

Contents

<b>1</b>	<b>Fundamentals</b>	<b>2</b>
1.1	Sets . . . . .	2
1.1.1	Definition . . . . .	2
1.1.2	Set operations . . . . .	2
1.1.3	Indexed sets . . . . .	2
1.1.4	Cartesian product . . . . .	3
1.2	Methods of Proof . . . . .	4
1.2.1	Proving equality via two inequalities . . . . .	4
1.2.2	Contradiction (bwoc) . . . . .	4
1.2.3	Proving the contrapositive . . . . .	5
1.2.4	Induction . . . . .	5
1.2.5	Pigeonhole principle . . . . .	5
1.3	Functions . . . . .	6
1.4	Relations . . . . .	10
1.5	Number Systems . . . . .	13
<b>2</b>	<b>Appendix</b>	<b>13</b>

# 1 Fundamentals

## 1.1 Sets

### 1.1.1 Definition

A **set** can be considered as a collection of elements; more intuitively, you can consider something a set if you can determine whether a given object belongs to it. Typically sets are defined as  $A = \{1, 2, \dots\}$ , by a property  $A = \{x \mid x \% 2 = 0\}$ , or with an appropriate verbal description.

### 1.1.2 Set operations

There are a number of ways to “combine” sets:

- **Union:**  $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- **Intersection:**  $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- **Difference:**  $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$

**Lemma 1.1.**  $A = (A \setminus B) \cup (A \cap B)$

*Proof.* To prove set equivalencies, we must prove that both  $\text{RHS} \subseteq \text{LHS}$  and  $\text{LHS} \subseteq \text{RHS}$ ; meaning, the LHS and RHS are subsets of each other, and are thus equal.

First, to prove  $\text{LHS} \subseteq \text{RHS}$ , let  $a \in A$ . If  $a \notin B$ , then  $a \in A \setminus B$ , and  $a \in \text{RHS}$ . Else, if  $a \in B$ , then  $a \in A \cap B$  and  $a \in \text{RHS}$ . Thus,  $\text{LHS} \subseteq \text{RHS}$ .

Next, to prove  $\text{RHS} \subseteq \text{LHS}$ , let  $a \in \text{RHS}$ . If  $a \in A \setminus B$ , then  $a \in A = \text{LHS}$ . Else,  $a \in A \cap B$ , and thus  $a \in A = \text{LHS}$ . Thus,  $\text{RHS} \subseteq \text{LHS}$ . Since  $\text{LHS} \subseteq \text{RHS}$  and  $\text{RHS} \subseteq \text{LHS}$ ,  $\text{LHS} = \text{RHS}$ . ■

### 1.1.3 Indexed sets

Let  $I$  be a set. If for every  $i \in I$ , we have a set  $B_i$ , we say that we have a *collection* of sets  $B_i$  indexed by  $I$ . We write  $\{B_i : i \in I\}$ .

**Example 1.1.** Let  $I = \{1, 2, 3\}$ , and  $B_i = \{1, 2, 3, 4\} \setminus \{i\}$  ( $B_i$  is the set of all numbers from 1 to 4, excluding  $i$ ), for  $i \in I$ . We thus have  $B_1 = \{2, 3, 4\}$  (etc.).

This concept of indexing allows us to introduce repeated unions/intersections. For instance, we can write

$$\bigcup_{i \in I} B_i = B_1 \cup B_2 \cup B_3 = \{1, 2, 3, 4\}.$$

Similarly,

$$\bigcap_{i \in I} B_i = \{4\}.^1$$

<sup>1</sup>You can somewhat consider these “large” unions/intersections as analogous to summations  $\Sigma$  and products  $\Pi$ .

**Example 1.2.** Let  $I = \mathbb{R}$ , and  $B_i = [i, \infty] = \{r \in \mathbb{R} : r \geq i\}$ . Then,  $\bigcup_{i \in \mathbb{R}} B_i = \mathbb{R}$  and  $\bigcap_{i \in \mathbb{R}} B_i = \emptyset$ .

#### 1.1.4 Cartesian product

Let  $A_1, A_2, \dots, A_n$  be sets. We define the **Cartesian product**

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \dots, x_n) : x_i \in A_i, \text{ for } 1 \leq i \leq n\}.$$

For instance,

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

**Example 1.3.** Let  $A = B = \mathbb{R}$ .  $A \times B = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2$  is the set of all points in the Cartesian plane.

