

**Definition 5.2.1.** Let  $(x_n)_{n \geq 1}$  be a sequence.

- (1)  $x_n$  is increasing if  $x_1 \leq x_2 \leq x_3 \leq \dots$
- (2)  $x_n$  is decreasing if  $x_1 \geq x_2 \geq x_3 \geq \dots$
- (3)  $x_n$  is strictly increasing if  $x_1 < x_2 < x_3 < \dots$
- (4)  $x_n$  is strictly decreasing if  $x_1 > x_2 > x_3 > \dots$

**Note 1.** A sequence is said to *eventually* have a certain property, if it does not have the said property across all its ordered instances, but will after some instances have passed.

**Note 2.**  $x_n$  is monotone if it is either increasing or decreasing, strictly increasing, or strictly decreasing.

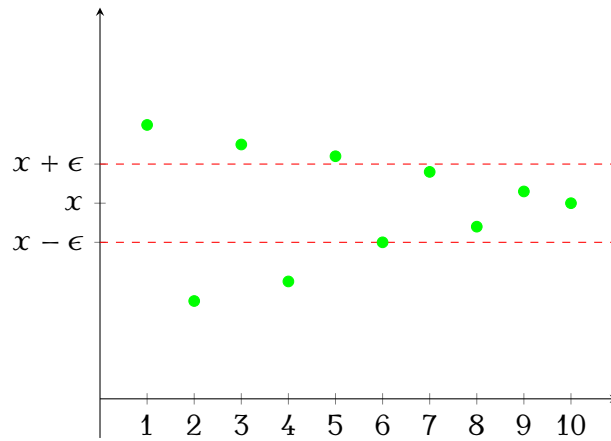
**Definition 5.2.2.** A sequence  $(x_n)_n$  in a metric space  $X$  converges to  $x \in X$  if:

$$(\forall \epsilon > 0)(\exists N_\epsilon \in \mathbf{N}) \text{ s.t. } n \geq N_\epsilon \implies d(x_n, x) < \epsilon.^2$$

If no such  $x$  exists, the sequence is divergent. If  $(x_n)_n$  converges to  $x$ , we write  $(x_n)_n \xrightarrow{n \rightarrow \infty} x$  or  $\lim_{n \rightarrow \infty} x_n = x$ .

<sup>2</sup>I try not to use first-order logic symbols but this will be one of the few exceptions.

**Example 5.2.1.** Let  $X = \mathbf{R}$ . Then from the above definition, write  $d(x_n, x) = |x_n - x|$ . Recall that this is equivalent to  $x_n \in V_\epsilon(x)$ . We can visually represent convergence as follows:



If the sequence is convergent it will eventually be contained between the two dashed lines.

**Example 5.2.2.** Prove that  $(\frac{1}{n})_{n \geq 1} \rightarrow 0$ .

*Solution.* This is a test for pushing to Github! This is another test