THE INTEGERS

1. Axioms of the Integers

The set of integers, denoted $\mathbb{Z}$, has the following properties:

1. **(Operations)** There are binary operations $+$ (addition) and $\cdot$ (multiplication), which take pairs of elements of $\mathbb{Z}$ to elements of $\mathbb{Z}$,
2. **(Commutativity)** For all $a, b \in \mathbb{Z}$,
$$a + b = b + a \qquad \text{and} \qquad a \cdot b = b \cdot a.$$
3. **(Associativity)** For all $a, b, c \in \mathbb{Z}$,
$$a + (b + c) = (a + b) + c \qquad \text{and} \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
4. **(Distributive Law)** For all $a, b, c \in \mathbb{Z}$,
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$
5. **(Identity)** There are elements $0, 1 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$,
$$a + 0 = a \qquad \text{and} \qquad a \cdot 1 = a.$$
Moreover, $0 \neq 1$.
6. **(Additive Inverses)** For each $a \in \mathbb{Z}$, there exists $-a \in \mathbb{Z}$ such that
$$a + (-a) = 0.$$
We write $b - a$ to mean $b + (-a)$.
7. **(Positive Integers)** There is a subset $\mathbb{N}$ of $\mathbb{Z}$ which we call the **positive integers**. We write $a < b$ when $b - a \in \mathbb{N}$.
8. **(Positive Closure)** For all $a, b \in \mathbb{N}$,
$$a + b \in \mathbb{N} \qquad \text{and} \qquad a \cdot b \in \mathbb{N}.$$
9. **(Trichotomy)** For every $a \in \mathbb{Z}$, exactly one of the the following is true:
   (i) $a \in \mathbb{N}$, or
   (ii) $a = 0$, or
   (iii) $-a \in \mathbb{N}$.
10. **(Well-Ordering)** Every non-empty subset of $\mathbb{N}$ has a smallest element.

These properties are **axioms**, meaning that we declare them to be true without proof.

2. Basic consequences of the axioms

The following lemmas are direct consequences of the axioms.

Lemma 1 (Additive Cancellation Property)**.** *For any $a, b, c \in \mathbb{Z}$, if $a + b = a + c$, then $b = c$.*

Proof. Let $a, b, c \in \mathbb{Z}$ and suppose $a + b = a + c$. We add the additive inverse $-a$ to both sides of this equation to get

$$-a + (a + b) = -a + (a + c).$$

By the Associativity axiom, we may rewrite this as

$$(-a + a) + b = (-a + a) + c.$$

By the Commutativity and Additive Inverses axioms, $-a + a = a + (-a) = 0$. Thus, we have

$$0 + b = 0 + c.$$

Finally, $0 + b = b$ and $0 + c = c$ by the Identity axiom. We conclude that $b = c$. □

Lemma 2 (Uniqueness of Additive Inverses)**.** *For any $a, b \in \mathbb{Z}$, if $a + b = 0$, then $b = -a$.*

Proof. Let $a, b \in \mathbb{Z}$ and suppose $a+b = 0$. We also know that $a+(-a) = 0$ by the Additive Inverses axiom. Thus,

$$a + b = a + (-a).$$

Applying the Additive Cancellation Property, we conclude $b = -a$. □

Lemma 3. *For any $a \in \mathbb{Z}$, $a \cdot 0 = 0$.*

Proof. Let $a \in \mathbb{Z}$. By the Identity axiom, $0 = 0 + 0$. Multiplying this equation by a and applying the Distributive Law gives

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

We also have $a \cdot 0 = a \cdot 0 + 0$ by the Identity axiom, so

$$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0.$$

Now, by the Additive Cancellation Property, we get $a \cdot 0 = 0$. □

Lemma 4. *For any $a \in \mathbb{Z}$, $-(-a) = a$.*

Proof. Left as an exercise.

□

Exercise 1. Prove Lemma 4 using the Additive Inverses axiom and Lemma 2.

