Constructing the Integers

We have seen how we can start with an algebraic system – the (informal) system of integers $\mathbb{Z}$ and create new "algebraic systems" $\mathbb{Z}_m$ whose members are actually equivalence classes. We are going to use this same idea – creating a new system whose members are equivalence classes – to carefully define a new, formal algebraic system $\mathbb{Z}$.

We will start with ω, a system that we have already carefully built from set theory. In constructing ω, we used the informal system of whole numbers as the guide for what we wanted to build. Now, we will be guided by the informal system of integers. We want to carefully construct, from ω, a new formal system $\mathbb{Z}$ that "behaves in exactly the same way" as the informal system of integers.

In line with our view that "everything in mathematics is a set," $\mathbb{Z}$ will turn out to be a collection of sets, and each set in this collection will be called an integer. Since "behavior" is all that counts for mathematicians, we can then agree to call this collection the "official" set $\mathbb{Z}$ of integers.

As with ω, verifying all the details gets tedious, so we will only check some of them – but enough, hopefully, to convince you that what's omitted is really just "more of the same."

Historically, the negative integers (and 0) developed later than the natural numbers. They were only accepted in Europe in the 17th century. In one sense negative integers seemed absurd. This was because they were unfamiliar "new numbers" that seemed to represent "something less than nothing." Of course, that point of view now seems quaint; early schooling gets us "adjusted" to the idea of negative integers early on – and gives us very practical uses for them. It seems perfectly natural for us to answer the question "How much did the temperature change from 1 a.m. to 2 a.m.?" by saying " $-3°$ F." Similarly, we attach different physical meanings to the velocities 32 ft/s and -32 ft/s.

Why did people create the negative integers? As algebra developed, some very simple equations "demanded" solutions. In ω, we can solve equations like $x + 4 = 5$ but not other equations like $x + 5 = 4$. People found it more satisfying aesthetically to invent "new numbers" so that all equations of the form $x + m = n$ (where $m, n \in \omega$) would have a solution than to say that some such equations don't have a solution. Oddly, this aesthetic insight was valuable: these "new numbers" turned out also to be useful!

We use the informal system of integers as a motivation for our construction. An equation like $x + 5 = 4$ should have solution "$4 - 5$" in the integers but there is no such number in the whole number system ω – because we can't always subtract in ω. We want to construct an enlarged number system that contains an "answer" for "$4 - 5$" and, more generally, for all such "subtraction problems" with the whole numbers.

Early mathematicians, in effect, simply said "OK, we simply declare that there are some new numbers called -1, -2, ... and here's how they work: $4 - 5 = -1$, ... "

This is, in fact, exactly behavior we want. But rather than just announcing "we declare that the are such numbers...", our goal is to show how to define these numbers using things we already have (the whole numbers – which, in turn, were carefully defined earlier as sets).

The last few paragraphs above contain the seed of an idea. For example, we want to have a number "$4 - 5$." Starting with ω, we could try saying that the ordered pair $(4, 5)$ of whole numbers is an integer (to be called -1). It is the integer which answers the subtraction problem "$4 - 5$". Similarly, we could think of the ordered pair $(5, 4)$ as being the integer 1 (it is the "answer" to $5 - 4$).

"An integer is an ordered pair of whole numbers." This seems promising, but it's just a little too simple: this approach would give us "too many" integers. Reasoning as above, we would want the whole numbers pairs $(4, 5)$, $(9, 10)$, $(21, 22)$, ... to be integers representing the "answers" to $4 - 5$, $9 - 10$, $21 - 22$, ... In other words, these different ordered pairs should all be considered as being the same integer!

More generally, if $a - b = c - d$ (in the informal system $\mathbb{Z}$), we would want (a, b) and (c, d) to represent the same integer, and we can see how to write this condition about whole numbers without ever mentioning subtraction. We want the ordered pairs (a, b) and (c, d) to represent the same integer if $a + d = b + c$. We can arrange to treat them as "the same" by using an equivalence relation that puts them into the same equivalence class. All this motivates the following formal definition of the set of integers, $\mathbb{Z}$.

Definition For (a, b) and $(c, d) \in \omega \times \omega$, we define a relation

$$(a, b) \simeq (c, d) \text{ iff } a + d = b + c.$$

(*To reiterate: the definition uses addition in ω. It is informally motivated by looking at subtractions in the (informal) system of integers. For our formal definition, we can't start with $a, b, c, d \in \omega$ and refer to "$a - b$" and "$c - d$" because subtraction isn't defined inside ω. So instead we phrase what we want in terms of addition.*)

Theorem $\simeq$ is an equivalence relation on the set $\omega \times \omega$.

