Constructing the Integers

We have seen how we can start with the (informal) system of integers, $\mathbb{Z}$ and use it to build new algebraic systems $\mathbb{Z}_m$. The members of $\mathbb{Z}_m$ are equivalence classes formed from the integers. If you think of the members of $\mathbb{Z}_m$ as "numbers" in this new system, then these "new numbers" are equivalence classes formed out of "old numbers" (integers).

When we constructed the whole number system ω, we used the intuitive, informal system of whole numbers as the guide for what we wanted to build. Starting with set theory, we built a collection of sets ω in which we were able to define $+$ and $\cdot$ (using the "successor set" operation). This collection of sets turned out to "act just like" the informal system of whole numbers. Therefore we agree to use ω as our official, formal definition of the system of whole numbers.

This time we will build on what we have already constructed. We will start with the whole number system ω and, using the behavior of the informal system of integers as our guide, we will create a new system in which we can add and multiply objects. When we're finished, this new system will "act just like" the informal system of integers. Since behavior is what's important, we can then agree to use this new system as our official, formal definition for $\mathbb{Z}$.

The objects in this new system will be equivalence classes of pairs of whole numbers. Each object (equivalence class) in the system will be an integer. Since each equivalence class is a set, and the members of each equivalence class are pairs of whole numbers (each of which is a set!) each integer will be a set – in line with our view that "everything in mathematics is a set."

As with ω, verifying every detail 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."

Before we begin, here's a bit of historical perspective. The negative integers (and 0) developed much later than the natural numbers. In Europe, they were only accepted in the 17th century. When they first began to appear on the scene, negative integers seemed absurd. This was because they were unfamiliar "new numbers" and it seemed like they we claiming to represent something "less than nothing." Of course, that point of view seems quaint to us; our schooling "conditions" us to the idea of negative integers very early – and it 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 these "unnatural" negative integers? Because some very simple equations "demanded" solutions. In ω, we can solve equations like $x + 4 = 5$ but not other equally simple equations like $x + 5 = 4$. On aesthetic grounds, mathematicians found that inventing "new numbers" so that all equations like $x + m = n$ (where $m, n \in \omega$) would have a solution was preferable to saying that some such equations don't have a solution. Oddly, this aesthetic feeling was valuable – because these "new numbers" turned out to be useful!

We begin our construction by thinking about what we want to build into this new system; we look to the informal system of integers for guidance. An equation like $x + 5 = 4$ has no solution in the whole number system, but it should have solution "$4 - 5$" in the integers. So we want the system we construct to contain an "answer" for the subtraction "$4 - 5$." In fact, it should contain an "answer" for every subtraction problem "$a - b$" where $a, b \in \omega$.

In effect, early mathematicians simply said "OK, we simply declare that there are some new numbers called $-1,\ -2,$ ... and here's how they work: $4-5=-1,$ ... " And this is, in fact, exactly behavior we want. But rather than just announcing "we declare that there are such numbers...", our goal is to show how to define these numbers using things we already have (the whole numbers).

The preceding two paragraphs contain the idea we will use. 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 going to be called an integer. It is the integer which answers the subtraction problem "$4-5$." Similarly, we might think of the ordered pair $(5,4)$ as being the integer 1 (it is the "answer" to $5-4$). So perhaps we could just simply say "an integer is an ordered pair of whole numbers."

This seems promising, but it's just a little too simple: this approach would tell us that each of the different pairs

$$\begin{array}{ll} (4,5) & (=\text{ answer to the subtraction "}4-5\text{"}) \\ (9,10) & (=\text{ answer to the subtraction "}9-10\text{"}) \\ (21,22) & (=\text{ answer to the subtraction "}21-22\text{"}) \\ \vdots & \end{array}$$

is a different integer and that's not we want: all those subtractions should "be answered" by the same integer.

So we devise an equivalence relation on $\omega\times\omega$ that puts all these pairs

$$..., (4,5), ..., (9,10), ..., (21,22), ...$$

into the same equivalence class: $\{ ..., (0,1), ..., (4,5), ..., (9,10), ..., (21,22), ... \}$.

