

Contents

<b>1</b>	<b>Logic, Sets, and Functions</b>	<b>2</b>
1.1	Mathematical Induction & The Naturals . . . . .	2
1.2	Extensions: Integers, Rationals, Reals . . . . .	4
<b>2</b>	<b>Appendix</b>	<b>5</b>

# 1 Logic, Sets, and Functions

## 1.1 Mathematical Induction & The Naturals

The **natural numbers**,  $\mathbb{N} = \{1, 2, 3, \dots\}$ , are specified by the 5 **Peano Axioms**:

- (1)  $1 \in \mathbb{N}$ <sup>1</sup>
- (2) every natural number has a successor in  $\mathbb{N}$
- (3) 1 is not the successor of any natural number
- (4) if the successor of  $x$  is equal to the successor of  $y$ , then  $x$  is equal to  $y$ <sup>2</sup>
- (5) **the axiom of induction**

The **Axiom of Induction** (AI), can be stated in a number of ways.

### Axiom 1.1 (AI.i)

Let  $S \subseteq \mathbb{N}$  with the properties:

- (a)  $1 \in S$
- (b) if  $n \in S$ , then  $n + 1 \in S$ <sup>3</sup>

then  $S = \mathbb{N}$ .

**Example 1.1.** Prove that, for every  $n \in \mathbb{N}$ ,  $1 + 2 + \dots + n = \frac{n(n+1)}{2} (\equiv (1))$

**Proof (via AI.i):** Let  $S$  be the subset of  $\mathbb{N}$  for which (1) holds; thus, our goal is to show  $S = \mathbb{N}$ , and we must prove (a) and (b) of AI.i.

- by inspection,  $1 \in S$  since  $1 = \frac{1(1+1)}{2} = 1$ , proving (a)
- assume  $n \in S$ ; then,  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$  by definition of  $S$ . Adding  $n + 1$  to both sides yields:

$$1 + 2 + \dots + n + (n + 1) = \frac{n(n + 1)}{2} + (n + 1) \quad (1)$$

$$= (n + 1)\left(\frac{n}{2} + 1\right) \quad (2)$$

$$= \frac{(n + 1)(n + 2)}{2} \quad (3)$$

$$= \frac{(n + 1)((n + 1) + 1)}{2} \quad (4)$$

---

<sup>1</sup>using 0 instead of 1 is also valid, but we will use 1 here.

<sup>2</sup>axioms (2)-(4) can be equivalently stated in terms of a successor function  $s(n)$  more rigorously, but won't here

<sup>3</sup>(a) is called the **inductive base**; (b) the **inductive step**. All AI restatements are equivalent in having both of these, and only differentiate on their specific values.

Line (4) is equivalent to statement (1) (substituting  $n$  for  $n + 1$ ), and thus if  $n \in S$ , then  $n + 1 \in S$  and (b) holds.

Thus, by A.I.i,  $S = \mathbb{N}$  and  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$  holds  $\forall n \in \mathbb{N}$ . ■

**Exercise 1.1.** Prove (by induction), that for every  $n \in \mathbb{N}$ ,  $1^3 + 2^3 + \dots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2$ .

(Solution)

Example 1.1 can also be proven directly (Gauss' method).

**Proof:** Let  $A(n) = 1 + 2 + 3 + \dots + n$ . We can write  $2 \cdot A(n) = 1 + 2 + 3 + \dots + n + 1 + 2 + 3 + \dots + n$ . Rearranging terms (1 with  $n$ , 2 with  $n - 1$ , etc.), we can say  $2 \cdot A(n) = (n + 1) + (n + 1) + \dots$ , where  $(n + 1)$  is repeated  $n$  times; thus,  $2 \cdot A(n) = n(n + 1)$ , and  $A(n) = \frac{n(n+1)}{2}$ . ■

### Axiom 1.2 (A.I.ii)

Let  $S \subseteq \mathbb{N}$  s.t.

(a)  $m \in S$

(b)  $n \in S \implies n + 1 \in S$

then  $\{m, m + 1, m + 2, \dots\} \subseteq S$ .

**Exercise 1.2.** Using A.I.ii, prove that for  $n \geq 2$ ,  $n^2 > n + 1$

(Solution)

### Axiom 1.3 (Principle of Complete Induction, A.I.iii)

Let  $S \subseteq \mathbb{N}$  s.t.

(a)  $1 \in S$

(b) if  $1, 2, \dots, n - 1 \in S$ , then  $n \in S$

then  $S = \mathbb{N}$ .

Finally, combining A.I.ii and A.I.iii;

### Axiom 1.4 (A.I.iv)

Let  $S \subseteq \mathbb{N}$  s.t.:

(a)  $m \in S$

(b) if  $m, m + 1, \dots, m + n \in S$ , then  $m + n + 1 \in S$

then  $\{m, m + 1, m + 2, \dots\} \subseteq S$ .