Proof Suppose (a, b), (c, d), $(e, f) \in \omega \times \omega$.

a) $\simeq$ is reflexive: $(a, b) \simeq (a, b)$ because $a + b = b + a$ in ω.
(*Here, and in the work that follows, all the calculations involving whole numbers $a, b, ...$ in ω are justified because of theorems that we already proved for ω – for example, the commutative, associative laws for addition and multiplication $+$, $\cdot$, the distributive law, cancellation laws for addition and multiplication in ω, ...*)

b) $\simeq$ is symmetric: If $(a, b) \simeq (c, d)$, then $(c, d) \simeq (a, b)$ because
if $a + d = b + c$, then $c + b = d + a$ in ω.

c) $\simeq$ is transitive: Suppose $\begin{cases} (a,b) \simeq (c,d) \\ (c,d) \simeq (e,f) \end{cases}$

that is, $\begin{cases} a+d = b+c & (1) \\ c+f = d+e & (2) \end{cases}$

We need to prove that $(a,b) \simeq (e,f)$.

Adding $e+f$ to both sides in (1) and rearranging (using the commutative and associative laws in ω) gives

$a+d+(e+f) = b+c+(e+f)$
$(a+f)+(d+e) = (b+e)+(c+f)$

Substituting $d+e$ for $c+f$ (from Equation (2)) gives

$(a+f)+(d+e) = (b+e)+(d+e)$.

Using the cancellation law for addition (which we proved for ω) to eliminate the $(d+e)$ on both sides, we get

$a+f = b+e$ (*), and that is what we needed to prove. •

What are the equivalence classes of $\simeq$ like? For example

$[(0,3)] = \{(0,3),\ (1,4),\ (2,5),\ (3,6),\ \ldots, (n,n+3), \ldots\}$ $\qquad (n \in \omega)$

We could also refer to this equivalence class as $[(1,4)]$ *or* $[(2,5)]$*, or ...* . $(0,3)$ *is just one possible choice as a representative for this class.*

Going back to the intuitive motivation, we think of this equivalence class as "the answer" to the all the problems $0-3,\ 1-4,\ 2-5,\ \ldots$. *If we think of this equivalence class as "an integer", it corresponds to the integer* -3 *(in the informal system of integers*).

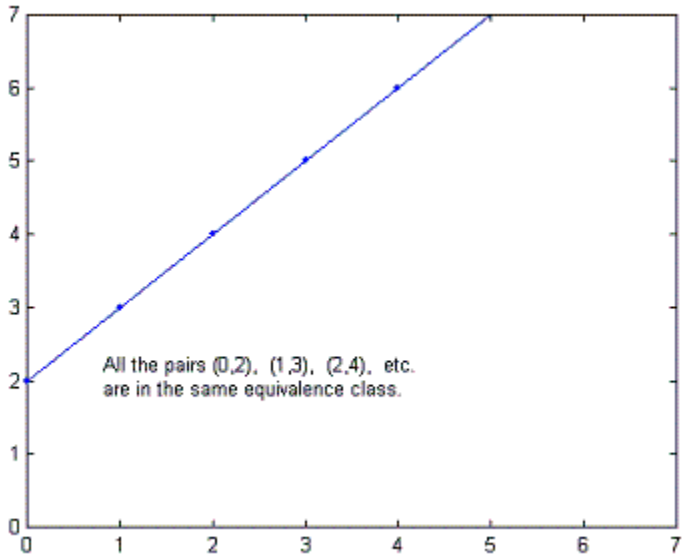
$[(1,0)] = \{(1,0),\ (2,1),\ (3,2),\ (4,3),\ \ldots, (n+1,n), \ldots\}$ $\qquad (n \in \omega)$

$[(0,0)] = \{(0,0),\ (1,1),\ (2,2),\ (3,3),\ \ldots,\ (n,n), \ldots\}$ $\qquad (n \in \omega)$

If we think of these equivalence classes as integers, they correspond to the integers 1 *and* 0 *in the informal system of integers.*

Although it's not necessary for our work, it might also help to picture these equivalence classes geometrically:

> The members of $\omega \times \omega$ are the points in the 1st quadrant of the plane, $\mathbb{R}^2$, with both coordinates whole numbers. Two different points (a, b) and (c, d) are equivalent iff $a + d = b + c$ iff $b - d = a - c$ iff $\frac{b-d}{a-c} = 1$ iff the straight line through (a, b) and (c, d) has slope 1.
>
> Therefore an equivalence class of $\simeq$ consists of all pairs of whole number pairs (a, b) that happen to lie on a particular straight line of slope 1. The dots (just the dots) on the part of the straight line shown below are some of the members in an equivalence class (*the parts of the straight line between dots are included just as a visual aid*). The particular equivalence class pictured is the one corresponding to the integer -2 in the informal system of integers.



Exercise: In the picture, equivalence classes representing negative integers lie on which straight lines? positive integers? the integer 0 *?*
Relate the picture relate to the content of the following theorem.

Theorem Every equivalence class $[(a, b)]$ contains an ordered pair with at least one 0 coordinate. Therefore every equivalence class can be written either as $[(0, k)]$ or $[(k, 0)]$ for some $k \in \omega$.

Proof (*Recall the definition of* $\leq$ *in* ω.) If $a \leq b$ in ω, then there is a $k \in \omega$ for which $a + k = b = b + 0$. This means that $(a, b) \simeq (0, k)$, so $[(a, b)] = [(0, k)]$.

If $b < a$ in ω, then there is a $k \in \omega$ for which $b + k = a = a + 0$. Then $(a, b) \simeq (k, 0)$, so $[(a, b)] = [(k, 0)]$. •

According to the theorem, we can list all the equivalence classes as:

$$..., [(0,3)],\ [(0,2)],\ [(0,1)],\ [(0,0)],\ [(1,0)],\ [(2,0)],\ [(3,0)], ...\ .$$

Officially, these equivalence classes are going to be "the integers." Here, finally, is the definition.

Definition $\mathbb{Z} = (\omega \times \omega)/\simeq$. A member of $\mathbb{Z}$ is called an integer.

We will now invent convenient names for these equivalence classes. (*Temporarily, we use underlining to distinguish integers from whole numbers.*)

$$\begin{aligned}
&\vdots\\
\underline{-3} &= [(0,3)]\\
\underline{-2} &= [(0,2)]\\
\underline{-1} &= [(0,1)]\\
\\
\underline{0} &= [(0,0)]\\
\\
\underline{1} &= [(1,0)]\\
\underline{2} &= [(2,0)]\\
\underline{3} &= [(3,0)]\\
&\vdots
\end{aligned}$$

In general, for each $n \in \omega$, the integer $[(0,n)]$ will be denoted $\underline{-n}$ and the integer $[(n,0)]$ will be denoted $\underline{n}$.

(*Of course, we could also write* $\underline{-2} = [(1,3)] = [(2,4)] = ...$.)

Before we continue, notice that each integer is a set. This is because each integer is a collection of ordered pairs of whole numbers, each ordered pair is itself a set, and each whole number is a set. For example, what set is the integer $\underline{2}$?

$\underline{2}$ is the set (equivalence class) $[(2,0)] = \{(2,0),\ (3,1),\ (4,2),\ ...\}$

Each member of the equivalence class is an ordered pair, and, in turn, an ordered pair is officially defined as a set: $(a,b) = \{\{a\},\{a,b\}\}$. So each ordered pair in $\underline{2}$ is itself a set. For example, $(2,0) = \{\{2\},\{2,0\}\}$

But 2 and 0 are whole numbers, and each whole number is a set:

$0 = \emptyset$ and
$2 = \{\emptyset,\{\emptyset\}\}$.

Therefore $(2,0) = \{\{2\},\{2,0\}\} = \{\{\{\emptyset,\{\emptyset\}\}\},\ \{\{\emptyset,\{\emptyset\}\},\ \emptyset\}\}$,

so $\underline{2} = [(2,0)]$

$= \{(2,0),\ (3,1),\ (4,2),\ \ldots\}$

$= \{\ \underline{\{\{\emptyset, \{\emptyset\}\}\}, \{\{\emptyset, \{\emptyset\}\}, \emptyset\}\}}, (3,1),\ (4,2),\ \ldots\} = \ldots$

↑

the pair $(2,0)$ is underlined; and each of the other ordered pairs can be similarly written as a set.