This equivalence class of pairs of whole numbers is what will be called the integer -1.

Let's enlarge this idea: suppose a, b, c, d are whole numbers. Thinking again for guidance the informal system of integers, we see that if $a-b=c-d$, then we would want think of (a,b) and (c,d) as representing the same integer. We do this by saying that (a,b) and (c,d) are equivalent if $a+d=b+c$.

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 $\simeq$ by

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

> *Note: why not say "* $(a,b)\simeq(c,d)$ *iff* $a-b=c-d$*"? Looking at the preceding paragraphs, that would say exactly what we want to say. We motivated what we're doing by thinking about subtraction in the informal system of integers. But when we come to write the official definition to use in constructing the integers, we have only* ω *to work with, and subtraction isn't defined in* ω *: we're not allowed to say "*$a-b$*" or "*$c-d$*" for* $a, b, c, d\in\omega$ *. So, we sneakily say the same thing in a way that is allowed in* ω *– by*

switching over to the language of addition: $a + d$ and $b + c$ always <u>are</u> always defined in ω .

What we have done to this point is the real, creative part of the job. (*You should go back and reread it each day for a few days; especially, reread it after we've finished all the detailed work that comes next.*) Now, we need

i) to check that $\simeq$ really is an equivalence relation on $\omega \times \omega$, and
ii) to define a way to add and multiply the equivalence classes
iii) confirm that this new formal algebraic system $\mathbb{Z}$ really does "act just like" the informal system of integers.

Doing all this occupies several pages.

Theorem I1 $\simeq$ 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 we know that $a + b = b + a$ in ω.

(*Notice: here, and in the work that follows, <u>all the calculations involving whole numbers</u> $a, b, \ldots$ are done <u>in</u> ω, and they are justified because of <u>theorems that we already proved are true in ω</u> – for example, the commutative, associative laws for addition and multiplication,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 $\begin{cases} (a, b) \simeq (c, d) \\ (c, d) \simeq (e, f) \end{cases}$

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

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

If we add $e + f$ to both sides of (1) and rearrange (using the commutative and associative laws in ω) we get

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

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

But $d + e = c + f$ (from Equation (2), so substituting gives

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

The <u>cancellation law for addition</u> (which we proved

for ω) lets us cancel $(d + e)$ from both sides leaving

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

What do the equivalence classes of $\simeq$ look like? For example, here is the equivalence class containing the pairs that are equivalent to the pair $(0, 3)$:

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

Of course, $(0, 3)$ *is just one possible representative of this equivalence class. We could write the same equivalence class as* $[(3, 6)]$ *or* $[(18, 21)]$ *or ...*

Going back to the intuitive motivation, we think of this equivalence class as "the answer" to the all the problems $0 - 3,\ 1 - 4,\ 2 - 5,\ 3 - 6 \ldots$ *, that is, we want to say that this equivalence class is the integer* -3. *Similarly*

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

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

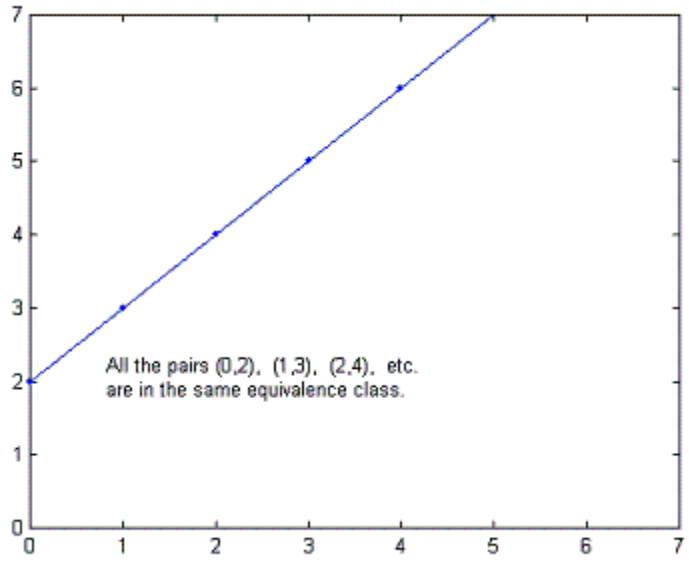
Our motivation indicates that we want to think of these equivalence classes as being the integer 1 *and the integer* 0.