We can also define Cartesian products over an index set. Let  $I$  be an index set, with  $A_i$  for all  $i \in I$ . Then, we can write

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} : a_i \in A_i\}$$

**Example 1.4.**

$$I = \mathbb{N}, A_0 = \{0, 1, 2, \dots\}, A_1 = \{1, 2, 3, \dots\}, \dots, A_i = \{i, i+1, i+2, \dots\}$$

$$Y := \prod_{i \in I} A_i = \{(a_0, a_1, a_2, \dots) : a_i \in \mathbb{N}, a_i \geq i\}$$

We can say that a particular vector  $(b_0, b_1, \dots) \in Y$  if for each  $b_i$ ,  $b_i \geq i$  (and  $b_i \in \mathbb{N}$ , of course).

In other words, a particular item of the vector must be greater than or equal to its index. Thus, we can say

$$(0, 1, 2, 3, \dots) \in Y$$

while

$$(2, 2, 2, 2, \dots) \notin Y$$

since  $a_3 = 2 \implies i = 3$ , and  $2 \not\geq 3$ .

**1.2 Methods of Proof****1.2.1 Proving equality via two inequalities**

In short, say  $x, y \in \mathbb{R}$ .  $x = y \iff x \leq y$  and  $y \leq x$ . Similarly, in the context of sets, we can say that, for two sets  $X, Y$ ,  $X = Y \iff X \subseteq Y$  and  $Y \subseteq X$ .

**1.2.2 Contradiction (bwoc)**

Given a statement  $P$ , we can prove  $P$  true by assuming  $P$  false ( $\equiv \neg P$ ), then arriving to a contradiction (this contradiction is often a violated axiom or basic rule of the system at hand.)

**Example 1.5.** Show that there are no solutions to  $x^2 - y^2 = 1$  in the positive integers.

*Proof (bwoc).* Assume there are, so  $x, y \in \mathbb{Z}_+$ .<sup>2</sup> We can then write

$$1 = x^2 - y^2 = (x - y)(x + y).$$

$x - y$  and  $x + y$  must be integers, and so we have two cases,  $\begin{cases} x - y = 1 \\ x + y = 1 \end{cases}$  and

$\begin{cases} x - y = -1 \\ x + y = -1 \end{cases}$ . In either case,  $y$  must be zero, contradicting our initial assumption and thus proving the statement. ■

<sup>2</sup> $\mathbb{Z}_+$  is used to denote positive integers; similarly,  $\mathbb{Z}_-$  denotes negative integers.

### 1.2.3 Proving the contrapositive

Logically,  $A \implies B \iff \neg B \implies \neg A$ <sup>3</sup>.

**Example 1.6.** Let  $X, Y$  be sets. Prove  $X = X \setminus Y \implies X \cap Y = \emptyset$ .

*Proof.* Prove contrapositive:  $X \cap Y \neq \emptyset \implies X \neq X \setminus Y$ .  $X \cap Y \neq \emptyset \implies \exists t \in X \cap Y \implies t \in X$  and  $t \in Y$ , thus  $t \notin X \setminus Y$ , but  $t \in X$ , so  $X \neq X \setminus Y$ . ■

<sup>3</sup>“I am hungry therefore I will eat”  
 $\iff$  “I will *not* eat therefore I am *not* hungry.” Notice too that  $B$  need not imply  $A$  (“I will eat therefore I am hungry”). If  $A \implies B \iff B \implies A$ ,  $A \equiv B$

### 1.2.4 Induction

**Axiom 1.1** (Well-Ordering Principle). Every  $S \subseteq \mathbb{N}$ , where  $S \neq \emptyset$ , has a minimal element, ie  $\exists a \in S$  s.t.  $\forall b \in S, a \leq b$ .

**Theorem 1.1** (Principle of Induction). Let  $n_0 \in \mathbb{N}$ . Say that for every  $n \in \mathbb{Z}, n \geq n_0$ , we are given a statement  $P_n$ . Assume

(a)  $P_{n_0}$  is true

(b) if  $P_n$  is true, then  $P_{n+1}$  is true

then  $P_n$  is true for all  $n \geq n_0$ .