Answering the question "What is 2?" (from the first lecture) seems to get more and more complicated.

Of course, we don't want to constantly think about integers as sets; but remember that integers were built on the foundation of set theory.

Arithmetic in $\mathbb{Z}$

We want to define addition and multiplication in $\mathbb{Z}$. When we defined new addition and multiplication operations in $\mathbb{Z}_m$, we used special symbols for them: $\oplus$ and $\odot$. Strictly speaking, we should do something similar now – to avoid confusing the "new addition and multiplication" (to be defined in $\mathbb{Z}$) with the "old addition and multiplication" operations (already defined in ω).

However, by this time, we are probably sophisticated enough to avoid using that notational crutch. So we will simply write $+$ and $\cdot$ for the new addition and multiplication in $\mathbb{Z}$. The context (whether $+$ and $\cdot$ stand between two integers or between two whole numbers) determines whether they represent operations in $\mathbb{Z}$ or in ω.

Definition Suppose $[(a,b)] \in \mathbb{Z}$ and $[(c,d)] \in \mathbb{Z}$. Define

1) Addition in $\mathbb{Z}$: $[(a,b)] + [(c,d)] = [(a+c, b+d)]$.

The "$+$" between the integers on the left is the new addition being defined in $\mathbb{Z}$; the "$+$'s" between the whole numbers a, c, b, d on the right refer to addition as defined already in ω.

2) Multiplication in $\mathbb{Z}$: $[(a,b)] \cdot [(c,d)] = [(ac+bd, bc+ad)]$

Here is the motivation for the definition. We are thinking of the integers $[(a,b)]$ and $[(c,d)]$ as providing "answers" for the subtraction problems $(a-b)$ and $(c-d)$ in the informal system of integers. In that informal system, $(a-b)(c-d) = (ac+bd) - (bc+ad)$. So the product should be the integer that "answers" the subtraction problem $(ac+bd) - (bc+ad)$.

We pointed out earlier (when defining addition and multiplication in $\mathbb{Z}_m$) that when operations are defined in terms of representatives of equivalence classes (such as a, b, c, d), we must check that the operations are well-defined (independent of the representatives chosen from each equivalence class).

For example, in the present setting, $[(1,3)] = [(2,4)]$ and $[(3,5)] = [(6,8)]$. Does the definition of integer multiplication $[(1,3)] \cdot [(3,5)]$ give the same answer as it does for $[(2,4)] \cdot [(6,8)]$? We hope so – and that's what it means to say that "$\cdot$ is well-defined in $\mathbb{Z}$."

Theorem Addition and multiplication in $\mathbb{Z}$ are well-defined.

Proof Assume that $\begin{cases} [(a,b)] = [(c,d)] \text{ and} \\ [(e,f)] = [(g,h)] \end{cases}$ that is, $\begin{cases} a+d = b+c & (1) \\ e+h = f+g & (2) \end{cases}$

1) Addition: We need to show that

$$[(a,b)] + [(e,f)] = [(c,d)] + [(g,h)] \text{ , or equivalently, that}$$
$$[(a+e, b+f)] = [(c+g, d+h)] \quad (*)$$

Adding equations (1) and (2) and rearranging the terms (using the commutativity and associativity of addition in ω) gives

$$(a+e) + (d+h) = (b+f) + (c+g).$$

which says that (*) is true.

2) Multiplication: (*Here, the details are a little messier, but not hard.*)

We need to show that

$$[(a,b)] \cdot [(e,f)] = [(c,d)] \cdot [(g,h)] \text{ , that is}$$
$$[(ae+bf, be+af)] = [(cg+dh, dg+ch)], \text{ that is}$$
$$(ae+bf) + (dg+ch) = (be+af) + (cg+dh) \qquad (*)$$

Since $a+d = b+c$ and $e+h = f+g$, we see that

$$\begin{aligned} & e(a+d) + f(c+b) + c(e+h) + d(g+f) \\ = \; & e(b+c) + f(a+d) + c(f+g) + d(e+h) \end{aligned}$$

Multiplying out both sides of this equation and using commutativity and associativity in ω to rearrange gives

$$\begin{aligned} & (ae+bf+dg+ch) + (de+cf+ce+df) \\ = \; & (be+af+cg+dh) + (de+cf+ce+df) \end{aligned}$$

Using the cancellation law for addition in ω gives

$$ae+bf+dg+ch = be+af+cg+dh \qquad (*)$$

which is just what we needed to prove. •

Example Using these definitions, we can calculate and prove theorems about $\mathbb{Z}$.

