Properties of the Integers

The set of all integers is the set
\[ \mathbb{Z} = \{ \cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots \}, \]
and the subset of \( \mathbb{Z} \) given by
\[ \mathbb{N} = \{ 0, 1, 2, 3, 4, \cdots \}, \]
is the set of nonnegative integers (also called the natural numbers or the counting numbers).

We assume that the notions of addition (+) and multiplication (\( \cdot \)) of integers have been defined, and note that \( \mathbb{Z} \) with these two binary operations satisfy the following.

Axioms for Integers

- **Closure Laws:** if \( a, b \in \mathbb{Z} \), then
  \[ a + b \in \mathbb{Z} \quad \text{and} \quad a \cdot b \in \mathbb{Z}. \]

- **Commutative Laws:** if \( a, b \in \mathbb{Z} \), then
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a. \]

- **Associative Laws:** if \( a, b, c \in \mathbb{Z} \), then
  \[ (a + b) + c = a + (b + c) \quad \text{and} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c). \]

- **Distributive Law:** if \( a, b, c \in \mathbb{Z} \), then
  \[ a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c. \]

- **Identity Elements:** There exist integers 0 and 1 in \( \mathbb{Z} \), with \( 1 \neq 0 \), such that
  \[ a + 0 = 0 + a = a \quad \text{and} \quad a \cdot 1 = 1 \cdot a = a \]
  for all \( a \in \mathbb{Z} \).

- **Additive Inverse:** For each \( a \in \mathbb{Z} \), there is an \( x \in \mathbb{Z} \) such that
  \[ a + x = x + a = 0, \]
  \( x \) is called the additive inverse of \( a \) or the negative of \( a \), and is denoted by \( -a \).

The set \( \mathbb{Z} \) together with the operations of + and \( \cdot \) satisfying these axioms is called a commutative ring with identity.
We can now prove the following results concerning the integers.

**Theorem.** For any \( a \in \mathbb{Z} \), we have \( 0 \cdot a = a \cdot 0 = 0 \).

**Proof.** We start with the fact that \( 0 + 0 = 0 \). Multiplying by \( a \), we have \( a \cdot (0 + 0) = a \cdot 0 \) and from the distributive law we have, \( a \cdot 0 + a \cdot 0 = a \cdot 0 \).

If \( b = -(a \cdot 0) \), then \( (a \cdot 0 + a \cdot 0) + b = a \cdot 0 + b = 0 \), and from the associative law, \( a \cdot 0 + (a \cdot 0 + b) = 0 \), that is, \( a \cdot 0 + 0 = 0 \), and finally, \( a \cdot 0 = 0 \).

**Theorem.** For any \( a \in \mathbb{Z} \), we have \(-a = (-1) \cdot a\).

**Proof.** Let \( a \in \mathbb{Z} \), then \( 0 = 0 \cdot a = [1 + (-1)] \cdot a = 1 \cdot a + (-1) \cdot a \), so that \( -a + 0 = -a + (a + (-1) \cdot a) \), that is, \( -a = (-a + a) + (-1) \cdot a \), that is, \( -a = 0 + (-1) \cdot a \), and finally, \( -a = (-1) \cdot a \).

**Theorem.** \((-1) \cdot (-1) = 1\).

**Proof.** We have \( (-1) \cdot (-1) + (-1) = (-1) \cdot (-1) + (-1) \cdot 1 = (-1) \cdot [(-1) + 1] = (-1) \cdot 0 = 0 \), so that \( [(-1) \cdot (-1) + (-1)] + 1 = 0 + 1 = 1 \), that is, \( (-1) \cdot (-1) + [(-1) + 1] = 1 \), or, \( (-1) \cdot (-1) + 0 = 1 \). Therefore, \((-1) \cdot (-1) = 1\).
We can define an ordering on the set of integers \( \mathbb{Z} \) using the set of positive integers \( \mathbb{N}^+ = \{1, 2, 3, \ldots\} \).

**Definition.** If \( a, b \in \mathbb{Z} \), then we define \( a < b \) if and only if \( b - a \in \mathbb{N}^+ \).

**Note:** By \( b - a \) we mean \( b + (-a) \), and if \( a < b \) we also write \( b > a \). Also, we note that \( a \) is a positive integer if and only if \( a > 0 \) if and only if \( a = a - 0 \in \mathbb{N}^+ \).