### Theorem 1.1 (Fundamental Theorem of Arithmetic)

Every natural number  $n$  can be written as a product of one or more primes.<sup>4</sup>

**Proof:** Let  $S$  be the set of all natural numbers that can be written as a product of one or more primes. We will use A.I.iv to show  $S = \{2, 3, \dots\}$ .

- (a) holds; 2 is prime and thus  $2 \in S$
- suppose that  $2, 3, \dots, 2 + n \in S$ . Consider  $2 + (n + 1)$ :

---

<sup>4</sup>1 is not a prime number

- if  $2 + (n + 1)$  is *prime*, then  $2 + (n + 1) \in S$ , as all primes are products of 1 and themselves and are thus in  $S$  by definition.
- if  $2 + (n + 1)$  is *not prime*, then it can be written as  $2 + (n + 1) = a \cdot b$  where  $a, b \in \mathbb{N}$ , and  $1 < a < 2 + (n + 1)$  and  $1 < b < 2 + (n + 1)$ . By the definition of  $S$ ,  $a, b \in S$ , and can thus be written as the product of primes. Let  $a = p_1 \cdot \dots \cdot p_l$  and  $b = q_1 \cdot \dots \cdot q_j$ , where the  $p$ 's and  $q$ 's are prime and  $l, j \geq 1$ . Then,  $a \cdot b$  is a product of primes, and thus so is  $2 + (n + 1)$ . Thus,  $2 + (n + 1) \in S$ , and by Al.iv,  $S = \{2, 3, 4, \dots\}$  ■

## 1.2 Extensions: Integers, Rationals, Reals

Consider the set of naturals  $\mathbb{N} = \{1, 2, 3, \dots\}$ . Adding 0 to  $\mathbb{N}$  defines  $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ . We define the **integers** as the set  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ , or the set of all positive and negative whole numbers.

Within  $\mathbb{Z}$ , we can define multiplication, addition and subtraction, with the naturals of 1 and 0, respectively. However, we cannot define division, as we are not guaranteed a quotient in  $\mathbb{Z}$ . This necessitates the **rationals**,  $\mathbb{Q}$ . We define

$$\mathbb{Q} = \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0 \right\}.$$

On  $\mathbb{Q}$ , we have the familiar operations of multiplication, addition, subtraction and properties of associativity, distributivity, etc. We can also define division, as  $\frac{\frac{p}{q}}{\frac{p'}{q'}} = \frac{pq'}{qp'}$ .

We can also define a relation  $<$  between fractions, such that

- $x < y$  and  $y < z \implies x < z$
- $x < y \implies x + z < y + z$

$\mathbb{Q}$ , together with its operations and relations above, is called an **ordered field**.

## 2 Appendix

### Axiom 1.1 (AI.i)

Let  $S \subseteq \mathbb{N}$  with the properties:

(a)  $1 \in S$

(b) if  $n \in S$ , then  $n + 1 \in S$

then  $S = \mathbb{N}$ .

**Exercise 1.1.** Prove (by induction), that for every  $n \in \mathbb{N}$ ,  $1^3 + 2^3 + \dots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2$ .

**Proof of Exercise 1.1:** Follows a similar structure to the previous example. Let  $S$  be the subset of  $\mathbb{N}$  for which the statement holds.  $1 \in S$  by inspection ((a) holds), and we prove (b) by assuming  $n \in S$  and showing  $n + 1 \in S$  (algebraically). Thus, by AI.i,  $S = \mathbb{N}$  and the statement holds  $\forall n \in \mathbb{N}$ . ■

### Axiom 1.2 (AI.ii)

Let  $S \subseteq \mathbb{N}$  s.t.

(a)  $m \in S$

(b)  $n \in S \implies n + 1 \in S$

then  $\{m, m + 1, m + 2, \dots\} \subseteq S$ .

**Exercise 1.2.** Using AI.ii, prove that for  $n \geq 2$ ,  $n^2 > n + 1$

**Proof of Exercise 1.2:** Again, very similar to the previous induction examples. Take  $S$  to be the subset of  $\mathbb{N}$  for which the statement holds. (a) of AI.ii holds by inspection (where  $m = 2$ ), and (b) holds by assuming  $n \in S$  and showing that  $n + 1 \in S$ . Thus,  $S = \{2, 3, 4, \dots\}$ , and the statement holds  $\forall n \geq 2$ .

### Axiom 1.3 (Principle of Complete Induction, AI.iii)

Let  $S \subseteq \mathbb{N}$  s.t.

(a)  $1 \in S$

(b) if  $1, 2, \dots, n - 1 \in S$ , then  $n \in S$

then  $S = \mathbb{N}$ .

### Axiom 1.4 (AI.iv)

Let  $S \subseteq \mathbb{N}$  s.t.:

(a)  $m \in S$

(b) if  $m, m + 1, \dots, m + n \in S$ , then  $m + n + 1 \in S$

then  $\{m, m + 1, m + 2, \dots\} \subseteq S$ .

**Theorem 1.1 (*Fundamental Theorem of Arithmetic*)**

*Every natural number  $n$  can be written as a product of one or more primes.* <sup>6</sup>