But here we are getting just a little ahead of ourselves. We will do a little more work before we assign integer names to all the equivalence classes.

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

The set $\omega \times \omega$ can be pictured as those points in the first quadrant of $\mathbb{R}^2$ for which both coordinates are whole numbers. Two of these 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. (*How do we know that* $a - c \neq 0$*?*)

Therefore an equivalence class for $\simeq$ consists of all whole number pairs (a, b) that happen to lie on a line of slope 1. The dots on the part of the straight line in the figure below show some of the members in the equivalence class $\{(0, 2), (1, 3), (2, 4),\ \ldots\}$ (*the parts of the straight line between dots are included just as a visual aid*). The particular equivalence class pictured is the one that will be the integer -2 .



Exercise: In the picture, equivalence classes that contain points of the y-axis are (intuitively) going to correspond to which integers? The picture also suggests the following theorem.

Theorem I2 Every equivalence class $[(a,b)]$ contains exactly one ordered pair that has a 0 coordinate. (*If we use that pair to represent the equivalence class, then 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 $[(a,b)] = [(k,0)]$.

Uniqueness : Suppose $\begin{cases} (k,0) \text{ and } (m,0) & \text{or} \\ (0,k) \text{ and } (0,m) & \text{or} \\ (k,0) \text{ and } (0,m) \end{cases}$ are in the same equivalence class.

In the first two cases, it must be that $k = m$ so the pairs are the same; in the third case, it must be that $k = m = 0$. Therefore one equivalence class cannot contain two different pairs with a 0 coordinate. •

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

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

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

Definition $\mathbb{Z} =$ the set of equivalence classes of $\simeq$
$= (\omega \times \omega)/\simeq$.
A member of $\mathbb{Z}$ is called an integer (*so an integer is one of the equivalence classes*)

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" 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 we are going to define in $\mathbb{Z}$. The context (whether the symbols $+$ 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 $(1,3)] = [(2,4)]$ and $[(3,5)] = [(6,8)]$.

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

Theorem I3 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

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

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 messier, but not hard.*)

We need to show that

$$[(a,b)] \cdot [(e,f)] = [(c,d)] \cdot [(g,h)] \text{ , that is}$$

$$[(ae+bf, be+af)] = [(cg+dh, dg+ch)]. \quad \text{So we need to show that}$$

$$(ae+bf, be+af) \simeq (cg+dh, dg+ch), \text{ and that means we need to show that}$$

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

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 Now that addition and multiplication are defined, $\mathbb{Z}$ is an algebraic system. We will give the names $\underline{0}$ and $\underline{1}$ to the integers $[(0,0)]$ and $[(1,0)]$. We can then prove that all the Axioms F1-F5′ and F6 are true in $\mathbb{Z}$ (*these are the same axioms we talked about when discussing* $\mathbb{Z}_m$)

F1 There are elements $\underline{0}$ and $\underline{1}$ in $\mathbb{Z}$ and $\underline{0} \neq \underline{1}$

Let $x, y, z \in \mathbb{Z}$: say $x = [(a,b)]$, $y = [(c,d)]$ and $z = [(e,f)]$

F2 & F2′ Addition and multiplication in $\mathbb{Z}$ are associative

Proof that $(x+y)+z = x+(y+z)$

$$(x+y)+z = (\,[(a,b)]+[(c,d)]\,)+[(e,f)] \qquad = [(a+c,b+d)]+[(e,f)]$$

$$= [\,((a+c)+e,(b+d)+f)] = [\,(a+(c+e)),b+(d+f))]$$

↑ *because addition is associative in* ω

$$= [\,(a,b)]+(\,[(c,d)]+[(e,f)]\,) = x+(y+z)$$

Proof that $(x \cdot y)\cdot z = x\cdot(y\cdot z)$

$$(x\cdot y)\cdot z = (\,[(a,b)]\cdot[(c,d)]\,)\cdot[(e,f)] = [(ac+bd,bc+ad)]\cdot[(e,f)]$$