*Proof (bwoc).* Assume not.<sup>4</sup> Then, we define  $S = \{n \in \mathbb{N} : n \geq n_0, P_n \text{ false}\}$ . By the Well-Ordering Principle, there exists a minimal element  $a \in S$ . By definition,  $a \geq n_0$ , and as  $P_{n_0}$  is taken to be true, then  $a > n_0$  since  $n_0 \notin S$ . Thus,  $a - 1 \notin S$ , as  $a$  is the minimal element of  $S$ , and therefore  $P_{a-1}$  is true. However, by (b), this implies  $P_a$  is also true, and thus  $a \notin P$ , contradicting our initial assumption. ■

<sup>4</sup>note that (a) and (b) of the Principle of Induction are still taken to be true; it is simply the conclusion that is assumed to be false.

### 1.2.5 Pigeonhole principle

**Axiom 1.2.** If there are more pigeons than pigeonholes, then at least one pigeonhole must contain more than one pigeon.<sup>5</sup>

<sup>5</sup>Alternatively, you can consider fractional pigeons (though a little gruesome); given  $n + 1$  pigeons and  $n$  holes, each hole will contain, on average,  $1 + \frac{1}{n}$  pigeons.

**Example 1.7.** Consider  $n_1, \dots, n_6 \in \mathbb{N}$ . There exist at least two of these  $n$ 's s.t.  $n_i - n_j$  is evenly divisible by 5.

*Proof.* Let us rewrite each  $n_i$  as  $n_i = 5k_i + r_i$ , where  $k_i, r_i \in \mathbb{N}$ ,  $k_i$  is the quotient, and  $r_i$  is the residual.  $r_i \in \{0, 1, 2, 3, 4\}$  (the only possible remainders when a number is divided by 5), and so there are 5 possible values of  $r_i$ , but 6 different  $n_i$ . Thus, two  $n_i$  must have the same  $r_i$ , and we can write:

$$\begin{aligned} n_i &= 5k_i + r; n_j = 5k_j + r \\ n_i - n_j &= (5k_i + r) - (5k_j + r) \\ &= 5(k_i - k_j) \end{aligned}$$

$(k_i - k_j) \in \mathbb{Z}$ , and so  $n_i - n_j$  is evenly divisible by 5. ■

### 1.3 Functions

**Definition 1.3.1** (Function). Given 2 sets  $A, B$ , a function  $f : A \rightarrow B$  is a rule such that  $\forall a \in A, \exists! f(a) \in B$ , where  $\exists!$  denotes “there exists a unique”.

**Definition 1.3.2** (Graph). Given a function  $f : A \rightarrow B$ , a graph  $\Gamma_f = \{(a, f(a)) : a \in A\} \subseteq A \times B$ . We can say that,  $\forall a \in A, \exists! b \in B$  such that  $(a, b) \in \Gamma_f$ .

**Example 1.8.** Consider the Cartesian plane, denoted  $\mathbb{R}^2$ . It is simply a graph  $\Gamma_f$  where  $f : \mathbb{R} \rightarrow \mathbb{R}$  is the identity function,  $f(x) = x$ .

**Definition 1.3.3** (Injective). A function is an injection iff  $\forall a_1, a_2 \in A, f(a_1) = f(a_2) \implies a_1 = a_2$ .

**Definition 1.3.4** (Surjective). A function is a surjection iff  $\forall b \in B, \exists a \in A$  such that  $f(a) = b$ . In other words, every element of  $B$  is mapped to by at least one element of  $A$ ; you can pick any element in the range and it will have a preimage.

**Definition 1.3.5** (Bijective). Both.

**Definition 1.3.6** (Fibre). The fibre of some  $y \in Y$  is  $f^{-1}(y) = f^{-1}(y)$

**Definition 1.3.7** (Cardinality). *The cardinality of a set  $A$ , denoted  $|A|$ , is the number of elements in  $A$ , if  $A$  is finite, or a more abstract notion of size if  $A$  is infinite.*

We say that two sets  $A, B$  have the same cardinality ( $|A| = |B|$ ) if  $\exists$  a bijection  $f : A \rightarrow B$ .<sup>6</sup> This necessitates the question, however: if two sets are not equal in cardinality, how do we compare their sizes?