$\underline{1} + \underline{3} = [(1,0)] + [(3,0)] = [(4,0)] = \underline{4}$
$\underline{3} + \underline{1} = [(3,0)] + [(1,0)] = [(4,0)] = \underline{4}$
Illustrating commutativity of addition in $\mathbb{Z}$

$\underline{2} \cdot \underline{4} = [(2,0)] \cdot [(4,0)] = [(2 \cdot 4 + 0 \cdot 0,\ 0 \cdot 4 + 0 \cdot 2)] = [(8,0)] = \underline{8}$
$\underline{4} \cdot \underline{2} = [(4,0)] \cdot [(2,0)] = [(4 \cdot 2 + 0 \cdot 0, 0 \cdot 2 + 4 \cdot 0)] = [(8,0)] = \underline{8}$
Illustrating commutativity of multiplication in $\mathbb{Z}$

$$\begin{aligned}(\underline{-1} + \underline{2}) + \underline{3} &= ([(0,1)] + [(2,0)]) + [(3,0)] = [(2,1)] + [(3,0)] \\ &= [(1,0)] + [(3,0)] \\ &= [(4,0)] \\ &= \underline{4}\end{aligned}$$

$$\begin{aligned}\underline{-1} + (\underline{2} + \underline{3}) &= [(0,1)] + ([(2,0)] + [(3,0)]) = [(0,1)] + [(5,0)] \\ &= [(5,1)] = [(4,0)] = \underline{4}\end{aligned}$$
Illustrating that addition is associative in $\mathbb{Z}$.

Do similar calculations to illustrate that multiplication in $\mathbb{Z}$ is associative and that the distributive law holds in $\mathbb{Z}$.

For $m, n \in \omega$:

$\underline{n} + \underline{0} = [(n,0)] + [(0,0)] = [(n+0, 0+0)] = [(n,0)] = \underline{n}$
$\underline{n} \cdot \underline{1} = [(n,0)] \cdot [(1,0)] = [(n \cdot 1 + 0 \cdot 0,\ 0 \cdot 1 + n \cdot 0)] = [(n,0)] = \underline{n}$
Showing that $\underline{0}$ *and* $\underline{1}$ *are the neutral "identity elements" for addition and multiplication in* $\mathbb{Z}$.

$\underline{n} + \underline{-n} = [(n,0)] + [(0,n)] = [(n,n)] = [(0,0)] = \underline{0}$, and similarly
$\underline{-n} + \underline{n} = \underline{0}$
An earlier theorem told us that every integer $[(a,b)]$ *can be written either as* $\underline{n} = [(n,0)]$ *or as* $\underline{-n} = [(0,n)]$. *Therefore this calculation shows that every integer has an additive inverse: an integer which adds to the given integer to produce* 0. *The additive inverse of* $\underline{n}$ *is* $-\underline{n}$; *the additive inverse of* $\underline{-n}$ *is* $\underline{n}$.

It's easy to show that the additive inverse of an integer is unique. (Look at the proof in class we did to show that the additive inverse of an element in a field is unique. The same proof works in $\mathbb{Z}$.)

The preceding examples either prove or illustrate that each of the field axioms except $6'$ is true in $\mathbb{Z}$. In the case of the illustrations, filling in the actual proofs is as easy as doing the illustrations. Here is a theorem of one fact merely illustrated above. .

Theorem Addition in $\mathbb{Z}$ is commutative.

Proof For any $[(a,b)]$ and $[(c,d)]$ in $\mathbb{Z}$,

$$\begin{aligned}[(a,b)]+[(c,d)] &= [(a+c,b+d)]\\ &= [(c+a,d+b)]\\ &= [(c,d)]+[(a,b)]. \quad \bullet\end{aligned}$$

Notice that we can prove that addition <u>in $\mathbb{Z}$</u> is commutative <u>because</u> we already proved that addition <u>in ω</u> is commutative: $a+c=c+a$, etc.

You should write down any additional proofs needed to show that the other field axioms (except 6′) are true in $\mathbb{Z}$.

Here are proofs of a few other arithmetic facts about $\mathbb{Z}$.

Theorem For any $\underline{z} \in \mathbb{Z}$, $z \cdot \underline{0} = \underline{0}$.