$$= [\,(ace+bde+bcf+adf,\ bce+ade+acf+bdf)]$$

and

$$x\cdot(y\cdot z) = [(a,b)]\cdot(\,[(c,d)]\ \cdot[(e,f)]\,) = [(a,b)]\cdot[(ce+df,de+cf)]$$

$$= [\,(ace+adf+bde+bcf,bce+bdf+ade+acf)]$$

$$= [\,(ace+bde+bcf+adf,\ bce+ade+acf+bdf)]$$

So the two computations come out the same (*using commutativity of addition and multiplication in* ω.)

F3 & F3′ Addition and multiplication in $\mathbb{Z}$ are commutative

Proof that $x+y = y+x$

$$x+y = [(a,b)]+[(c,d)] = [(a+c,b+d)] = [(c+a,d+b)]$$

↑

because addition is commutative in ω

$$= [(c,d)]+[(a,b)] = y+x$$

Proof that $x\cdot y = y\cdot x$

$$x \cdot y = [(a,b)] \cdot [(c,d)] = [(ac+bd, bc+ad)]$$
$$= [(ca+db, da+cb)] = [(c,d)] \cdot [(a,b)] = y \cdot x$$
$$\uparrow \textit{ because multiplication and addition are commutative in } \omega$$

F4 The distributive law holds in $\mathbb{Z}$

Proof that $x \cdot (y+z) = x \cdot y + y \cdot z$

$$x \cdot (y+z) = [(a,b)] \cdot ([(c,d)] + [(e,f)]) = [(a,b)] \cdot [(c+e, d+f)]$$
$$= [(ac+ae+bd+bf,\ bc+be+ad+af)]$$

and

$$x \cdot y + x \cdot z = [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)]$$
$$= [(ac+bd, bc+ad)] + [(ae+bf, be+af)]$$
$$= [(ac+bd+ae+bf,\ bc+ad+be+af)]$$
$$= [(ac+ae+bd+bf, bc+be+ad+af)]$$

So the two computations come out the same (what properties of arithmetic in ω are used?)

F5 & F5′ Neutral elements for addition and multiplication

Proof that $x + \underline{0} = x$

$$x + \underline{0} = [(a,b)] + [(0,0)] = [(a+0, b+0)] = [(a,b)] = x$$
$$\uparrow$$
$$\textit{Property of } 0 \textit{ in } \omega$$

Proof that $x \cdot \underline{1} = x$

$$x \cdot \underline{1} = [(a,b)] \cdot [(1,0)] = [(a \cdot 1 + b \cdot 0,\ b \cdot 1 + a \cdot 0)] = [(a,b)] = x$$
$$\uparrow$$
$$\textit{Properties of addition and multiplication in } \omega$$

F6 Existence of additive inverses

Suppose $x = [(a,b)] \in \mathbb{Z}$. We want to show that there is a $y \in \mathbb{Z}$ for which $x + y = \underline{0}$

Choose $y = [(b,a)]$. Then $x + y = [(a,b)] + [(b,a)] = [(a+b, b+a)]$

$$= [(0,0)]$$
$$\uparrow$$
$$\textit{because } (a+b, b+a) \simeq (0,0)$$
$$\textit{since } a+b+0 = b+a+0 \textit{ in } \omega\,.$$

Because $\mathbb{Z}$ is an algebraic system in which all the Axioms F1-F5′ and F6 are true, then all the definitions and theorems we proved from those axioms must be true in $\mathbb{Z}$. (*Here is a list of those*

theorems from the earlier notes; but here theorems have been renumbered to fit into the numbering sequence for the "integer theorems" in this set of notes). Therefore we know all of the following things about $\mathbb{Z}$:

Theorem I4 $(\forall x)(\exists!\, y)\ x + y = \underline{0}$

Definition I5 If $x \in \mathbb{Z}$, then the unique y for which $x + y = \underline{0}$ is denoted by $-x$.