We write

$$|A| \leq |B| \iff \exists f : A \rightarrow B \text{ where } f \text{ is injective}$$

and

$$|A| \geq |B| \iff \exists f : A \rightarrow B \text{ where } f \text{ is surjective.}^7$$

Note that  $|B| \leq |A|$  if either  $A = \emptyset$  or, as above,  $\exists f : B \rightarrow A$  surjective.

**Definition 1.3.8** (Composition). *Given two functions  $f : A \rightarrow B, g : B \rightarrow C$ , the composition is the function  $g \circ f : A \rightarrow C$*

**Proposition 1.1.** *If  $|A| = |B|$  and  $|B| = |C|$  then  $|A| = |C|$*

*Proof.*  $\exists f : A \rightarrow B$  bijective, and  $\exists g : B \rightarrow C$  bijective. We desire to show that  $\exists h : A \rightarrow C$  that is bijective. We can write  $h = g \circ f$ , where  $h(a) = g(f(a))$ .

To show that  $h$  bijective:

- **injective:** Suppose  $h(a_1) = h(a_2)$ , then  $g(f(a_1)) = g(f(a_2))$ , and since  $g$  is injective,  $f(a_1) = f(a_2)$ . Since  $f$  is injective,  $a_1 = a_2$ , and thus  $h$  is injective.
- **surjective:** Let  $c \in C$ . Since  $g$  is surjective,  $\exists b \in B$  such that  $g(b) = c$ . Since  $f$  is surjective,  $\exists a \in A$  such that  $f(a) = b$ . Thus,  $h(a) = g(f(a)) = g(b) = c$ , and thus  $h$  is surjective.

Thus,  $h$  is bijective, and  $|A| = |C|$ . ■

**Lemma 1.2.** *If  $g \circ f$  injective,  $f$  injective. If  $g \circ f$  surjective,  $g$  surjective.*

**Definition 1.3.9** (Image). *The image of a function  $f : A \rightarrow B$  is the set  $Im(f) = \{f(a) : a \in A\}$ , ie the set of all elements in  $B$  that are mapped to by  $f$ . Note that  $Im(f) \subseteq B$ , and  $Im(f) = B$  if  $f$  is surjective.*

**Proposition 1.2.**  $|A| \leq |B|$  if  $|B| \geq |A|$

<sup>6</sup>Consider this in the finite case: a bijection indicates that all elements in the domain map uniquely to a single element in the range, and the range is completely “covered” by the function.

<sup>7</sup>Consider this intuitively; if your domain is smaller than your range, then you will “run out” of things to map from the domain to the range before you “run out” of things in the range, hence, you have a injection. Similarly, if your domain is larger than your range, then you will have “leftover” elements in the domain (that will map to “already mapped to” elements in the range), hence, you have a surjection.

*Proof.* If  $A = \emptyset$ ,  $|B| \geq |A|$  clearly.

If  $A \neq \emptyset$ , we are given  $\exists f : A \rightarrow B$  injective. Let us choose some  $a_0 \in A$ . We define  $g : B \rightarrow A$  as

$$g(b) = \begin{cases} a_0 & b \notin \text{Im}(f) \\ a & b = f(a) \in \text{Im}(f) \end{cases}^8$$

Note that  $g(f(a)) = g(b) = a$ , so  $g$  is surjective. Thus,  $|B| \geq |A|$ . ■

<sup>8</sup>Note that  $a$  is unique in  $A$ , as  $f$  is injective.

**Proposition 1.3.**  $|B| \geq |A|$  if  $|A| \leq |B|$

**Theorem 1.2** (Cantor-Bernstein Theorem).  $|A| \leq |B|$  and  $|B| \leq |A| \implies |A| = |B|$ .<sup>9</sup>

Equivalently, if  $\exists f : A \rightarrow B$  injective and  $\exists g : B \rightarrow A$  injective, then  $\exists h : A \rightarrow B$  bijective.