Lemma 5. *For any $a \in \mathbb{Z}$, $-a = (-1) \cdot a$.*

Proof. Let $a \in \mathbb{Z}$. By the Identity axiom, we have $a = 1 \cdot a$. Therefore,

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a.$$

By the Distributive Law,

$$1 \cdot a + (-1) \cdot a = \big(1 + (-1)\big) \cdot a = 0 \cdot a.$$

Since $0 \cdot a = 0$ by Lemma 3, we may combine these equalities to obtain $a + (-1) \cdot a = 0$. By Lemma 2, we get $(-1) \cdot a = -a$. □

Lemma 6. *The multiplicative identity* 1 *is an element of* $\mathbb{N}$.

Proof. By the Trichotomy axiom, exactly one of the following possibilities holds: $1 \in \mathbb{N}$, $1 = 0$, or $-1 \in \mathbb{N}$. We cannot have $1 = 0$, because this would violate the Identity axiom. Thus, it suffices to show that $-1 \notin \mathbb{N}$.

Assume, by way of contradiction, that $-1 \in \mathbb{N}$. Then by the Positive Closure axiom, we have $(-1) \cdot (-1) \in \mathbb{N}$. Now, by Lemma 5, $(-1) \cdot (-1) = -(-1)$. By Lemma 4, $-(-1) = 1$. Thus, we see that the assumption that $-1 \in \mathbb{N}$ implies that $1 \in \mathbb{N}$ as well, which violates the Trichotomy axiom; we cannot have both $1 \in \mathbb{N}$ and $-1 \in \mathbb{N}$. This contradiction shows that we cannot have $-1 \in \mathbb{N}$. □

Lemma 7. *For any* $a, b \in \mathbb{Z}$, *if* $a \cdot b = 0$, *then* $a = 0$ *or* $b = 0$.

Proof. Left as an exercise.

□

Exercise 2. Prove Lemma 7. You may use only the axioms for the integers and Lemmas 1 through 6. [HINT: Prove the contrapositive statement. If an integer x is not zero, then by the Trichotomy axiom, either $x \in \mathbb{N}$ or $-x \in \mathbb{N}$. Now, consider cases and use the Positive Closure axiom.]

Theorem 8 (Multiplicative Cancellation Property)**.** *For any* $a, b, c \in \mathbb{Z}$ *with* $a \neq 0$, *if* $a \cdot b = a \cdot c$, *then* $b = c$.

Proof. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Suppose that $a \cdot b = a \cdot c$. Then $a \cdot b - a \cdot c = 0$. By the Distributive Law, we may rewrite this as

$$a \cdot (b - c) = 0.$$

By Lemma 7, we have $a = 0$ or $b - c = 0$. But $a \neq 0$, so it must be true that $b - c = 0$. Therefore, $b = c$. □

3. Order Properties of the Integers

Recall that, for integers $a, b \in \mathbb{Z}$, we defined $a < b$ to mean $b - a \in \mathbb{N}$. In particular, $0 < b$ is equivalent to $b \in \mathbb{N}$. We shall write $a \leq b$ to mean $a = b$ or $a < b$.

Here we establish some basic properties of inequalities.

Lemma 9. *For any* $a, b \in \mathbb{Z}$, *exactly one of the following is true:*

(i) $a < b$, *or*
(ii) $a = b$, *or*
(iii) $b < a$.

Proof. Left as an exercise. □

Exercise 3. Prove Lemma 9. [HINT: You will need to use the Trichotomy axiom, the Distributive Law, and Lemmas 4 and 5.]

Lemma 10. *Let $a, b, c \in \mathbb{Z}$.*

1. *If $a < b$, then $a + c < b + c$.*
2. *If $a < b$ and $0 < c$, then $a \cdot c < b \cdot c$.*

Proof. First, suppose $a < b$. Then $b - a \in \mathbb{N}$. Therefore, $(b + c) - (a + c) = b - a$ is an element of $\mathbb{N}$. By the definition of inequality, we have $a + c < b + c$.

To prove the second statement, suppose $a < b$ and $0 < c$. Then $b - a$ and c are both elements of $\mathbb{N}$. By the Positive Closure axiom, $(b - a)c \in \mathbb{N}$. By the Distributive Law, $bc - ac \in \mathbb{N}$. Now, by the definition of inequality, we have $ac < bc$. □

Theorem 11. *The integer 1 is the smallest element of $\mathbb{N}$.*

Proof. By the Well-Ordering axiom, $\mathbb{N}$ does in fact have a smallest element. Let $a \in \mathbb{N}$ be this smallest element, so that $a \leq n$ for every $n \in \mathbb{N}$. In particular, $a \leq 1$, so we must have $a < 1$ or $a = 1$. If $a = 1$, then we are done.