Definition I6 We define subtraction in $\mathbb{Z}$ as follows: $x - y = x + (-y)$

Theorem I7 If $x \in \mathbb{Z}$, then $x \cdot \underline{0} = \underline{0}$

Theorem I8 **(**Various "sign rules") For all $x, y, z \in \mathbb{Z}$:

i) $-(x + y) = -x - y$
ii) $-(-x) = x$
iii) $(-x)y = -(xy)$
iv) $x(-y) = -(xy)$
v) $(-x)(-y) = xy$
vi) $x(y - z) = xy - xz$

Theorem I9 For all x, y, z: $\in \mathbb{Z}$: if $x + y = x + z$, then $y = z$.

$\mathbb{Z}$ is not a field. (*Why? In terms of the formal definition of integers, show why* $[(2, 0)]$ *cannot have a multiplicative inverse: if* $[(m, n)] \cdot [(2, 0)] = [(1, 0)]$, *then ... ? Therefore axiom F6′ is false in* $\mathbb{Z}$.) Nevertheless, it is possible to prove a cancellation theorem for multiplication.

Theorem I10 (Cancellation Rule for Multiplication in $\mathbb{Z}$) Suppose $u, v, x \in \mathbb{Z}$.
If $xu = xv$ and $x \neq 0$, then $u = v$.

Proof We know from Theorem I2 that either $x = [(k, 0)]$ or $x = [(0, k)]$ for some $k \in \omega$, and that $k \neq 0$ (since $x \neq \underline{0}$). (*Note: we could start out saying: "suppose* $x = [(a, b)]$*". Picking a representative pair for the equivalence class* x *that has a* 0 *coordinate is not necessary to do this proof, but it makes the algebra simpler. The trade-off is that we have to consider two cases.*)

Suppose $u = [(c, d)]$ and $v = [(e, f)]$

Case 1: $x = [(k, 0)]$, where $0 \neq k \in \omega$. Then $xu = xv$ becomes

$[(k, 0)] \cdot [(c, d)] = [(k, 0)] \cdot [(e, f)]$ 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 $k \neq 0$, we can use the cancellation law for multiplication already proved in ω to get

$c + f = d + e.$ Therefore

$(c, d) \simeq (e, f)$ so

$[(c, d)] = [(e, f)]$ so

$u = v$

Case 2: $x = [(0, k)]$, where $0 \neq k \in \omega$. Then $xu = xv$ becomes

$[(0, k)] \cdot [(c, d)] = [(0, k)] \cdot [(e, f)]$ 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 $k \neq 0$, we can use the cancellation law for multiplication already proved in ω to get

$d + e = c + f$ that is,

$(c, d) \simeq (e, f)$ so

$[(c, d)] = [(e, f)]$ that is,

$u = v$ •

As we begin to prove theorems in this system $\mathbb{Z}$, we might need to go all the way back to the basic definitions about $\mathbb{Z}$ to do a proof : that an integer is an equivalence class $[(a, b)]$, etc. But as more theorems about $\mathbb{Z}$ are proved, they can be used to make later proofs more efficient – as, for example, in proving the following corollary to Theorem I10.

Corollary I11 If $u, v \in \mathbb{Z}$ and $u \cdot v = \underline{0}$, then $u = \underline{0}$ or $v = \underline{0}$.

Proof We are given that $u \cdot v = \underline{0}$. By Theorem I7, $u \cdot \underline{0} = \underline{0}$ so $u \cdot v = u \cdot \underline{0}$. If $u \neq 0$, then $v = \underline{0}$ by cancellation (Theorem I10). •

As we noted following Theorem I2, we can list all the integers (equivalence classes) as follows:

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

Since $[(0,k)] + [(k,0]] = [(k,k)] = [(0,0)]$, we see that $[(0,k)]$ is the additive inverse for $[(k,0)]$. So we write $[(0,k)] = -[(k,0)]$.