**Proposition 1.4.** If  $|A_1| = |A_2|$  and  $|B_1| = |B_2|$  then  $|A_1 \times B_1| = |A_2 \times B_2|$ .

*Proof.* The first two statements define bijections  $f : A_1 \rightarrow A_2$  and  $g : B_1 \rightarrow B_2$ , and we desire to have  $f \times g : A_1 \times B_1 \rightarrow A_2 \times B_2$ . We define  $f \times g(a_1, b_1) := (f(a_1), g(b_1))$ . We must show that  $f \times g$  is bijective. ■

**Example 1.9.** Consider  $A$  as the set of all points in the unit circle centered at  $(0, 0)$  in  $\mathbb{R}^2$ , and  $B$  as the set of all points in the square of side length 2 centered at  $(0, 0)$  in  $\mathbb{R}^2$  (ie, the circle is inscribed in the square). We wish to prove that  $|A| = |B|$ .

*Proof.* Let  $f : A \rightarrow B$ ,  $f(x) = x$ .  $f$  is injective, and thus  $|A| \leq |B|$ . Let  $g : A \rightarrow B$ ,

$$g(x) = \begin{cases} 0; \sqrt{2}x \notin B \\ \sqrt{2}x; \sqrt{2}x \in B \end{cases} \quad . \text{ In simpler terms, consider this as multiplying points of } A \text{ by}$$

$\sqrt{2}$ ; any point in this new “expanded” circle that lies within  $B$  maps to itself, and any that lies outside maps to 0. This is thus a surjection, and thus  $|B| \leq |A|$ . By the Cantor-Bernstein Theorem,  $|A| = |B|$ . ■

**Proposition 1.5.**  $A = \{0, 1, 4, 9, \dots\}$ .  $|A| = |\mathbb{N}|$ .

*Proof.* Define  $f : \mathbb{N} \rightarrow A$ ,  $f(n) = n^2$ . This is clearly injective<sup>10</sup>, and thus  $|A| \leq |\mathbb{N}|$ . ■

**Proposition 1.6.**  $B = \{p \in \mathbb{N} : p \text{ prime}\}$  is infinite ( $|B| = |\mathbb{N}|$ ).

*Proof (Euclid).* Let  $f : \mathbb{N} \rightarrow B$ ,  $f(n) =$  the  $n$ th prime. This is clearly bijective, and is an example of enumerating a set. ■

<sup>9</sup>It is often very difficult to define an arbitrary bijective function between two sets in order to prove their cardinality is equal. The Cantor-Bernstein Theorem allows us to prove that two sets have the same cardinality by proving that there exists an injection from  $A$  to  $B$  and an injection from  $B$  to  $A$ , which is typically far easier.

<sup>10</sup>Notice that  $f$  is only injective if we restrict the domain to  $\mathbb{N}$ ; if we were to consider  $\mathbb{Z}$ , for instance,  $f(-1) = f(1) = 1$ .



**Definition 1.3.10** (Countable/enumerable). A set  $A$  is countable if  $|A| = |\mathbb{N}|$ , or  $A$  is finite.

If  $A$  is finite of size  $n$ ,  $\exists$  a bijection  $f : \{0, 1, 2, \dots, n-1\} \rightarrow A$ .

If  $A$  is infinite,  $\exists$  a bijection  $f : \mathbb{N} \rightarrow A$ .

**Proposition 1.7.**  $|\mathbb{N}| = |\mathbb{Z}|$

*Proof.* We aim to find a bijection  $f : \mathbb{Z} \rightarrow \mathbb{N}$ , ie one that maps integers to natural numbers. Consider the function

$$f(x) = \begin{cases} 2x & x \geq 0 \\ -2x - 1 & x < 0 \end{cases}.$$

This function is an injection because if  $f(x_1) = f(x_2)$ , then  $x_1 = x_2$  (positive case:  $2x_1 = 2x_2 \implies x_1 = x_2$ , negative case:  $-2x_1 - 1 = -2x_2 - 1 \implies x_1 = x_2$ , and  $2x_1 \neq -2x_2 - 1$  for any integer). It is also a surjection (there is no natural number that cannot be mapped to by an integer). Thus, the function is a bijection and  $|\mathbb{N}| = |\mathbb{Z}|$ .<sup>11</sup> ■

<sup>11</sup>Note what would happen if  $f$  was defined as  $-2x$  for  $x < 0$ ; then,  $f$  would not be surjective (eg,  $f(-1) = 2 = f(1)$ .)

