INTEGERS

PAUL L. BAILEY

Abstract. We continue our study of number systems. In this installment, we develop the integers in detail.

1. Motivation

The goal is to create the integers from the natural numbers. This will give us a formal number system in which subtraction is possible. We know where we want to go with this; we just wish to formalize it in a manner that makes proving things about the integers possible. Thus it is allowable and desirable to use our intuitive understanding of the number system we wish to devise as a beacon.

The plan is two take ordered pairs of natural numbers, and think of them as integers. The pair (m, n) is to be thought of as the integer $m - n$. Thus $(5, 0)$ should represent 5, and $(0, 5)$ should represent -5. Unfortunately, $(3, 8)$ should also represent -5. Thus there are too many pairs.

This situation is alleviated via the use of equivalence relations. We take the set of ordered pairs of natural numbers and partition it into blocks of pairs which represent the same integer. Here, two integers represent the same integer if they differ by the same amount. Since we do not yet have the operation of subtraction, instead of defining "differing by the same amount" as $a - b = c - d$, instead we say that (a, b) and (c, d) differ by the same amount if $a + d = b + c$.

Then we define an integer to be a block in the partition of $\mathbb{N} \times \mathbb{N}$ induced by this equivalence relation.

Date: May 4, 1996.

2. Definition

Proposition 1. *Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation on X by*

$$(a, b) \equiv (c, d) \Leftrightarrow a + d = b + c.$$

Then $\equiv$ is an equivalence relation.

Proof. We wish to show that $\equiv$ is reflexive, symmetric, and transitive.

(Reflexivity) Let $(a, b) \in X$. Then $a + b = b + a$ because addition of natural numbers is commutative. Thus $(a, b) \equiv (a, b)$, and $\equiv$ is reflexive.

(Symmetry) Let $(a, b), (c, d) \in X$. Then by symmetry of equality and commutativity of addition of natural numbers,

$$(a, b) \equiv (c, d) \Leftrightarrow a + d = b + c \Leftrightarrow c + b = d + a \Leftrightarrow (c, d) \equiv (a, b).$$

Thus $\equiv$ is symmetric.

(Transitivity) Let $(a, b), (c, d), (e, f) \in X$. Suppose that $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Add f to both sides of the first equation and add b to both sides of the second to obtain $a + d + f = b + c + f$ and $b + c + f = b + d + e$. Thus $a + d + f = b + d + e$. By the commutativity of addition and cancellation, we obtain $a + f = b + e$. Thus $(a, b) \equiv (e, f)$, and $\equiv$ is transitive. □

The set of equivalence classes in this equivalence relation is called the set of *integers*, and is denoted $\mathbb{Z}$. The equivalence class of (a, b) is denoted $[a, b]$.

3. Addition

We define addition in $\mathbb{Z}$ by

$$[a, b] + [c, d] = [a + c, b + d].$$

To define addition, we select members from two different equivalence classes and define their sum in terms of the selected members. What if we had selected different members? For example, is $[3, 5] + [2, 1] = [6, 8] + [9, 8]$? We need to reassure ourselves that the defined operation makes sense in this regard. If it does, it is called *well-defined*.

Proposition 2. *Addition in $\mathbb{Z}$ is well defined.*

Proof. To show that addition is well-defined, we select two arbitrary representatives from each equivalence class and show that they produce the same equivalence class upon being added.

Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{N}$ such that

$$[a_1, b_1] = [a_2, b_2] \text{ and } [c_1, d_1] = [c_2, d_2].$$

This means that $(a_1, b_1) \equiv (a_2, b_2)$ and $(c_1, d_1) \equiv (c_2, d_2)$, so

$$a_1 + b_2 = b_1 + a_2; \tag{1}$$

$$c_1 + d_2 = d_1 + c_2 \tag{2}$$

by our definition of equivalence.

Our definition of addition of equivalence classes gives that

$$[a_1, b_1] + [c_1, d_1] = [a_1 + c_1, b_1 + d_1]$$

and

$$[a_2, b_2] + [c_2, d_2] = [a_2 + c_2, b_2 + d_2].$$

We wish to show that $[a_2 + c_1, b_1 + d_1] = [a_2 + c_2, b_2 + d_2]$.