Let's give the name $\underline{k}$ to the integer $[(k,0)]$. Then $-\underline{k} = -[(k,0)] = [(0,k)]$.
(*We already assigned the names* $\underline{0}$ *and* $\underline{1}$ *to the integers* $[(0,0)]$ *and* $[(1,0)]$ *earlier.*)

Then a list of all the different integers is:

$$..., \ -\underline{3}, \ -\underline{2}, \ -\underline{1}, \ \underline{0}, \ \underline{1}, \ \underline{2}, \ \underline{3}, \ ...$$

Here we are using an "underline" $\underline{k}$ as a name for the integer $[(k,0)]$ to distinguish between the integer $\underline{k}$ and the whole number k: they are not officially the same. For example:

The whole number 2 was defined to be the set $\{\emptyset, \{\emptyset\}\}$.

What set is the integer $\underline{2}$?

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

Each member of this equivalence class is an ordered pair, and an ordered pair is officially defined as a set: $(a,b) = \{\{a\}, \{a,b\}\}$. So each ordered pair in $\{ (2,0), (3,1), (4,2), ... \}$ 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

$\underline{2} = [(2,0)] = \{(2,0), (3,1), (4,2), ... \}$

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

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

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

Some Arithmetic in $\mathbb{Z}$

We can do additions and multiplications in $\mathbb{Z}$ by applying the definitions to the equivalence classes. Sometimes we can save time by using theorems like Theorem I8.

$$\underline{5}+\underline{2}=[(5,0)]+[(2,0)]=[(5+2,0)]=[(7,0)]=\underline{7}$$

$\uparrow$

$5+2=7$ *is an addition performed in* ω *where facts about addition of whole numbers have already been worked out.*

$$\underline{5}-\underline{2}=\underline{5}+(-\underline{2})=[(5,0)]+[(0,2)]=[(5,2)]=[(3,0)]=\underline{3}$$

$$\underline{2}-\underline{5}=\underline{2}+(-\underline{5})=[(2,0)]+[(0,5)]=[(2,5)]=[(0,3)]=-\underline{3}$$

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

$\uparrow$

Theorem I8 ii): $-(-x)=x$

$\underline{5}-\underline{5}=\underline{5}+(-\underline{5})=\underline{0}$: *we can either "work it out" like the examples above or, more simply, use the fact that* $\underline{5}$ *was defined as the additive inverse of* $\underline{5}$.

For multiplication:

$$\underline{5}\cdot\underline{2}=[(5,0)]\cdot[(2,0)]=[(5\cdot 2+0\cdot 0,\ 0\cdot 2+5\cdot 0)]=[(10,0)]=\underline{10}$$

$\uparrow$

$5\cdot 2=10$*, etc., are multiplications performed in* ω *where facts about multiplication of whole numbers have already been worked out.*

$$(-\underline{5})\cdot(-\underline{2})=[(0,5)]\cdot[(0,2)]=[(0\cdot 0+5\cdot 2,\ 5\cdot 0+0\cdot 2)]=[(10,0)]=\underline{10}$$

(*or, easier, using Theorem I8 v),* $(-\underline{5})\cdot(-\underline{2})=\underline{5}\cdot\underline{2}=\underline{10}$)

$$\underline{5}\cdot(-\underline{2})=[(5,0)]\cdot[(0,2)]=[(5\cdot 0+0\cdot 2,\ 0\cdot 0+5\cdot 2)]=[(0,10)]=-\underline{10}$$

(*or, easier, using Theorem I8 iv),* $\underline{5}\cdot(-\underline{2})=-(\underline{5}\cdot\underline{2})=-\underline{10}$

$(-\underline{5})\cdot\underline{2}=-\underline{10}$ *using Theorem I2 iii* (*or, you could work it out directly in terms of the equivalence classes*)

$$\underline{5}^2=[(5,0)]\cdot[(5,0)]=[(5^2,0)]=[(25,0)]=\underline{25}$$

We can also define "positive," "negative" and a relation called $<$ in $\mathbb{Z}$.