**Proposition 1.8.**  $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$

**Remark 1.1.** It is possible to construct a bijective  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ; see assignment 1.

*Proof.* Let  $f : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ ,  $f(n) = (n, 0)$ , clearly an injection ( $\implies |\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$ )<sup>12</sup>. The function  $g(m, n) = 2^n 3^m$  is also injective, and thus  $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$ . ■

<sup>12</sup>Note that this function is *not* surjective!

**Corollary 1.1.**  $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$

*Proof.* Consider  $h : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ , a bijection<sup>13</sup>, and  $f : \mathbb{N} \rightarrow \mathbb{Z}$ . Let  $g = (f, f) : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z} \times \mathbb{Z}$ . The composition  $g \circ h \circ f^{-1} : \mathbb{Z} \rightarrow \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z} \times \mathbb{Z}$  is also a bijection, and thus  $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$ . ■

<sup>13</sup>Which must exist by the proof of the previous proposition.

**Example 1.10.** Show that  $|\mathbb{N}| = |\mathbb{Q}|$ .

*Proof.* First, we find an injection  $\mathbb{Q} \rightarrow \mathbb{N}$ . Let  $f : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}$ ,  $f(n) = (p, q)$  where  $\frac{p}{q} = n$  (by definition of  $\mathbb{Q}$ ). Using the same function definitions as in Corollary 1.1, the composition  $h^{-1} \circ g^{-1} \circ f : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ . This is a composition of injections, and is thus an injection itself, and thus  $|\mathbb{Q}| \leq |\mathbb{N}|$ . The identity function  $1 : \mathbb{N} \rightarrow \mathbb{Q}$ ,  $1(n) = n$  is clearly an injection as well as all naturals are rationals, and thus  $|\mathbb{N}| \leq |\mathbb{Q}|$ . By the Cantor-Bernstein Theorem,  $|\mathbb{N}| = |\mathbb{Q}|$ . ■

**Definition 1.3.11.** We say  $|A| < |B|$  if  $|A| \leq |B|$  but  $|A| \neq |B|$ , ie  $\exists f : A \rightarrow B$  is injective, but no such bijective.

**Remark 1.2.** We denote an injective function as  $\mathbb{N} \hookrightarrow \mathbb{Z}$ , and a surjective function as  $\mathbb{Z} \twoheadrightarrow \mathbb{N}$ . We say that a particular element  $n$  maps to some other element  $n'$  by  $n \mapsto n'$

**Theorem 1.3 (Cantor).**  $|\mathbb{N}| < |\mathbb{R}|$

*Proof (Cantor's Diagonal Argument).* We clearly have an injection  $\mathbb{N} \hookrightarrow \mathbb{R}, n \mapsto n$ , thus  $|\mathbb{N}| \leq |\mathbb{R}|$ .

Now, suppose  $|\mathbb{N}| = |\mathbb{R}|$ . Then, we can enumerate the real numbers as  $a_0, a_1, \dots$  with signs  $\epsilon_i$ . We denote the decimal expansion of each number as<sup>14</sup>

$$a_0 = \epsilon_0 0.a_{00}a_{01}a_{02} \dots$$

$$a_1 = \epsilon_1 0.a_{10}a_{11}a_{12} \dots$$

$$a_2 = \epsilon_2 0.a_{20}a_{21}a_{22} \dots$$

$$\vdots$$

Consider the number  $0.e_0e_1e_2 \dots$ , where  $e_i = \begin{cases} 3 & a_{ii} \neq 3 \\ 4 & a_{ii} = 3 \end{cases}$ . This number is different than any given  $a_i$  at the  $i + 1$ -th decimal place, and is thus not in the enumeration, contradicting our initial assumption. ■

**Remark 1.3 (Continuum Hypothesis).** *Cantor claimed that there's no set  $|A|$  such that  $|\mathbb{N}| < |A| < |\mathbb{R}|$ . It has been proven today that this is “undecidable”.*

**Definition 1.3.12 (Algebra on Cardinalities).** *If  $\alpha, \beta$  are cardinalities  $\alpha = |A|, \beta = |B|$ ,*

*Cantor defined:*

$$\alpha + \beta = |A \sqcup B| \text{ (disjoint union)}$$

$$\alpha \cdot \beta = |A \times B|$$

$$\alpha^\beta = |B^A| \text{ (set of all functions from } A \text{ to } B)$$

<sup>14</sup>We make the clarification that, despite the fact that  $1.000 \dots = 0.999 \dots$ , we will take the “infinite zeroes” interpretation, and thus every real number has a unique decimal expansion. This is an important, if subtle, distinction.

