The Ring of Integers

The integers \( \mathbb{Z} \) form a mathematical structure known as a **commutative ring with unity**. The ring axioms for \( \mathbb{Z} \) are given below. These axioms aren’t sufficient to characterize or define \( \mathbb{Z} \); there are additional axioms needed (for example, there are axioms which deal with the **order relation** on \( \mathbb{Z} \)). I’m mentioning these now so that they’ll look familiar when I discuss rings in general later on.

**Axioms for the Ring of Integers.** There are binary operations defined on the set of integers. The binary operation of addition is denoted \(+\) and satisfies the following axioms:

1. **(Associativity)** If \( a, b, c \in \mathbb{Z} \), then
   \[ a + (b + c) = (a + b) + c. \]

2. **(Identity)** There is an element \( 0 \in \mathbb{Z} \) such that if \( a \in \mathbb{Z} \), then
   \[ a + 0 = a \quad \text{and} \quad 0 + a = a. \]

3. **(Inverses)** For every element \( a \in \mathbb{Z} \), there is an element \( -a \in \mathbb{Z} \) (the **additive inverse** of \( a \)) which satisfies
   \[ a + (-a) = 0 \quad \text{and} \quad -a + a = 0. \]

4. **(Commutativity)** If \( a, b \in \mathbb{Z} \), then
   \[ a + b = b + a. \]

The binary operation of multiplication is denoted \( \cdot \); but as usual, I may write “\( xy \)” as shorthand for “\( x \cdot y \)”. Multiplication satisfies the following axioms:

5. **(Associativity)** If \( a, b, c \in \mathbb{Z} \), then
   \[ a \cdot (b \cdot c) = (a \cdot b) \cdot c. \]

6. **(Identity)** There is an element \( 1 \in \mathbb{Z} \) such that if \( a \in \mathbb{Z} \), then
   \[ a \cdot 1 = a \quad \text{and} \quad 1 \cdot a = a. \]

7. **(Commutativity)** If \( a, b \in \mathbb{Z} \), then
   \[ a \cdot b = b \cdot a. \]

Finally, addition and multiplication are related by:

8. **(Distributivity)** If \( a, b, c \in \mathbb{Z} \), then
   \[ a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c. \]

The algebraic properties of \( \mathbb{Z} \) follow from these axioms. Here are a couple of examples.

**Example.** Let \( x \in \mathbb{Z} \). Prove that \( 0 \cdot x = 0 \).

The start of the proof requires a little trick: \( 0 = 0 + 0! \)

\[
0 \cdot x = (0 + 0) \cdot x \quad \text{Additive identity}
\]

\[
= 0 \cdot x + 0 \cdot x \quad \text{Distributivity}
\]

\[
= 0.
\]
Now add \(-\langle 0 \cdot x \rangle\) to both sides:
\[
\begin{align*}
-\langle 0 \cdot x \rangle + (0 \cdot x) & = -(0 \cdot x) + (0 \cdot x + 0 \cdot x) \\
0 & = -(0 \cdot x) + 0 + 0 \cdot x \quad \text{Additive inverses, associativity} \\
0 & = 0 + 0 \cdot x \quad \text{Additive inverses} \\
0 & = 0 \cdot x \quad \text{Additive identity}
\end{align*}
\]

**Example.** Let \(x \in \mathbb{Z}\). Prove that \((-1) \cdot x = -x\).

This is one of those annoying results which is really “obvious” — but can be tricky to prove, because it’s hard to know how to get started!

What does \((-1) \cdot x = -x\) mean?

\(-x\) means “the additive inverse of \(x\):” The element which gives 0 when it is added to \(x\). Thus, \((-1) \cdot x = -x\) asserts that \((-1) \cdot x\) is the additive inverse of \(x\).

How do you check whether something is the additive inverse of \(x\)? By definition, you add it to \(x\) and see if you get 0:
\[
\begin{align*}
x + (-1) \cdot x & = 1 \cdot x + (-1) \cdot x \quad \text{Multiplicative identity} \\
& = (1 + (-1)) \cdot x \quad \text{Distributivity} \\
& = 0 \cdot x \quad 1 \text{ and } -1 \text{ are inverses} \\
& = 0 \quad \text{Previous result}
\end{align*}
\]

This proves that \((-1) \cdot x = -x\). ☐

For the most part, I’ll take *elementary* properties of the integers for granted. Here is a property which is *not* so elementary, even though it may look rather obvious.

**Well-Ordering Principle.** The positive integers \(\mathbb{Z}^+\) are well-ordered — that is, every nonempty subset of the positive integers has a smallest element.

Even though your experience with the integers may lead you to think this is obvious, it’s actually an *axiom* of the positive integers \(\mathbb{Z}^+\). It has many important consequences; *Mathematical Induction* is one, and the following result is another.

Note that Well-Ordering applies to nonempty subsets of the *nonnegative* integers as well. If such a subset contains 0, then 0 is the smallest element; if the subset doesn’t contain 0, then it consists of only positive integers, and Well-Ordering for the positive integers implies that it has a smallest element.

**Example.** Show that there is no positive integer less than 1.

In this proof, I’m going to assume familiar facts about inequalities involving integers, since the point is to illustrate how you might use Well-Ordering.

Suppose that there is a positive integer less than 1. Let \(S\) be the set of positive integers less than 1. Then \(S\) is nonempty, so by Well-Ordering, \(S\) has a smallest element.

Suppose that \(x\) is the smallest element of \(S\). Now \(0 < x < 1\), so multiplying by \(x\), I get
\[
0 < x^2 < x, \quad \text{and} \quad x < 1, \quad \text{so} \quad 0 < x^2 < x < 1.
\]

Thus, \(x^2\) is a positive integer less than 1 which is *smaller than* \(x\). This is a contradiction. Therefore, there is no positive integer less than 1. ☐