Proof Suppose $z=[(a,b)]$. Then $z \cdot \underline{0} = [(a,b)] \cdot [(0,0)] = [(a \cdot 0 + b \cdot 0,$
$b \cdot 0 + a \cdot 0)] = [(0,0] = \underline{0.}$ $\bullet$
$\uparrow$
(because $a \cdot 0 = 0$, $b \cdot 0 = 0$ and $0+0=0$ <u>in ω</u>)

Theorem (Cancellation Rule for Multiplication in $\mathbb{Z}$) Suppose $\underline{u}, \underline{v}, \underline{z} \in \mathbb{Z}$.
If $\underline{zu} = \underline{zv}$ and $\underline{z} \neq \underline{0}$, then $\underline{u} = \underline{v}$.

Proof We know that either $\underline{z}=[(k,0)]$ or $\underline{z}=[(0,k)]$ for some $k \in \omega$, and since $\underline{z} \neq \underline{0}$, we also know that $k \neq 0$. (*Note: Picking a representative for the equivalence class $\underline{z}$ that has a 0 coordinate is not necessary, but doing so makes the algebra easier – at the cost of making us consider two cases.*) Suppose $\underline{u}=[(c,d)]$ and $\underline{v}=[(e,f)]$

Case 1: $\underline{z}=[(k,0)]$, where $0 \neq k \in \omega$. Then

$\underline{zu} = \underline{zv}$, that is		
$[(k,0)] \cdot [(c,d)] = [(k,0)] \cdot [(e,f)]$	so	
$[(kc+0d,\ 0c+kd)] = [(ke+0f, 0e+kf)]$	so	
$[(kc,kd)] = [(ke,kf)]$		so
$(kc,kd) \simeq (ke,kf)$	so	
$kc+kf = kd+ke$	so	
$k(c+f) = k(d+e)$	Since $k \neq 0$, using the cancellation law for multiplication <u>in ω</u> gives	
$c+f=d+e$	that is,	

$(c, d) = (e, f)$ so
$[(c, d)] = [(e, f)]$ so
$\underline{u} = \underline{v}$

Case 2: $\underline{z} = [(0, k)]$, where $0 \neq k \in \omega$. Then

$\underline{zu} = \underline{zv}$, that is
$[(0, k)] \cdot [(c, d)] = [(0, k)] \cdot [(e, f)]$ so
$[(0c + kd,\ kc + 0d)] = [(0e + kf, ke + 0f)]$ so
$[(kd, kc)] = [(kf, ke)]$ so
$(kd, kc) \simeq (kf, ke)$ so
$kd + ke = kc + kf$ so
$k(d + e) = k(c + f)$ Since $k \neq 0$, using the cancellation law for multiplication <u>in ω</u> gives
$d + e = c + f$ that is,
$(c, d) = (e, f)$ so
$[(c, d)] = [(e, f)]$ so
$\underline{u} = \underline{v}$ •

At the beginning, as in the proofs for preceding theorems, we usually need to go all the way back to basics about $\mathbb{Z}$ to do a proof : an integer is an equivalence class $[(a, b)]$. But as more results about $\mathbb{Z}$ are proved, we can then use them to prove new theorems without needing to go all the way down to the equivalence class definition of an integer – as, for example, in proving the following corollary to the Cancellation Rule Theorem.

Corollary If $\underline{u}$, $\underline{v} \in \mathbb{Z}$ and $\underline{u} \cdot \underline{v} = \underline{0}$, then $\underline{u} = \underline{0}$ or $\underline{v} = \underline{0}$.

Proof We are given that $\underline{u} \cdot \underline{v} = \underline{0}$. By a previous theorem, $\underline{u} \cdot \underline{0} = \underline{0}$
$\underline{u} \cdot \underline{v} = \underline{u} \cdot \underline{0}$. If $\underline{u} \neq 0$, then $\underline{v} = \underline{0}$ by the Cancellation Theorem. •

Example (“Sign Rules” for Multiplication in $\mathbb{Z}$)

$$\begin{aligned}(\underline{-3}) \cdot 3 &= [(0, 3)] \cdot [(3, 0)] \\ &= [(0 \cdot 3 + 3 \cdot 0, 3 \cdot 3 + 0 \cdot 0)] \\ &= [(0, 9)] = \underline{-9}\end{aligned}$$

$$\begin{aligned}(\underline{-3}) \cdot (\underline{-3}) &= [(0, 3)] \cdot [(0, 3)] \\ &= [(0 \cdot 0 + 3 \cdot 3, 0 \cdot 3 + 3 \cdot 0)] \\ &= [(9, 0)] = \underline{9}\end{aligned}$$

