Constructing **Z** from **N**

In these notes we will construct a set $\mathbf{Z}$ which will have all the familiar properties the integers. Since our purpose here is to *construct* the integers, and *prove* they have certain properties, we must be careful not to *assume* ahead of time that they have these properties.

In our past work we have constructed the natural numbers $\mathbf{N}$ (assuming the Peano Axioms) and shown that these numbers behave the way we expect. We can therefore base our construction of $\mathbf{Z}$ on the properties we have proven to be true of $\mathbf{N}$.

Define $X = \mathbf{N} \times \mathbf{N}$. Define a relation on X by declaring $(m, n) \sim (m', n')$ iff $m + n' = n + m'$. (Note: my "thought process" here is that I'm thinking of (m, n) as $m - n$, and I want the two ordered pairs above to be equivalent if $m - n = m' - n'$. The definition chosen is a sneaky way to get around the fact that we haven't defined $m - n$ if $m \leq n$; we haven't defined zero or negative numbers. My "thought process" is *purely motivation*; it cannot be used to justify any steps in a proof.)

Exercises

1. Prove that $\sim$ is an equivalence relation.
2. Prove that $(m, n) \sim (m', n')$ iff $(m + p, n + p) \sim (m' + p, n' + p)$ $\forall p \in \mathbf{N}$.
3. Prove that if $(m, p) \sim (n, p)$, or if $(p, m) \sim (p, n)$, then $m = n$.
4. Determine all elements of X that are equivalent to (1,1).

Definition. Define an operation $+$ on X by $(m, n) + (m', n') = (m + m', n + n')$.

Exercise

5. Prove that if $a, b, a', b' \in X$ and $a \sim a', b \sim b'$, then $a + b \ \sim \ a' + b'$.

Definition and notation. Let $\mathbf{Z}$ denote the set of equivalence classes determined by $\sim$. Write $[(m, n)]$ for the equivalence class of (m, n); thus $[(m, n)] = [(m', n')]$ iff $m+n' = n+m'$. Define $0 = [(1, 1)]$. Define an operation $+$ on $\mathbf{Z}$ as follows. Given $a, b \in \mathbf{Z}$, there exist $m, n, p, q \in \mathbf{N}$ such that $a = [(m, n)], b = [(p, q)]$. Consider $[(m, n) + (p, q)]$. The numbers m, n, p, q are not uniquely determined by a, b; however, if we choose any other numbers m', n', p', q' such that (m', n') and (p', q') represent the same equivalence classes as (m, n) and (p, q) respectively (i.e. $[(m', n')] = a, [(p', q')] = b$), then by Exercise 5, $[(m', n') + (p', q')] = [(m, n) + (p, q)]$. Thus this final equivalence class depends only on the equivalence classes a and b, not on the choices of elements of X we choose to represent these classes. Hence we can take the following equation as the definition of an operation $+$ on $\mathbf{Z}$:

$$[(m,n)] + [(p,q)] = [(m+p, n+q)] \quad (= [(m,n) + (p,q)]) \;\; \forall m,n,p,q \in \mathbf{N}.$$

(We say that the $+$ on the left is *well-defined* by this equation.) We will refer to $+$ as *addition* on both $\mathbf{N}$ and $\mathbf{Z}$. (Note: we now have three distinct binary operations labeled "+": one on $\mathbf{N}$, one on X, and one on $\mathbf{Z}$. As long as we are careful to use the plus sign only between two elements of $\mathbf{N}$, between two elements of X, or between two elements of $\mathbf{Z}$, the context eliminates any ambiguity in the meaning. Of course, we must be careful not to put the plus sign between an element of one of the sets $\mathbf{N}, X, \mathbf{Z}$, and an element of a different one of these sets, since such an operation would have no meaning.)

Exercises.