Assume, for the sake of contradiction, that $a < 1$. Because $a = a - 0 \in \mathbb{N}$, we have $0 < a$. Thus, by Lemma 10, we may multiply the inequality $a < 1$ by the positive integer a to get

$$a \cdot a < 1 \cdot a.$$

Therefore, $a \cdot a < a$ by the Identity axiom. Since $a \in \mathbb{N}$, we also have $a \cdot a \in \mathbb{N}$ by the Positive Closure axiom. That is, $a \cdot a$ is an element of $\mathbb{N}$ which is smaller than a. This contradicts the fact that a is the smallest element of $\mathbb{N}$, and so $a < 1$ cannot be true. □

4. The Principle of Mathematical Induction

The **Principle of Mathematical Induction** says the following: Let S be a subset of $\mathbb{N}$. If both statements

1. **(Base Case)** $1 \in S$, and
2. **(Inductive Step)** For all $n \in \mathbb{N}$, if $n \in S$ then $n + 1 \in S$

are true, then $S = \mathbb{N}$. In propositional logic, the Principle of Mathematical Induction is the conditional sentence

$$(1 \in S) \wedge \big[(\forall n \in \mathbb{N})\big((n \in S) \Rightarrow (n + 1 \in S)\big)\big] \implies (S = \mathbb{N}).$$

In class, we let S be the set of natural numbers for which some sentence $P(n)$ is true. The Principle of Mathematical Induction then provides a method for showing that $P(n)$ is true for all $n \in \mathbb{N}$.

Note that we did not *prove* the Principle of Mathematical Induction. Rather, we appealed to our intuition to explain why it is reasonable to believe. Here, we show that the Principle of Mathematical Induction follows from the axioms of the integers.

Theorem 12. *The Principle of Mathematical Induction is true.*

Proof. Let S be a subset of $\mathbb{N}$, and suppose both hypotheses of the Principle of Mathematical Induction (the Base Case and the Inductive Step) are true. We must show that $S = \mathbb{N}$.

Assume, for the sake of contradiction, that $S \neq \mathbb{N}$, and let T be the set of all positive integers which are *not* in S. Because $S \neq \mathbb{N}$, we know that T is non-empty. By the Well-Ordering axiom, there is a smallest element $n_0 \in T$. That is, n_0 is the smallest positive integer which is not in S.

Observe that $n_0 \neq 1$, because $1 \in A$ by the Base Case. Therefore, $n_0 > 1$ by Theorem 11. Thus, $n_0 - 1 \in \mathbb{N}$ by our definition of inequalities. Moreover, $n_0 - 1 < n_0$, so because n_0 is the smallest positive number not in S, we must have $n_0 - 1 \in S$.

But now, since $n_0 - 1 \in S$, the Inductive Step implies that $(n_0 - 1) + 1 = n_0 \in S$, which is a contradiction. Therefore, our assumption that $S \neq \mathbb{N}$ must be false. □

Remark. Essentially, the Principle of Mathematical Induction says that $\mathbb{N}$ (which *a priori* is only defined by axioms 7–10) is the familiar set of natural numbers. We know by Theorem 11 that 1 is the smallest element of $\mathbb{N}$. Then $2 = 1 + 1 \in \mathbb{N}$ by the Positive Closure axiom, and $3 = 2 + 1 \in \mathbb{N}$ by Positive Closure again, and so on. The Principle of Mathematical Induction says that we will generate all of $\mathbb{N}$ in this way, i.e.,

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Remark. It turns out that the Principle of Mathematical Induction is *equivalent* to the Well-Ordering Principle, in that the Principle of Mathematical Induction can replace Well-Ordering as the 10th axiom of the integers. To see this, one needs to *prove* that the Well-Ordering Principle is true if we assume the Principle of Mathematical Induction and the other axioms of the integers. This is not especially difficult, but we will not do it here.