Math 309 **Summer 2014**
The Definition of $\mathbb{Z}$ **Drew Armstrong**

Here's a joke definition of the integers:

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

We all "know" the basic properties of this set because it is supposed to model our experience with counting things, lining them up, and putting them in rectangular arrays. For thousands of years that was good enough, but in the 19th century people started to worry: how solid, really, is our knowledge about numbers? Around this time people began to develop a **formal definition** of the integers. Here I will describe the ideas put forward by Richard Dedekind in his 1888 paper *Was sind und was sollen die Zahlen?* (What are numbers and what should they be?) and then refined by Giuseppe Peano in his 1889 paper *Arithmetices principia, nova methodo exposita* (The principles of arithmetic presented by a new method).

First I'll give Dedekind's "friendly" definition. As you will see, it's a bit long. After that I'll give Peano's more efficient (but much more subtle) definition.

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)
  - $\forall\, a, b, c \in \mathbb{Z}$, $(a = b$ AND $b = c) \Rightarrow a = c$ (transitive),
- a total ordering "$\leq$" defined by
  - $\forall\, a, b \in \mathbb{Z}$, $(a \leq b$ AND $b \leq a) \Rightarrow a = b$ (antisymmetric)
  - $\forall\, a, b, c \in \mathbb{Z}$, $(a \leq b$ AND $b \leq c) \Rightarrow a \leq c$ (transitive)
  - $\forall\, a, b \in \mathbb{Z}$, $a \leq b$ OR $b \leq a$ (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) $\exists\, 1 \in \mathbb{Z}, 1 \neq 0, \forall\, a \in \mathbb{Z}$, $1a = a$ (multiplicative identity exists)

Notice that elements of $\mathbb{Z}$ do **not** (necessarily) 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) $\forall\, a, b, c \in \mathbb{Z},\ (a \leq b \text{ AND } 0 \leq c) \Rightarrow ac \leq bc$

(O3) $0 < 1$ (this means $0 \leq 1$ AND $0 \neq 1$)

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** so 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 $\mathbb{N} = \{n \in \mathbb{Z} : 0 \leq n\}$ denote the set of natural numbers. Then every nonempty subset of $\mathbb{N}$ has a smallest element. Formally,

(W) $\forall\, X \subseteq \mathbb{N}, X \neq \emptyset,\ \exists\, a \in X,\ \forall\, b \in X,\ a \leq b$

This axiom is also known as the principle of induction; it will be our main topic of discussion for the rest of Math 309. Thus ends 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. Giuseppe Peano (1889) came up a definition using **only four axioms**. 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" function $S : \mathbb{N} \to \mathbb{N}$, satisfying the following four axioms:

(P1) $0 \in \mathbb{N}$ (0 is in $\mathbb{N}$)

(P2) $\forall\, n \in \mathbb{N},\ S(n) \neq 0$ (0 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
- $0 \in K$, 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 Peano's $\mathbb{N}$ and S to construct the set $\mathbb{Z}$ with all of the appropriate operations and then prove that it has all of the friendly properties. Good luck to you. I'll stick with the friendly definition.