**Order Axioms for the Integers**

- **Closure Axioms for \( \mathbb{N}^+ \):** If \( a, b \in \mathbb{N}^+ \), then

  \[ a + b \in \mathbb{N}^+ \quad \text{and} \quad a \cdot b \in \mathbb{N}^+. \]

- **Law of Trichotomy:** For every integer \( a \in \mathbb{Z} \), exactly one of the following is true:

  \[ a \in \mathbb{N}^+ \quad \text{or} \quad -a \in \mathbb{N}^+ \quad \text{or} \quad a = 0. \]

**Exercise.** Use the Law of Trichotomy together with the fact that \((-1) \cdot (-1) = 1\) to show that \( 1 > 0 \).

**Definition.** We say that an integer \( a \) is a **zero divisor** or **divisor of zero** if and only if \( a \neq 0 \) and there exists an integer \( b \neq 0 \) such that \( a \cdot b = 0 \).

Now we can show that \( \mathbb{Z} \) with the usual notion of addition and multiplication has no zero divisors.

**Theorem.** If \( a, b \in \mathbb{Z} \) and \( a \cdot b = 0 \), then either \( a = 0 \) or \( b = 0 \).

**Proof.** Suppose that \( a, b \in \mathbb{Z} \) and \( a \cdot b = 0 \). If \( a \neq 0 \) and \( b \neq 0 \), since

\[ a \cdot b = (-a) \cdot (-b) \quad \text{and} \quad -a \cdot b = (-a) \cdot b = a \cdot (-b), \]

by considering all possible cases, the fact that \( \mathbb{N}^+ \) is closed under multiplication and the Law of Trichotomy imply that \( a \cdot b \neq 0 \), which is a contradiction. Therefore, if \( a \cdot b = 0 \), then either \( a = 0 \) or \( b = 0 \). \(\square\)

Thus, \( \mathbb{Z} \) with the usual notion of addition and multiplication is a commutative ring with identity which has no zero divisors, such a structure is called an **integral domain**, and we have the following result.

**Theorem. (Cancellation Law)** If \( a, b, c \in \mathbb{Z} \) with \( c \neq 0 \), and if \( a \cdot c = b \cdot c \), then \( a = b \).

**Proof.** If \( a \cdot c = b \cdot c \), then \((a - b) \cdot c = 0\), and since \( c \neq 0 \), then \( a - b = 0 \). \(\square\)
Exercise. Show that the relation on \( \mathbb{Z} \) defined by \( a \leq b \) if and only if \( a < b \) or \( a = b \), is a partial ordering, that is, it is

- **Reflexive:** For each \( a \in \mathbb{Z} \), we have \( a \leq a \).

- **Antisymmetric:** For each \( a, b \in \mathbb{Z} \), if \( a \leq b \) and \( b \leq a \), then \( a = b \).

- **Transitive:** For each \( a, b, c \in \mathbb{Z} \), if \( a \leq b \) and \( b \leq c \), then \( a \leq c \).

Show also that this is a total ordering, that is, for any \( a, b \in \mathbb{Z} \), either \( a \leq b \) or \( b \leq a \).

We have the standard results concerning the order relation on \( \mathbb{Z} \). We will prove (ii), (iv), and (v), and leave the rest as exercises.

**Theorem.** If \( a, b, c, d \in \mathbb{Z} \), then

(i) if \( a < b \), then \( a + c \leq b + c \).

(ii) If \( a < b \) and \( c > 0 \), then \( a \cdot c < b \cdot c \).

(iii) If \( a < b \) and \( c < 0 \), then \( a \cdot c > b \cdot c \).

(iv) If \( 0 < a < b \) and \( 0 < c < d \), then \( a \cdot c < b \cdot d \).

(v) If \( a \in \mathbb{Z} \) and \( a \neq 0 \), then \( a^2 > 0 \). In particular, \( 1 > 0 \).

**Proof.**

(ii) If \( a < b \) and \( c > 0 \), then \( b - a > 0 \) and \( c > 0 \), so that \((b - a) \cdot c > 0\), that is, \( b \cdot c - a \cdot c > 0 \). Therefore, \( a \cdot c < b \cdot c \).

(iv) We have

\[
 b \cdot d - a \cdot c = b \cdot d - b \cdot c + b \cdot c - a \cdot c = b \cdot (d - c) + c \cdot (b - a) > 0
\]

since \( b > 0 \), \( c > 0 \), \( d - c > 0 \), and \( b - a > 0 \).

(v) Let \( a \in \mathbb{Z} \), if \( a > 0 \), then (ii) implies that \( a \cdot a > a \cdot 0 \), that is, \( a^2 > 0 \).

If \( a < 0 \), then \( -a > 0 \), and (ii) implies that \( a^2 = (-a) \cdot (-a) > 0 \). Finally, since \( 1 \neq 0 \), then \( 1 = 1^2 > 0 \).

**Exercise.** Show that if \( a, b, c \in \mathbb{Z} \) and \( a \cdot b < a \cdot c \) and \( a > 0 \), then \( b < c \).
Finally, we need one more axiom for the set of integers.