More generally,

$$\begin{aligned}\underline{n}\cdot\ \underline{-m} &= [(n,0)]\cdot[(0,m)]\\ &= [(n\cdot 0+0\cdot m,\ 0\cdot 0+n\cdot m)] = [(0,n\cdot m)] = \underline{-(n\cdot m)}\end{aligned}$$

$$\begin{aligned}\underline{-n}\cdot\ \underline{-m} &= [(0,n)]\cdot[(0,m)] = [(0\cdot 0+n\cdot m,\ n\cdot 0+0\cdot m)]\\ &= [(n\cdot m,\ 0)] = \underline{n\cdot m}\end{aligned}$$

Subtraction in $\mathbb{Z}$

The fact that we can't subtract in ω is the problem we were trying to fix by enlarging the number system. Have we succeeded? Can we define subtraction in $\mathbb{Z}$?

We noted earlier that every integer can be written in the form $[(n, 0)]$ or $[(0, n)]$, where $n \in \omega$. We created the notation $\underline{n}$ and $\underline{-n}$ for these integers, and we checked that $\underline{n} + (\underline{-n}) = (\underline{-n}) + \underline{n} = \underline{0}$.

Integers are additive inverses (of each other) if their sum is $\underline{0}$. Thus, each integer $\underline{z}$ has an additive inverse $\underline{-z}$. (*This is not true in* ω.)

Definition Let $\underline{u}, \underline{v} \in \mathbb{Z}$. We define the difference $\underline{u} - \underline{v} = \underline{u} + (\underline{-v})$.

Thus, we define subtraction in terms of addition: "subtract v" means "add the additive inverse $\underline{-v}$."

Example

$$\underline{n} - \underline{n} = \underline{n} + (\underline{-n}) = \underline{0}$$

$$\underline{3} - \underline{2} = \underline{3} + (\underline{-2}) = [(3,0)] + [(0,2)] = [(3,2)] = [(1,0)] = \underline{1}$$

$$\underline{2} - \underline{3} = \underline{2} + (\underline{-3}) = [(2,0)] + [(0,3)] = [(2,3)] = [(0,1)] = \underline{-1}$$

$$\underline{3} - (\underline{-2}) = \underline{3} + (\textit{additive inverse of } \underline{-2})$$
$$= \underline{3} + \underline{2} = \underline{5}$$

Example In $\mathbb{Z}$, solve the equation $\underline{x} + \underline{3} = \underline{2}$.

Solution: Subtract $\underline{3}$ from both sides (*and use associativity, commutativity, etc., as needed)*

$$\underline{x} + \underline{3} - \underline{3} = \underline{2} - \underline{3} = \underline{-1}$$

All the usual arithmetic facts about addition, subtraction and multiplication in $\mathbb{Z}$ can be proved using what we have developed so far. None of the proofs are much different from what you've seen above. We assume, now, that all this has been done and that we can use all these results freely.

Order in $\mathbb{Z}$

The only additional thing we need in $\mathbb{Z}$ is to define an order relation, $\leq$.

Definition For each integer $\underline{z} \in \mathbb{Z}$, we write

$$\begin{cases} \underline{z} \leq \underline{0} & \text{iff } \underline{z} = [(0,k)] \\ \underline{0} \leq \underline{z} & \text{iff } \underline{z} = [(k,0)] \end{cases}$$

(*Of course, we agree that* $\underline{z} \leq \underline{0}$ *and* $\underline{0} \geq \underline{z}$ *mean the same thing.*)

By definition then: if $n \in \omega$, $\begin{cases} \underline{0} \leq \underline{n} & \text{because } \underline{n} = [(n,0)] \\ -\underline{n} \leq \underline{0} & \text{because } \underline{-n} = [(0,n)] \end{cases}$

Clearly, $\underline{z} \leq \underline{0}$ and $\underline{z} \geq \underline{0}$ iff $\underline{z} = [(0,0)] = \underline{0}$.