Here are the main ideas. We will explore a few of these facts about inequalities in $\mathbb{Z}$ in the homework.

Definition I13 Let $z \in \mathbb{Z}$.

i) z is called <u>positive</u> if $z = [(k, 0)]$ where $k \in \omega$ and $k \neq 0$
ii) z is called <u>negative</u> if $z = [(0, k)]$ where $k \in \omega$ and $k \neq 0$

$P =$ the set of positive integers is $\{[(1,0)], [(2,0)], [(3,0)], \ldots\} = \{\ \underline{1}, \ \underline{2}, \ \underline{3}, \ldots\}$
$N =$ the set of negative integers is $\{[(0,1)], [(0,2)], [(0,3)], \ldots\} = \{-\underline{1}, -\underline{2}, -\underline{3}, \ldots\}$

The sets P, N, and $\{\underline{0}\}$ are pairwise disjoint and $\mathbb{N} = N \cup \{\underline{0}\} \cup P$

Definition I14 For integers z, w we write $z > w$ (*or equivalently,* $w < z$) iff $z - w$ is positive.

Notice that, according to Definition I14, $z - \underline{0} = z$ <u>is positive means the same thing as</u> $z > \underline{0}$.

Using these definitions and the rules of algebra we developed in $\mathbb{Z}$, we can prove the standard facts about inequalities.

Just for example:

Theorem I15 Suppose $z, w \in \mathbb{Z}$ If $z \in \mathbb{Z}$ and $z \neq \underline{0}$, then $z^2 > \underline{0}$.

i) if $z > \underline{0}$, then $-z < \underline{0}$; if $z < \underline{0}$, then $-z > \underline{0}$.
ii) if $z > \underline{0}$ and $w > \underline{0}$, then $z \cdot w > \underline{0}$
iii) if $z < \underline{0}$ and $w < \underline{0}$, then $z \cdot w > \underline{0}$
iv) if $z > \underline{0}$ and $w < \underline{0}$, then $z \cdot w < \underline{0}$

Proof i) If $z > \underline{0}$, then $z = [(k, 0)]$ for some $k \in \omega$. Then $-z = [(0, k)]$, which is one of the negative integers. The proof of the other part is similar since $-[(0,k)] = [(k,0)]$.

ii) If z and w are both positive, then $z = [(k, 0)]$ and $w = [(m, 0)]$ for some $k, m \in \omega$. Then $z \cdot w = [(k,0)] \cdot [(m,0)] = [(km + 0 \cdot 0,\ 0 \cdot m + k \cdot 0)] = [(km, 0)]$ which is one of the positive integers.

iii) If z and w are both negative, then $z = [(0, k)]$ and $w = [(0, m)]$ for some whole numbers k and m. Then $z \cdot w = [(0,k)] \cdot [(0,m)] = [(0 \cdot 0 + k \cdot m,\ k \cdot 0 + 0 \cdot m)]$
$= [(km, 0)]$ which is one of the positive integers.

iv) Homework Exercise •

Theorem I16 Suppose $z, u, v \in \mathbb{Z}$. Then

i) if $u > v$ and $z > 0$, then $zu > zv$

ii) if $u > v$ and $z < 0$, then $zu < zv$

Proof Homework exercise.

Some Concluding Remarks

We could continue to prove additional theorems about the algebra of addition, multiplication and inequalities in the formal system $\mathbb{Z}$. But what we have done here already should be enough to convince you that this formal system $\mathbb{Z}$ "acts just like" the informal system of integers. Therefore we can agree that it is reasonable to use $\mathbb{Z} = (\omega \times \omega)/\simeq$ as the official definition of the set of integers.

The point is not that, henceforth, you should think of integers as equivalence classes of pairs of whole numbers. For day-to-day purposes, we will use the integers the way we always have. The point is that we have carefully constructed a collection $\mathbb{Z}$ that we consider to contain the "official" integers: the members of $\mathbb{Z}$, such as $\underline{2}$ and $\underline{5}$, behave just like the informal integers – and this system $\mathbb{Z}$ is constructed entirely of sets. We are gradually seeing that "everything in mathematics" (whole numbers, integers, relations,...) can be formulated in terms of sets.