## 1.4 Relations

**Definition 1.4.1 (Relation).** *A relation on a set  $A$  is a subset  $S \subseteq A \times A (= \{(x, y) : x, y \in A\})$ .*

*We say that  $x$  is related to  $y$  if  $(x, y) \in S$ , where we denote  $x \sim y$ .*

*Conversely, if we are given  $x \sim y$ , we can define an  $S = \{(x, y) : x \sim y\}$ .*

**Example 1.11.** Following are examples of relations on  $A$ .

- 1) Let  $S = A \times A$ ; any  $x \sim$  any  $y$  because  $(x, y) \in S$  for all  $(x, y)$ .
- 2) Let  $S = \emptyset$ ; no  $x \sim$  any  $y$  (even to itself).
- 3)  $S = \text{diag.} = \{(a, a) : a \in A\}$ ;  $x \sim x \forall x$ , but  $x \not\sim y$  if  $y \neq x$ .
- 4)  $A = [0, 1](\in \mathbb{R})$ . Say  $x \sim y$  if  $x \leq y$ . Thus,  $S = \{(x, y) : x \leq y\}$  (the diagonal, and everything above).
- 5)  $A = \mathbb{Z}$ ,  $x \sim y$  if  $5|(x - y)$ , ie  $x$  and  $y$  have same residue mod 5.<sup>15</sup>

<sup>15</sup>Where  $a|b$  denotes that  $b$  divides  $a$ .

**Definition 1.4.2 (Reflexive).** A relation is reflexive if for any  $x \in A$ ,  $x \sim x$ .

This includes examples 1), 2) (iff  $A$  is empty), 3), 4), and 5) above.

**Definition 1.4.3 (Symmetric).** A relation is symmetric if  $x \sim y \implies y \sim x$ .

This includes 1), 2), 3), and 5) above.

**Definition 1.4.4 (Transitive).** A relation is transitive if  $x \sim y$  and  $y \sim z$  implies  $x \sim z$ .

This includes 1), 2), 3), 4), and 5) above.

**Definition 1.4.5 (Partial Order).** A partial order on a set  $A$  is a relation  $x \sim y$  s.t.

1.  $x \sim x$  (reflexive)
2. if  $x \sim y$  and  $y \sim x$ ,  $x = y$  (antisymmetric)
3.  $x \sim y$  and  $y \sim z \implies x \sim z$  (transitive)

It is common to use  $\leq$  in place of  $\sim$  for partial orders.

We call a set on which a partial order exists a partially ordered set (poset).

This is called *partial*, as it is possible that for some  $x, y \in A$  we have  $x \not\sim y$  and  $y \not\sim x$ , ie  $x, y$  are not comparable. A partial order is called *linear/total* if for every  $x, y \in A$ , either  $x \leq y$  or  $y \leq x$ , eg.,  $A = [0, 1], \mathbb{R}, \mathbb{Z}, \dots$ , with  $x \leq y$ . Consider the above examples:

- 1) is not total, if  $A$  has at least two element, because  $\exists x \neq y$  but both  $x \sim y$  and  $y \sim x$ , and thus not antisymmetric.
- 3) yes
- 5) no, as this is symmetric, since  $5|(x - y) \implies 5|(y - x)$ , and thus  $x \sim y, y \sim x \not\implies y = x$

**Example 1.12.** Let<sup>16</sup>  $A = \mathbb{N}_+ = \{1, 2, 3, 4, \dots\}$ , and define  $a \sim b$  if  $a|b$ . We verify:

- $a \sim a$  (since  $a|a$ )
- $a \sim b, b \sim a \implies a = b$ , since in  $\mathbb{N}_+$ ,  $a|b \implies a \leq b$ , and we thus have  $a \leq b$  and  $b \leq a$ , and thus  $a = b$ .
- suppose  $a \sim b$  and  $b \sim c$ , then  $a|b$  and  $b|c$ . We can write  $b = a \cdot m$  and  $c = b \cdot n$  for  $n, m \in \mathbb{N}$ . This means that  $c = bn = amn = a(mn)$ , which means that  $a|c$ , so  $a \sim c$ .