Definition For $\underline{v}, \underline{w} \in \mathbb{Z}$, we write $\underline{v} \leq \underline{w}$ iff $\underline{w} - \underline{v} \geq \underline{0}$. We write $\underline{v} < \underline{w}$ if $\underline{v} \leq \underline{w}$ and $\underline{v} \neq \underline{w}$.

With these definitions, we can prove all the usual rules for inequalities and how they interact with addition, subtraction and multiplication in $\mathbb{Z}$. A couple of example follow.

Theorem Suppose $\underline{v}, \underline{w} \in \mathbb{Z}$. If $\underline{v} \geq \underline{0}$ and $\underline{w} \geq \underline{0}$, than $\underline{v} \cdot \underline{w} \geq \underline{0}$.

Proof Since $\underline{v} \geq \underline{0}$ and $\underline{w} \geq \underline{0}$, $\underline{v} = [(k,0)]$ and $\underline{w} = [(l,0)]$ for some $k, l \in \omega$.
Then $\underline{v} \cdot \underline{w} = [(k,0)] \cdot [(l,0)] = [(kl + 0 \cdot 0, 0 \cdot l + k \cdot 0)] = [(kl,0)] \geq \underline{0}$. •

Corollary Suppose $\underline{u}, \underline{v}, \underline{w} \in \mathbb{Z}$. If $\underline{v} \geq \underline{w}$ and $\underline{u} \geq \underline{0}$, then $\underline{uv} \geq \underline{uw}$.

Proof $\underline{w} - \underline{v} \geq \underline{0}$ and $\underline{u} \geq \underline{0}$. By the preceding theorem $\underline{u} \cdot (\underline{w} - \underline{v}) \geq \underline{0}$, that is $\underline{uw} - \underline{vw} \geq \underline{0}$, so $\underline{uw} \geq \underline{vw}$. •

With these definitions, all the usual rules about inequalities in $\mathbb{Z}$ (and how the interacts with $+$ and $\cdot$) can be proved. We now assume that has been done and use those results in $\mathbb{Z}$ freely.

Concluding Comments

At this point we have given precise, formal definitions for ω (the whole number system) and $\mathbb{Z}$ (the system of integers:

$$\begin{array}{ll} \omega: & 0,\ 1,\ 2,\ 3,\ ... \\ \mathbb{Z}: & \underline{-3},\ \underline{-2},\ \underline{-1},\ \underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ ... \end{array}$$

The way we constructed things, the whole number 2 is not the same as the integer $\underline{2}$:

$$2 \neq \underline{2}$$

However, it's easy to check that the nonnegative integers $\underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ ...$ form a Peano system just as the whole numbers $0, 1, 2, 3...$ do. Since "all Peano systems look the same", the systems

$$\{\underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ ...\} \text{ and}$$
$$\{0,\ 1,\ 2,\ 3,...\}$$

behave exactly alike. We can think of $\{\underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ ...\}$ as simply being a "photocopy" of $\{0,\ 1,\ 2,\ 3...\}$ inside $\mathbb{Z}$. Therefore for ordinary mathematical purposes (that is, for work not concerned directly with the foundations of mathematics) we can treat the original $\{0,\ 1,\ 2,\ 3...\}$ and the copy $\{\underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ ...\}$ as being identical. If we do that, then we can think of ω as a subset of $\mathbb{Z}$

$$\begin{array}{ccccccccc} & & \{ & 0, & 1, & 2, & 3, & ...\} \\ & & & \downarrow & \downarrow & \downarrow & \downarrow & \\ \{..., & \underline{-3}, & \underline{-2}, & \underline{-1}, & \underline{0}, & \underline{1}, & \underline{2}, & \underline{3}, & ...\} \end{array}$$

In fact, to help us ignore the difference, we now throw away the notational crutch: for integers $\underline{2}$ and $\underline{-2}$, we drop the underlinings and just write 2 and -2. Notationally you can no longer tell whether 2 means "the whole number 2" or "the integer 2" but, unless we're back dealing with the foundations of the number system, the difference between them doesn't matter.

This new formal number system $\mathbb{Z}$ still has some serious deficiencies: for example, a simple equation like $2x = 1$ has no solution in $\mathbb{Z}$. We will briefly address that issue later by enlarging the system again to give a careful, formal construction of the set of rational numbers, $\mathbb{Q}$. It will turn out that each rational number is an equivalence class of pairs of integers.

We could move ahead and do this right now. But just to change the pace for a bit, we'll postpone the construction of $\mathbb{Q}$.