Adding equations (1) and (2) yields:

$$(a_1 + b_2) + (c_1 + d_2) = (b_1 + a_2) + (d_1 + c_2).$$

Since addition of natural numbers is commutative and associative,

$$(a_1 + c_1) + (b_2 + d_2) = (b_1 + d_1) + (a_2 + c_2).$$

Thus $(a_1 + c_1, b_1 + d_1) \equiv (a_2 + c_2, b_2 + d_2)$. Therefore $[a_1 + c_1, b_1 + d_1] = [a_2 + c_2, b_2 + d_2]$, and addition is well-defined. □

4. Multiplication

We define multiplication in $\mathbb{Z}$ by

$$[a, b] \cdot [c, d] = [ac + bd, ad + bc].$$

Proposition 3. *Multiplication in $\mathbb{Z}$ is well defined.*

Proof. Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{N}$ such that

$$[a_1, b_1] = [a_2, b_2] \text{ and } [c_1, d_1] = [c_2, d_2].$$

This means that $(a_1, b_1) \equiv (a_2, b_2)$ and $(c_1, d_1) \equiv (c_2, d_2)$, so

$$a_1 + b_2 = b_1 + a_2 \text{ and } c_1 + d_2 = d_1 + c_2$$

by our definition of equivalence.

Our definition of multiplication of equivalence classes gives that

$$[a_1, b_1][c_1, d_1] = [a_1c_1 + b_1d_1, a_1d_1 + b_1c_1]$$

and

$$[a_2, b_2][c_2, d_2] = [a_2c_2 + b_2d_2, a_2d_2 + b_2c_2].$$

We wish to show that $[a_1c_1 + b_1d_1, a_1d_1 + b_1c_1] = [a_2c_2 + b_2d_2, a_2d_2 + b_2c_2]$. This is a little tricky, so we introduce some additional notation to shorten things. Define

$$x = a_1c_1 + b_1d_1 + a_2d_2 + b_2c_2;$$
$$y = a_1d_1 + b_1c_1 + a_2c_2 + b_2d_2.$$

Now if we show that $x = y$, we will be done by definition of equivalence. Let

$$z = a_1d_2 + b_2d_1 + b_1c_2 + a_2c_1.$$

By the cancellation law of addition of natural numbers, it suffices to show that $x + z = y + z$. This is accomplished by showing that each side is equal to $2(a_1b_2)(c_1d_2)$.

First add z to both sides of the definition of x, expand z on the right side, and use commutativity of addition to insert shuffle the terms of z into the expresssion, acheiving

$$a_1c_1 + a_1d_2 + b_2c_2 + b_2d_1 + b_1d_1 + b_1c_2 + a_2d_2 + a_2c_1 = x + z.$$

Distributivity converts this into

$$a_1(c_1 + d_2) + b_2(c_2 + d_1) + b_1(d_1 + c_2) + a_2(d_2 + c_1) = x + z.$$

Now use the fact that $c_1 + d_2 = c_2 + d_1$ to obtain

$$(a_1 + b_2 + b_1 + a_2)(c_1 + d_2) = x + z.$$

Since $a_1 + b_2 = a_2 + b_1$, we have

$$2(a_1 + b_2)(c_1 + d_2) = x + z.$$

Perform the same manner of computation on the equation defining y, and you will find that

$$2(a_1 + b_2)(c_1 + d_2) = y + z.$$

□

5. Algebraic Properties

Theorem 1. *Let $a, b, c \in \mathbb{Z}$. Then*

(1) $a + b = b + a$ (commutativity of addition);
(2) $a + (b + c) = (a + b) + c$ (associativity of addition);
(3) $\exists! z \in \mathbb{Z}$ *such that* $a + z = a$ (additive identity);
(4) $\exists! - a \in \mathbb{Z}$ *such that* $a + (-a) = z$ (additive inverses);
(5) $ab = ba$ (commutativity of multiplication);
(6) $a(bc) = (ab)c$ (associativity of multiplication);
(7) $\exists! e \in \mathbb{Z}$ *such that* $ae = a$ (multiplicative identity);
(8) $a(b + c) = ab + ac$ (distributivity of multiplication over addition).

These eight properties state that $\mathbb{Z}$ is a *commutative ring*. We prove or comment on each.