6. Prove that addition in $\mathbf{Z}$ is commutative and associative.

7. Prove that $a + 0 = a, \; \forall a \in \mathbf{Z}$.

8. Prove that for all $a \in \mathbf{Z}$, there exists a unique $b \in \mathbf{Z}$ such that $a+b = 0$. Henceforth let $-a$ denote the b of the previous sentence. If $(m,n) \in X$ represents a, what is an obvious representative for $-a$? Prove that $-(-a) = a$.

9. Prove that for all $a, b \in \mathbf{Z}$, there exists a unique $x \in \mathbf{Z}$ such that $a + x = b$. Henceforth denote the x of the previous sentence by $b - a$. Prove that $0 - a = -a, \forall a \in \mathbf{Z}$.

We are used to thinking of the natural numbers as a subset of the integers. To see that our model for the integers, $\mathbf{Z}$, is consistent with this way of thinking, define a function $f_+ : \mathbf{N} \to \mathbf{Z}$ by $f(n) = [(n+1, 1)]$, and define a subset $\mathbf{Z}_+ \subset \mathbf{Z}$, to be called the *positive integers*, by $\mathbf{Z}_+ = image(f_+)$

Exercises.

10. Prove that f_+ is injective, and hence gives a bijection between $\mathbf{N}$ and $\mathbf{Z}_+$.

We use the bijection f_+ to endow $\mathbf{Z}_+$ with a successor function. Specifically, for $a \in \mathbf{Z}_+$, there is a unique $n \in \mathbf{N}$ such that $f_+(n) = a$; we call this n "$f_+^{-1}(a)$". Then we can define $s' : \mathbf{Z}_+ \to \mathbf{Z}_+$ by $s'(a) = f_+(s(f_+^{-1}(a)))$ (where s is the successor function on $\mathbf{N}$).

Exercises

11. What is the (unique) element $1' \in \mathbf{Z}_+$ that has no predecessor?

12. Show that for $a \in \mathbf{Z}_+$, $s'(a) = a + 1'$, where in this equation "+" is the operation on $\mathbf{Z}$ we defined above.

13. Understand why $\mathbf{Z}_+$ is "essentially the same" as $\mathbf{N}$. Thus f_+ is a "dictionary" (the technical term is "isomorphism") enabling us to translate statements about $\mathbf{N}$ into equivalent statements about $\mathbf{Z}_+$.

14. Prove that for all $a \in \mathbf{Z}$, exactly one of the following statements is true: (i) $a \in \mathbf{Z}_+$; (ii) $a = 0$; or (iii) $-a \in \mathbf{Z}_+$.

We still need to define multiplication on $\mathbf{Z}$. Our definition should *extend* what we already have defined to be multiplication on $\mathbf{Z}_+$ (i.e. on $\mathbf{N}$); the product of two positive integers should not be different from what we get by viewing these integers as natural numbers.

Definition. Define an operation $*$ on X by

$$(m, n) * (p, q) = (mp + nq, mq + np).$$

Exercise

15. Prove that if $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$, then $(m, n) * (p, q) \sim (m', n') * (p', q')$.

As a result of exercise 15, the following formula gives a well-defined operation $\cdot$, which we will call *multiplication*, on $\mathbf{Z}$:

$$[(m, n)] \cdot [(p, q)] = [(mp + nq, mq + np)].$$

Exercises

16. Prove that multiplication on $\mathbf{Z}$ is associative and commutative, and that it distributes over addition.

17. Let $\mathbf{1} = f_+(1)$ (where $f_+ : \mathbf{N} \to \mathbf{Z}$ is as on the previous page). Prove that for all $a \in \mathbf{Z}$ we have $a \cdot \mathbf{1} = a$, and that $\mathbf{1}$ is the unique element of $\mathbf{Z}$ with this property.

18. Prove that for all $a \in \mathbf{Z}$, $\quad a \cdot 0 = 0$. Also prove that if $a, b \in \mathbf{Z}$ and $a \cdot b = 0$, then $a = 0$ or $b = 0$.