Thus,  $A$  is a poset. Note that this is not a linear order, as  $2 \not\sim 3$ , and  $3 \not\sim 2$  (not all  $a, b$  are comparable).

<sup>16</sup>Try this with integers, see where it fails

**Definition 1.4.6** (Equivalence Relation). We aim to, abstractly, define some  $\sim$  such that if  $x \sim x, x \sim y$ , then  $y \sim x$ , and if  $x \sim y, y \sim z$ , then  $x \sim z$ .

Specifically, an equivalence relation  $\sim$  on the set  $A$  is a relation  $x \sim y$  s.t. it is

- reflexive;
- symmetric;
- transitive.<sup>17</sup>

<sup>17</sup>Note that, generally, equivalence and order relations are very different.

**Example 1.13.** 1. Let  $n \geq 1$  be an integer. A permutation  $\sigma$  of  $n$  elements is a bijection  $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ . Their number is  $n!$ , ie there are  $n!$  permutations of  $n$  elements. The collection of all permutations of  $n$  elements is denoted  $S_n$ , which we call the “symmetric group” on  $n$  elements. We aim to define an equivalence relation on  $S_n$ .

Let us define  $\sigma \sim \tau$  if  $\sigma(1) = \tau(1)$ . We verify that this is an equivalence relation:

- (a)  $\sigma \sim \sigma, \sigma(1) = \sigma(1)$ , so yes
- (b)  $\sigma \sim \tau$  means  $\sigma(1) = \tau(1)$ , so yes
- (c)  $\sigma \sim \tau, \tau \sim \rho, \sigma(1) = \tau(1), \tau(1) = \rho(1)$ , so  $\sigma(1) = \rho(1)$ , hence  $\sigma \sim \rho$ , so yes.

Thus,  $\sim$  is an equivalence relation on  $S_n$ .

**Example 1.14.** Define a relation on  $\mathbb{Z}$  by saying that  $x \sim y$  if  $x - y$  even, ie  $2|(x - y)$ . This is reflexive, as  $2|(x - x) = 0, x \sim x$ , symmetric, since  $(y - x) = -(x - y)$ , and transitive  $x - z = \underbrace{(x - y)}_{\text{even}} + \underbrace{(y - z)}_{\text{even}} \implies x \sim z$ .

## 1.5 Number Systems

**Definition 1.5.1** (Complex Numbers).  $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ . Equivalently, we can consider complex numbers as the points  $(a, b) \in \mathbb{R}^2$ .<sup>18</sup>

Given some  $z = a + bi$ , we can write  $\operatorname{Re}(z) = a$ ,  $\operatorname{Im}(z) = b$ .

**Definition 1.5.2** (Complex Conjugate). Given  $z = a + bi$ , the complex conjugate of  $z$  is  $\bar{z} = a - bi$ .

**Lemma 1.3.** The following hold for complex conjugates:<sup>19</sup>

(a)  $\bar{\bar{z}} = z$ .

(b)  $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$ ,  $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$ .

(c)  $\operatorname{Re}(z) = \frac{z + \bar{z}}{2}$ ,  $\operatorname{Im}(z) i = \frac{z - \bar{z}}{2}$ .

(d) Given  $|z| = \sqrt{a^2 + b^2}$ ,

(i)  $|z|^2 = z \cdot \bar{z}$

(ii)  $|z_1 + z_2| \leq |z_1| + |z_2|$

(iii)  $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

<sup>18</sup>We can define the function  $f : \mathbb{C} \rightarrow \mathbb{R}^2$ ,  $f(a + bi) = (a, b)$ , a bijection.

<sup>19</sup>(a), (b), and (c) are simply algebraic rearrangements of two complex numbers. (d.i) and (d.iii) follow from similar arguments, and finally (ii) is the triangle inequality restated in terms of complex numbers.

## 2 Appendix