**Well-Ordering Axiom for the Integers** If $B$ is a nonempty subset of $\mathbb{Z}$ which is bounded below, that is, there exists an $n \in \mathbb{Z}$ such that $n \leq b$ for all $b \in B$, then $B$ has a smallest element, that is, there exists a $b_0 \in B$ such that $b_0 < b$ for all $b \in B$, $b \neq b_0$.

In particular, we have

**Theorem. (Well-Ordering Principle for $\mathbb{N}$)** Every nonempty set of nonnegative integers has a least element.

Now we show that if the product of two integers is 1, then either they are both 1 or they are both $-1$, but first we need a lemma.

**Lemma.** There does not exist an integer $n$ satisfying $0 < n < 1$.

**Proof.** Let $B = \{n \mid n \in \mathbb{Z}, \text{ and } 0 < n < 1\}$.

If $B \neq \emptyset$, since $B$ is bounded below by 0, then by the Well-Ordering Principle $B$ has a smallest element, say $n_0 \in B$, but then multiplying the inequality $0 < n_0 < 1$ by the positive integer $n_0$, we have

$$0 < n_0^2 < n_0 < 1.$$  

However, $n_0^2$ is an integer and so $n_0^2 \in B$, which contradicts the fact that $n_0$ is the smallest element of $B$. Therefore, our original assumption is incorrect and $B = \emptyset$, that is, there does not exist an integer $n$ satisfying $0 < n < 1$. Note that we have shown that 1 is the smallest positive integer.

**Theorem.** If $a, b \in \mathbb{Z}$ and $a \cdot b = 1$, then either $a = b = 1$ or $a = b = -1$.

**Proof.** If $a \cdot b = 1$, then we know that $a \neq 0$ and $b \neq 0$, since if $a = 0$ or $b = 0$, this would imply that $1 = 0$, which is a contradiction. Also, since $1 > 0$, we know that $a$ and $b$ are either both positive or both negative. In fact, if $a > 0$ and $b < 0$, then $-b > 0$, implies $a \cdot (-b) = -(a \cdot b) > 0$, that is, $-1 > 0$ which is a contradiction. Therefore, we may assume without loss of generality that $a > 0$ and $b > 0$.

From the lemma we have $a \geq 1$ and $b \geq 1$, so that

$$0 \leq (a-1)(b-1) = a \cdot b - (a+b) + 1 = 2 - (a+b)$$

and so

$$0 < a + b \leq 2.$$

Now, if either $a > 1$ or $b > 1$ this would imply that

$$a + b > 1 + 1 = 2,$$

which is a contradiction, and so we must have $0 < a \leq 1$ and $0 < b \leq 1$. Therefore, the Law of Trichotomy implies that $a = 1$ and $b = 1$. 

\[\square\]
We will show that the Well-Ordering Principle for $\mathbb{N}$ is logically equivalent to the Principle of Mathematical Induction, so we may assume one of them as an axiom and prove the other one as a theorem.

**Exercise.** Show that the following statement is equivalent to the Well-Ordering Axiom for the Integers:

Every nonempty subset of integers which is bounded above has a largest element.

**Example.** The set of rational numbers

$$\mathbb{Q} = \{ a/b \mid a, b \in \mathbb{Z}, b \neq 0 \}$$

with the usual ordering is not a well-ordered set, that is, there exists a nonempty subset $B$ of $\mathbb{Q}$ which is bounded below, but which has no smallest element.

**Proof.** In fact, we can take $B = \mathbb{Q}^+$, the set of all positive rational numbers; clearly $\mathbb{Q}^+ \neq \emptyset$ and $0 < q$ for all $q \in \mathbb{Q}^+$, so it is also bounded below.

Now, suppose that $\mathbb{Q}^+$ has a smallest element, say $q_0 \in \mathbb{Q}^+$, then $q_0/2 \in \mathbb{Q}^+$ also, and $q_0/2 < q_0$, which is a contradiction. Therefore, our original assumption must have been false, and $\mathbb{Q}^+$ has no smallest element, so $\mathbb{Q}$ is not well-ordered.

**Definition.** The set of irrational numbers is the set of all real numbers that are not rational, that is, the set $\mathbb{R} \setminus \mathbb{Q}$.

**Example.** The real number $\sqrt{2}$ is irrational.

**Proof.** We will show this using the Well-Ordering Principle. First note that the integer 2 lies between the squares of two consecutive positive integers (consecutive squares), namely, $1 < 2 < 4$, and therefore

$$1 < \sqrt{2} < 2,$$

(since $0 < \sqrt{2} \leq 1$ implies $2 \leq 1$, a contradiction; while $\sqrt{2} \geq 2$ implies $2 \geq 4$, again, a contradiction).

