

Here's a joke definition of the integers:

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

We all “know” the basic properties of this set because we’ve been fooling around with it since childhood. But if we want to **prove** anything about  $\mathbb{Z}$  (and we do) then we need a formal definition. First I’ll give a friendly definition. This just states everything we already “know” in formal language. As you see, it’s a bit long. Afterwards I’ll give a more efficient (but much more subtle) definition of  $\mathbb{Z}$ .

#### FRIENDLY DEFINITION

Let  $\mathbb{Z}$  be a set equipped with

- an equivalence relation “=” defined by
  - $\forall a \in \mathbb{Z}, a = a$  (reflexive)
  - $\forall a, b \in \mathbb{Z}, (a = b) \Rightarrow (b = a)$  (symmetric)
  - $\forall a, b, c \in \mathbb{Z}, (a = b \wedge b = c) \Rightarrow (a = c)$  (transitive),
- a total ordering “ $\leq$ ” defined by
  - $\forall a \in \mathbb{Z}, a \leq a$  (reflexive)
  - $\forall a, b \in \mathbb{Z}, (a \leq b \wedge b \leq a) \Rightarrow (a = b)$  (antisymmetric)
  - $\forall a, b, c \in \mathbb{Z}, (a \leq b \wedge b \leq c) \Rightarrow (a \leq c)$  (transitive)
  - $\forall a, b \in \mathbb{Z}, (a \leq b \vee b \leq a)$  (total)
- and two binary operations
  - $\forall a, b \in \mathbb{Z}, \exists a + b \in \mathbb{Z}$  (addition)
  - $\forall a, b \in \mathbb{Z}, \exists ab \in \mathbb{Z}$  (multiplication)

which satisfy the following properties:

#### Axioms of Addition.

- (A1)  $\forall a, b \in \mathbb{Z}, a + b = b + a$  (commutative)
- (A2)  $\forall a, b, c \in \mathbb{Z}, a + (b + c) = (a + b) + c$  (associative)
- (A3)  $\exists 0 \in \mathbb{Z}, \forall a \in \mathbb{Z}, 0 + a = a$  (additive identity exists)
- (A4)  $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a + b = 0$  (additive inverses exist)

These four properties tell us that  $\mathbb{Z}$  is an **additive group**. It has a special element called 0 that acts as an “identity element” for addition, and every integer  $a$  has an “additive inverse”, which we will call  $-a$ .

#### Axioms of Multiplication.

- (M1)  $\forall a, b \in \mathbb{Z}, ab = ba$  (commutative)
- (M2)  $\forall a, b, c \in \mathbb{Z}, a(bc) = (ab)c$  (associative)
- (M3)  $\exists 1 \in \mathbb{Z}_{\neq 0}, \forall a \in \mathbb{Z}, 1a = a$  (multiplicative identity exists)

Notice that elements of  $\mathbb{Z}$  do **not** have “multiplicative inverses”. That is, we can’t divide in  $\mathbb{Z}$ . So  $\mathbb{Z}$  is not quite a group under multiplication. We also need to say how addition and multiplication behave together.

#### Axiom of Distribution.

- (D)  $\forall a, b, c \in \mathbb{Z}, a(b + c) = ab + ac$

We can paraphrase these first eight properties by saying that  $\mathbb{Z}$  is a (commutative) ring. Next we will describe how arithmetic and order interact.

### Axioms of Order.

- (O1)  $\forall a, b, c \in \mathbb{Z}, (a \leq b) \Rightarrow (a + c \leq b + c)$
- (O2)  $\forall a, b, c \in \mathbb{Z}, (a \leq b \wedge 0 \leq c) \Rightarrow (ac \leq bc)$
- (O3)  $0 < 1$  (this means that  $0 \leq 1 \wedge 0 \neq 1$ )

These first eleven properties tell us that  $\mathbb{Z}$  is an **ordered ring**. However, we have not yet defined  $\mathbb{Z}$  because there are other ordered rings, for example the real numbers  $\mathbb{R}$ . To distinguish  $\mathbb{Z}$  among the ordered rings we need one final axiom. This last axiom is **not obvious** and it took a long time for people to realize that it is an axiom and not a theorem.

### The Well-Ordering Axiom.

Let  $\mathbb{N} = \{a \in \mathbb{Z} : 1 \leq a\}$  denote the set of **natural numbers**. Then every nonempty subset of  $\mathbb{N}$  has a smallest element. Formally, let  $\wp(\mathbb{N})_{\neq \emptyset}$  be the **set** of nonempty subsets of  $\mathbb{N}$ . Then we have

- (WO)  $\forall X \in \wp(\mathbb{N})_{\neq \emptyset}, \exists a \in X, \forall b \in X, a \leq b$

This axiom is also known as the **principle of induction**; we will use it a lot. Thus endeth the friendly definition.

### SUBTLE DEFINITION

The above definition is friendly and practical. **But it is quite long!** You might ask whether we can define  $\mathbb{Z}$  using fewer axioms; the answer is “Yes”. The most efficient definition of  $\mathbb{Z}$  is due to Giuseppe Peano (1858–1932). His definition is efficient, but it no longer looks much like the integers.

**Peano’s Axioms.** Let  $\mathbb{N}$  be a set equipped with an equivalence relation “ $=$ ” and a unary “successor” operation  $S : \mathbb{N} \rightarrow \mathbb{N}$ , satisfying the following four axioms:

- (P1)  $1 \in \mathbb{N}$  (1 is in  $\mathbb{N}$ )
- (P2)  $\forall n \in \mathbb{N}, S(n) \neq 1$  (1 is not the successor of any natural number)
- (P3)  $\forall m, n \in \mathbb{N}, (S(m) = S(n)) \Rightarrow (m = n)$  ( $S$  is an injective function)
- (P4) (The induction principle) **If** a set  $K \subseteq \mathbb{N}$  of natural numbers satisfies
  - $1 \in K$ , and
  - $\forall n \in \mathbb{N}, (n \in K) \Rightarrow (S(n) \in K)$ ,**then**  $K = \mathbb{N}$ .

With a lot of work, one can use  $\mathbb{N}$  and  $S$  to define a set  $\mathbb{Z}$  with addition, multiplication, a total ordering, etc., and show that it has the desired properties. Good luck to you. I’ll stick with the friendly definition.