Formal construction of number systems.

Mathematicians create new objects when they need them, but to ensure that they have not introduced inconsistencies into mathematics they try to show that these objects can be constructed from the axioms of set theory. There is a general approach to constructing such objects, like new number systems, which will be explained in this note.

The intuitive idea is that we begin with a set A that may be considered to be an alphabet of symbols, then describe a subset $W \subseteq A^n$ of sequences that may be thought of as words over the alphabet A. These are the words that name the elements of our structure. Very often two words name the same element, so we define an equivalence relation E on W that relates two words if they represent the same element of the structure. Then the structure is built out of the set $W/E = \{[w]_E \mid w \in W\}$ of equivalence classes of words.

Example 1. Construction of $\mathbb{Z}$ from $\mathbb{N}$.

In this example the alphabet of symbols is $A = \mathbb{N}$. The 'words' used in naming integers are the 2-element sequences $W = \mathbb{N} \times \mathbb{N}$. Each pair $(m, n) \in W$ is thought of as representing a shift of the number line m units in the positive direction followed by a shift of n units in the negative direction, so (m, n) 'names' the integer that we intend to call $m - n$. (Minus hasn't been defined yet, so this reference to it is informal only). Two pairs $(k, l), (m, n) \in \mathbb{N} \times \mathbb{N}$ should represent the same integer if $k - l = m - n$, which cannot be expressed in the natural numbers because of the minus. But it can be rewritten as $k + n = m + l$, which *can* be expressed in the natural numbers. Thus, the equivalence relation we define is

$$E = \{((k, l), (m, n)) \in (\mathbb{N} \times \mathbb{N})^2 \mid k + n = m + l\}.$$

Lemma 1. *E is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Define $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/E$, so a typical integer is really of the form $[(k, l)]_E$. In particular, the integer known as "zero" is really the infinite set $0_{\mathbb{Z}} = [(0, 0)]_E = \{(0, 0), (1, 1), (2, 2), \ldots\}$, and the integer known as "one" is really $1_{\mathbb{Z}} = [(1, 0)]_E = \{(1, 0), (2, 1), (3, 2), \ldots\}$. More generally, there is a function $\mathbb{N} \to \mathbb{Z}\colon k_{\mathbb{N}} \mapsto [(k, 0)]_E = k_{\mathbb{Z}}$ which describes a correspondence between the natural numbers and some of the integers.

There are a number of things to define and prove, now. One must define the arithmetic operations on $\mathbb{Z}$ $(+, -, *)$ and the order on $\mathbb{Z}$. Then one must prove the basic properties of these operations and order.

The arithmetic operations are defined as follows: $[(k, l)]_E + [(m, n)]_E = [(k + m, l + n)]_E$; $-[(k, l)]_E = [(l, k)]_E$; and $[(k, l)]_E * [(m, n)]_E = [(km + ln, kn + lm)]_E$. The order is defined by $[(k, l)]_E \leq [(m, n)]_E$ in $\mathbb{Z}$ if and only if $k + n \leq m + l$ in $\mathbb{N}$.

One proves a law of integer arithmetic, like the associative law for addition, in the following way:

$$\begin{aligned}
[(k,l)]_E + ([(m,n)]_E + [(p,q)]_E) &= [(k,l)]_E + [(m+p,n+q)]_E \\
&= [(k+(m+p),l+(n+q))]_E \\
&= [((k+m)+p,(l+n)+q)]_E \\
&= [(k+m,l+n)]_E + [(p,q)]_E \\
&= ([(k,l)]_E + [(m,n)]_E) + [(p,q)]_E
\end{aligned}$$

Example 2. Construction of $\mathbb{Q}$ from $\mathbb{Z}$.

Each fraction $m/n \in \mathbb{Q}$ is really just a pair of integers where the denominator may be taken to be positive. Thus we define $\mathbb{Q}$ by starting with the subset

$$W = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid n > 0\},$$

defining an equivalence relation E on W by

$$E = \{((k,l),(m,n)) \in (\mathbb{Z} \times \mathbb{Z})^2 \mid kn = ml\},$$

and then defining $\mathbb{Q} = W/E$. Instead of writing $[(m,n)]_E$ we write m/n. Operations are defined the way you think: $[(k,l)]_E + [(m,n)]_E = [(kn+ml,ln)]_E$ (since $k/l + m/n$ should be $(kn+ml)/ln$), $-[(k,l)]_E = [(-k,l)]_E$, and $[(k,l)]_E * [(m,n)]_E = [(km,ln)]_E$. One must check that these are valid operations and that they satisfy the expected properties.

Example 3. Construction of $\mathbb{Z}_n$ from $\mathbb{Z}$.

This construction may be new. Define an equivalence relation on $\mathbb{Z}$ by

$$E = \{(a,b) \in \mathbb{Z}^2 \mid n \text{ divides } a-b\}.$$

(Check that this is an equivalence relation.) Let $\mathbb{Z}_n = \mathbb{Z}/E$. Define arithmetic on $\mathbb{Z}_n$ by $[a]_E + [b]_E = [a+b]_E$, $-[a]_E = [-a]_E$, and $[a]_E * [b]_E = [ab]_E$. (Check that these are operations.) The arithmetic of $\mathbb{Z}_n$ is used in number theory, cryptography, computer science and other places.