Proposition 4. *Let $a, b \in \mathbb{Z}$. Then $a + b = b + a$.*

Proof. Since a and b are integers, they are represented by pairs of natural numbers, say $a = [m, n]$ and $b = [u, v]$. Then

$$a + b = [m, n] + [u, v] = [m + u, n + v] = [u + m, v + n] = [u, v] + [m, n] = b + a.$$

□

Proposition 5. *Let $a, b, c \in \mathbb{Z}$. Then $(a + b) + c = a + (b + c)$.*

Proof. This follows easily from the definitions and the fact that addition is associative in the natural numbers in a manner entirely analogous to the proof above. □

Proposition 6. *There exists a unique element $z \in \mathbb{Z}$ such that for every $a \in \mathbb{Z}$ we have $a + z = a$.*

Proof. Let $z = [0, 0]$. The fact that $a + z = a$ is immediate from the definition and the analogous fact in $\mathbb{N}$. Later, we will justify calling this element z by the name zero.

For uniqueness, suppose that y also satifies $a + y = a$ for all $a \in \mathbb{Z}$. Then $z = z + y = y + z = y$. □

Proposition 7. *For every $a \in \mathbb{Z}$ there exists a unique element $-a \in \mathbb{Z}$ such that $a + (-a) = z$.*

Proof. Let $a = [m, n]$, where $m, n \in \mathbb{N}$. Define $-a = [n, m]$. Then $a + (-a) = [m + n, m + n] = [0, 0]$. Call this element *negative* a.

For uniqueness, suppose $a + b = z$. Then $a + b = a + (-a)$. By commutativity, $b + a = (-a) + a$. Adding $(-a)$ to both sides gives $b = b + z = b + a + (-a) = (-a) + a + (-a) = (-a) + z = (-a)$. □

Now we may define *subtraction* on $\mathbb{Z}$ by

$$a - b = a + (-b).$$

Clearly subtraction in not commutative or associative.

Proposition 8. *Let $a, b \in \mathbb{Z}$. Then $ab = ba$.*

Proof. Let $a = [m, n]$ and $b = [u, v]$. Then $ab = [mu + nv, mv + nu] = [um + vn, vm + un] = ba$. □

Proposition 9. *Let $a, b, c \in \mathbb{Z}$. Then $a(bc) = (ab)c$.*

Proof. Same idea as the proof of commutativity. □

Proposition 10. *There exists a unique element $e \in \mathbb{Z}$ such that for every $a \in \mathbb{Z}$ we have $ae = a$.*

Proof. Let $e = [1, 0]$ and let $a = [m, n]$. Then $ae = [1m+0n, 1n+0m] = [m, n] = a$.

For uniqueness, suppose that $y \in \mathbb{Z}$ also satifies $ay = a$ for all $a \in \mathbb{Z}$. Then $y = ye = ey = e$. □

Proposition 11. *Let $a, b, c \in \mathbb{Z}$. Then $a(b + c) = ab + ac$.*

Proof. Let $a = [m, n]$, $b = [u, v]$, and $c = [x, y]$. Then

$$\begin{aligned} a(b+c) &= [m,n][u+x, v+y] \\ &= [m(u+x) + n(v+y), m(v+y) + n(u+x]] \\ &= [mu + mx + nv + ny, mv + my + nu + nx] \\ &= [mu + nv + mx + ny, mv + nu + my + nx] \\ &= [mu + nv, mv + nu] + [mx + my, my + nx] \\ &= [m,n][u,v] + [m,n][x,y] \\ &= ab + ac. \end{aligned}$$

□

To define exponentiation in $\mathbb{Z}$, one may use the Recursion Theorem.

Let $b \in \mathbb{Z}$ and let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(a) = ba$. Let $\epsilon_b : \mathbb{N} \to \mathbb{Z}$ be the unique function, whose existence is guaranteed by the Recursion Theorem, defined by $\epsilon_b(0) = 1$ and $\epsilon_b(n^+) = f(\epsilon_b(n)) = b\epsilon_b(n)$. Then $\epsilon_b(n)$ is defined to be b raised to the n^{th} power, and is denoted by b^n:

$$b^n = \epsilon_b(n).$$

Note that if $a \in \mathbb{Z}$, then b^a is undefined.

6. Embedding

We wish to show that, in a very meaningful sense, the natural numbers can be regarded as integers. To do this, we create an injective function $\mathbb{N} \hookrightarrow \mathbb{Z}$ which preserves all of the properties of the natural numbers with which we are concerned. That is, what matters to us about the natural numbers is not how they were defined, but how they behave. Specifically, they can be added and multiplied. Thus we want our injective function to preserve these properties.