Now let

$$B = \{ b \in \mathbb{N}^+ \mid \sqrt{2} = a/b \text{ for some } a \in \mathbb{Z} \},$$

if $\sqrt{2} \in \mathbb{Q}$, then $B \neq \emptyset$. Since $B$ is bounded below by 0, then the Well-Ordering Principle implies that $B$ has a smallest element, call it $b_0$, so that

$$\sqrt{2} = \frac{a_0}{b_0}$$

where $a_0, b_0 \in \mathbb{N}^+$, and $2b_0^2 = a_0^2$. Since

$$1 < \frac{a_0}{b_0} < 2,$$

then $b_0 < a_0 < 2b_0$, and therefore $0 < a_0 - b_0 < b_0$. Now we find a positive integer $x$ such that

$$\frac{x}{a_0 - b_0} = \frac{a_0}{b_0},$$

that is, $b_0x = a_0(a_0 - b_0) = a_0^2 - a_0b_0 = 2b_0^2 - a_0b_0 = b_0(2b_0 - a_0)$, so we may take $x = 2b_0 - a_0$, and

$$\sqrt{2} = \frac{2b_0 - a_0}{a_0 - b_0} = \frac{a_0}{b_0},$$

so that $a_0 - b_0 \in B$, and $0 < a_0 - b_0 < b_0$. However, this contradicts the fact that $b_0$ is the smallest element in $B$, so our original assumption is incorrect. Therefore, $B = \emptyset$ and $\sqrt{2}$ is irrational. $\square$
**Exercise.** Show that if \( m \) is a positive integer which is not a perfect square, that is, \( m \) is not the square of another integer, then \( \sqrt{m} \) is irrational.

**Hint:** The proof mimics the proof above for \( \sqrt{2} \).

**Definition.** If \( n \in \mathbb{Z} \), then we say that \( n \) is **even** if and only if there exists an integer \( k \in \mathbb{Z} \) such that \( n = 2k \). We say that \( n \) is **odd** if and only if there is an integer \( k \in \mathbb{Z} \) such that \( n = 2k + 1 \).

We will use the Well-Ordering Principle to show that every integer is either even or odd.

**Theorem.** Every integer \( n \in \mathbb{Z} \) is either even or odd.

**Proof.** Suppose there exists an integer \( N \in \mathbb{Z} \) such that \( N \) is neither even nor odd, let

\[
B = \{ n \in \mathbb{Z} \mid n \text{ is even or odd and } n \leq N \},
\]

then \( B \neq \emptyset \) and \( B \) is bounded above by \( N \). By the Well-Ordering Property, \( B \) has a largest element, say \( n_0 \in B \). Since \( n_0 \) is either even or odd, and \( n_0 \leq N \), then we must have the strict inequality \( n_0 < N \).

If \( n_0 \) is even, then \( n_0 + 1 \) is odd, and since \( n_0 \) is the largest such integer in \( B \), then we must have

\[
n_0 < N < n_0 + 1.
\]

If \( n_0 \) is odd, then \( n_0 + 1 \) is even, and again, since \( n_0 \) is the largest such integer in \( B \), we must have

\[
n_0 < N < n_0 + 1.
\]

Thus, in both cases, \( N - n_0 \) is an integer and

\[
0 < N - n_0 < 1,
\]

which is a contradiction. Therefore, our original assumption was incorrect, and there does not exist an integer \( N \in \mathbb{Z} \) which is neither even nor odd, that is, every integer \( n \in \mathbb{Z} \) is either even or odd. \( \square \)

**Theorem.** There does not exist an integer \( a \in \mathbb{Z} \) which is both even and odd. Thus the set of integers \( \mathbb{Z} \) is partitioned into two disjoint classes, the even integers and the odd integers.

**Proof.** Suppose that \( a \in \mathbb{Z} \) and \( a \) is both even and odd, then there exist \( k, \ell \in \mathbb{Z} \) such that

\[
a = 2k \quad \text{and} \quad a = 2\ell + 1,
\]

and therefore \( 2\ell + 1 = 2k \), so that \( 2(k - \ell) = 1 \).

Now, since \( 1 > 0 \), the law of trichotomy implies that \( k - \ell > 0 \). Also, since \( 2 = 1 + 1 > 1 + 0 = 1 \), then

\[
1 = 2 \cdot (k - \ell) > 1 \cdot (k - \ell) = k - \ell.
\]

Therefore, \( k - \ell \) is an integer satisfying \( 0 < k - \ell < 1 \), which is a contradiction, and our assumption that there exists an integer \( a \) which is both even and odd is false. \( \square \)