We should now make one last agreement about notation.

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

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

We noticed, earlier, that

$$\begin{array}{ll} & 2 = \{\emptyset, \{\emptyset\}\} \\ \text{and} & \underline{2} = [(2,0)] = \{\, \underline{\{\{\emptyset, \{\emptyset\}\}\, ,\, \{\{\emptyset, \{\emptyset\}\}, \emptyset\}\}},\ \ldots\, ,\ \} \end{array}$$

Because of the way we constructed whole numbers and integers, the whole number 2 is not (officially) the same as the integer $\underline{2}$:

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

However, it's easy to check that the sets

$$\begin{cases} \{\underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ \ldots\ \} & \text{with successor operation "add } \underline{1}\text{"} \quad \text{and} \\ \{0,\ 1,\ 2,\ 3, \ldots\ \} & \text{with successor operation "add } 1\text{"} \end{cases}$$

are both Peano systems, and "all Peano systems look the same." In other words,

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

behave in exactly the same way, so we can think of $\{\underline{0},\ \underline{1}, \underline{2},\ \underline{3},\ \ldots\}$ as simply being a "photocopy" of $\{0,\ 1,\ 2,\ 3\ldots\}$ inside $\mathbb{Z}$:

$$\begin{array}{rl} & \{\ 0,\ \ 1,\ \ 2,\ \ \ 3,\ \ldots\} \\ & \quad\downarrow\ \ \downarrow\ \ \downarrow\ \ \downarrow \\ \{\ldots,\ \underline{-3},\ \underline{-2},\ \underline{-1},\ \underline{0},\ \ \underline{1},\ \ \underline{2},\ \ \underline{3}, \ldots\} & \end{array}$$

Therefore for ordinary mathematical purposes (that is, for work not concerned directly with the foundations of the number systems) we can treat the original $\{0,\ 1,\ 2,\ 3...\}$ and the copy $\{\underline{0},\ \underline{1},\ \underline{2},\ \underline{3},\ ...\}$ as being identical. If for convenience we make that mental identification, then we can think of ω as a subset of $\mathbb{Z}$

In fact, to help us ignore the difference, we now throw away the notational crutch: for an integer $\underline{k}$, we drop the underlining and just write k. This means that the notation no longer tells you whether "2" means "the whole number 2" or "the integer 2." But, unless we consciously dealing with questions about the foundations of mathematics, the difference between them doesn't matter. Behavior is what counts!

The algebraic system $\mathbb{Z}$ works well for some purposes, but it still has serious mathematical deficiencies: for example, a very simple equation like $2x = 1$ has no solution in $\mathbb{Z}$. We will briefly address that issue later by enlarging the number system again and giving 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.

> *For those who would like to think ahead and be inventive:*
>
> *Think about the "informal" rational number $\frac{-1}{2}$ and ask how we could construct a formal definition for it using the integers we have already constructed.*
>
> *Perhaps we could think of $\frac{-1}{2}$ as being an ordered pair of integers: $(-1, 2)$. Similarly, maybe we could think of the ordered pair $(-2, 4)$ as the formal definition for $\frac{-2}{4}$. But for the informal system of rationals, $\frac{-2}{4} = \frac{-1}{2}$. So we would want*
>
> $(-1, 2)$ *and* $(-2, 4)$ *and* $(-3, 6)$ *and* $(4, -8)$ *and ...*
>
> *all to represent the same rational number. This suggests that the rational "one-half" should be an equivalence class like*
>
> $\{..., (-1, 2),\ (-2, 4),\ (-3, 6),\ (4, -8),\ ...\}$
>
> *The official definition of $\mathbb{Q}$ actually is: $\mathbb{Q} = \{(z, w) :\ z, w \in \mathbb{Z},\ w \neq 0\} /\ \simeq$, where $\simeq$ is some equivalence relation.*
>
> *Then the "official" $\mathbb{Q}$ is the set of all equivalences classes. How would you define the relation $\simeq$?*