Let $\phi : \mathbb{N} \to \mathbb{Z}$. We say that ϕ is an *embedding* if

- $\phi(1) = e$, where e is the multiplicative identity of $\mathbb{Z}$;
- $\phi(m + n) = \phi(m) + \phi(n)$;
- $\phi(mn) = \phi(m)\phi(n)$.

There is a unique function $\phi : \mathbb{N} \to \mathbb{Z}$ which satifies all of these properties, and it is given by $\phi(n) = [n, 0]$.

This also gives us additional properties which motivated us in the first place:

- $\forall n \in \mathbb{N} \exists b \in \mathbb{Z}$ such that $\phi(n) + b = \phi(0)$;
- $\forall a \in \mathbb{Z} \exists n \in \mathbb{N}$ such that either $a = \phi(n)$ or $a = -\phi(n)$.

The first of these says that $\mathbb{Z}$ contains the additive inverses of the natural numbers, and the second says that $\mathbb{Z}$ is, in some sense, the smallest set that does so.

Thus from now on, whenever it is convenient, we view $\mathbb{N}$ as a subset of $\mathbb{Z}$. Then to say that $a \in \mathbb{N} \cap \mathbb{Z}$ we mean that $a \in \phi(\mathbb{N}) \subset \mathbb{Z}$. The meaning should be clear from the context.

In particular, $\phi(1) = e$ by definition and $\phi(0) = z$ because the additive identity of $\mathbb{Z}$ is unique. Thus we identity 1 with e and 0 with z, and may drop these temporary names.

7. Order

Let $\phi : \mathbb{N} \hookrightarrow \mathbb{Z}$ be the embedding given by $n \mapsto [n, 0]$.
We define a relation $\leq$ on $\mathbb{Z}$ by

$$a \leq b \Leftrightarrow b - a \in \phi(\mathbb{N}).$$

This leads to other relations:

- $a < b \Leftrightarrow (a \leq b) \wedge (a \neq b)$;
- $a > b \Leftrightarrow \neg(a \leq b)$;
- $a \geq b \Leftrightarrow \neg(a < b)$.

Proposition 12. *The relation $\leq$ on $\mathbb{Z}$ is a total order.*

Proposition 13. *Let $m, n \in \mathbb{N}$. Then $m \leq n$ if and only if $\phi(m) \leq \phi(n)$.*

Proposition 14. *The relation $\leq$ on $\mathbb{Z}$ has the following properties:*

(1) $a \leq b \Rightarrow a + c \leq b + c$;
(2) $(c \geq 0) \wedge (a \leq b) \Rightarrow ac \leq bc$;
(3) $(c \leq 0) \wedge (a \leq b) \Rightarrow ac \geq bc$.

We define a function $|\cdot| : \mathbb{Z} \to \mathbb{N}$ by

$$|a| = \begin{cases} a \text{ if } a \geq 0; \\ -a \text{ otherwise .} \end{cases}$$

We call $|a|$ the *absolute value* of a.

8. Exercises

Construct the rational numbers as follows.

Exercise 1. Find an appropriate set on which to work. Define an relation on this set, and show that it is an equivalence relation. Define the set $\mathbb{Q}$ of rational numbers to be the equivalence classes of this equivalence relation.

Exercise 2. Define addition and multiplication on $\mathbb{Q}$ and show that it is well defined.

Exercise 3. Let $a, b, c \in \mathbb{Q}$. Show that

(1) $a + b = b + a$;
(2) $a + (b + c) = (a + b) + c$;
(3) $\exists! 0 \in \mathbb{Q}$ such that $a + 0 = a$;
(4) $\exists! - a \in \mathbb{Q}$ such that $a + (-a) = 0$;
(5) $ab = ba$;
(6) $a(bc) = (ab)c$;
(7) $\exists! 1 \in \mathbb{Q}$ such that $a1 = a$;
(8) $a \neq 0 \Rightarrow \exists a^{-1} \in \mathbb{Q}$ such that $aa^{-1} = 1$;
(9) $a(b + c) = ab + ac$.

The nine properties above assert that $\mathbb{Q}$ is a *field*.

Exercise 4. Define a relation on $\mathbb{Q}$ which coincides with the common notion of their ordering, and show that this is a total order relation.

Department of Mathematics, University of California, Irvine
E-mail address: pbailey@@math.uci.edu