

**MATH 304: CONSTRUCTING THE REAL NUMBERS<sup>†</sup>****Peter Kahn****Spring 2007****Contents**

<b>2</b>	<b>The Integers</b>	<b>1</b>
2.1	The basic construction . . . . .	1
2.2	Adding integers . . . . .	7
2.3	Ordering integers . . . . .	18
2.4	Multiplying integers . . . . .	20

**2 The Integers**

Before we begin the mathematics of this section, it is worth recalling the mind-set that informs our approach. We have started with a basic axiom, The Axiom of Integrality (or, equivalently, the Peano Axioms), and some logic and set-theory background to build the set of natural numbers  $\mathbb{N}$ , together with its usual operations and order relation. In this section, we continue this constructive process, using only the same logic and set-theoretic background, to enlarge  $\mathbb{N}$  so as to obtain the familiar system of integers.

**2.1 The basic construction**

Our starting point will be Exercise 8 of the section on natural numbers (Section 1), as well as the observation immediately preceding it. That is, for arbitrary natural

---

<sup>†</sup>©May 21, 2007

numbers  $a$  and  $b$ , we consider the following predicate in the variable  $x$ , which, for now, is assumed to range over the natural numbers.

$$E_{a,b}(x) : a + x = b. \quad (1)$$

The observation in question asserts the first of two following statements, whereas Exercise 8 asks you to prove the second:

$$(\exists x)E_{a,b}(x) \iff a \leq b. \quad (2)$$

$$((\exists x)(\exists y)(E_{a,b}(x) \wedge E_{a,b}(y)) \Rightarrow (x = y)).$$

In particular, unless  $a \leq b$ , there are no specializations of  $x$  in  $\mathbb{N}$  for which  $(\exists x)E_{a,b}(x)$  is true. We consider this a limitation on the system  $\mathbb{N}$ . To overcome this limitation, we try to enlarge  $\mathbb{N}$ , i.e., to enlarge the set over which the variable  $x$  is allowed to vary. The hope is that if we do this in the right way, meaningful solutions to all possible equations like (1) can be found.

One natural inclination is to posit a “hypothetical solution” for each equation. Of course, some of these already exist as elements of  $\mathbb{N}$ , but perhaps the others could be somehow constructed and adjoined to  $\mathbb{N}$  to give us the larger system. So, we could start with the idea that each equation has such a hypothetical solution. However, even before getting into the problem of how to actually construct such a solution for each equation, we need to assure ourselves that a given equation cannot determine more than one solution, and we need to deal with the question of what to do if *different* equations have the *same* solution.

We shall do all this, by conducting a couple of mental experiments. For each experiment, we *pretend* that the desired enlarged system can be constructed as desired—that is, it contains  $\mathbb{N}$ , and it has a “+” operation extending that of  $\mathbb{N}$ , with all the analogous properties (cf., Theorem 2 of Section 1)—and we suppose that, for any  $a$  and  $b$  in  $\mathbb{N}$ , solutions to equation (1) can be found in the enlarged system.

For the first experiment, choose any natural numbers  $a$  and  $b$ , keep them fixed, and consider two possibly different solutions to (1), say  $r$  and  $s$ . Then, we have two equations,

$$a + r = b, \text{ and}$$

$$b = a + s.$$

Here, we are using the symmetry property of the relation of equality to get the second equation from (1). Now we add the equations, obtaining,

$$(a + r) + b = b + (a + s).$$

Since we are assuming that our hypothetical system follows the usual algebraic rules, we can manipulate this last equation, cancel  $a + b$  from both sides, and conclude that  $r = s$ . This experiment shows that if we are able to construct an enlarged system as described, then each equation has exactly one solution.

Hypothetical solutions are unique

**Exercise 1.** In the above experiment, why didn’t we simply “solve” the equations, obtaining  $r = b - a$  and  $s = b - a$ , thus concluding that  $r = s$ ?

For the second experiment, let us suppose we have two equations  $E_{a,b}$  and  $E_{c,d}$ ,

with  $a, b, c, d \in \mathbb{N}$ , each having the same solution, say  $r$ . We express these as follows:

$$a + r = b, \quad \text{and}$$

$$d = c + r.$$

Adding these two equations and doing the usual algebra, we may cancel  $r$ 's from both sides, coming up with

$$a + d = b + c. \tag{3}$$

So if  $E_{a,b}$  and  $E_{c,d}$  have the same solution in our enlarged system, then the natural numbers  $a, b, c$ , and  $d$  must satisfy condition (3). That is, this argument shows that (3) is a *necessary* condition for  $E_{a,b}$  and  $E_{c,d}$  to have the same solution.

Condition for two equations to have the same solution

But condition (3) is also a *sufficient* condition for  $E_{a,b}$  and  $E_{c,d}$  to have the same solution. To verify this, assume only that you are given equation (3) and a hypothetical solution  $r$  of either  $E_{a,b}$  or of  $E_{c,d}$ . Then, using this information, proceed to show that  $r$  is also a solution of the other equation.

**Exercise 2.** Verify this last assertion.

Therefore, this experiment shows that, assuming solutions exist,  $E_{a,b}$  and  $E_{c,d}$  will have the same solutions *if and only if* condition (3) holds.

These two experiments now lead us to the following construction.

We consider the set  $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ , which consists of all ordered pairs  $(a, b)$ ,  $a \in \mathbb{N}$  and  $b \in \mathbb{N}$ . Each such pair corresponds to an equation  $E_{a,b}$ . We want to think of  $(a, b)$  as a solution to  $E_{a,b}$ , but this won't quite work. It won't work, in part, because if  $(a, b)$  and  $(c, d)$  are different pairs satisfying (3), they should represent the same solution:

i.e., they should be equal, which they are not. However, this problem is easily solved by defining an equivalence relation on the set  $\mathbb{N}^2$ , as follows:

**Definition 1.** If  $a, b, c, d$  are natural numbers, we say that  $(a, b)$  is *solution-equivalent* to  $(c, d)$ , written  $(a, b) \sim (c, d)$ , if and only if equation (3) holds: i.e.,  $a+d=b+c$ .

**Exercise 3.** Verify that  $\sim$  is an equivalence relation.

The equivalence class of a pair  $(a, b)$  is usually denoted by  $[(a, b)]$ , but we'll abbreviate this to  $[a, b]$  for convenience. The equivalence class  $[a, b]$  consists of all pairs  $(c, d)$  that are solution-equivalent to  $(a, b)$ , and these pairs correspond to all equations  $E_{c,d}$  having the same hypothetical solution as  $E_{a,b}$ . Therefore, it makes sense to use the class  $[a, b]$  to stand for this hypothetical solution.

By definition, the set of all equivalence classes  $[a, b]$  is known as the quotient set  $\mathbb{N}^2 / \sim$  (cf. the section on equivalence classes in the *Set Theory* notes). We shall give this set a new name and symbol.

**Definition 2.** Each equivalence class  $[a, b]$  is called an *integer*. The set of all integers, which is just the quotient set  $\mathbb{N}^2 / \sim$ , will be denoted by  $\mathbb{Z}$ .

The  
integers

The set  $\mathbb{Z}$  is certainly a reasonable candidate for the set of hypothetical solutions for our enlarged system. However, a lot of ingredients are still missing:

- For example, we have not explained in what sense our original set  $\mathbb{N}$  can be considered to be a subset of  $\mathbb{Z}$ .
- Further, we have not discussed how to add two integers.
- Moreover, even if we fill these gaps, we still have to verify that our goal has been met: namely, that the integers we have constructed can really be considered as honest solutions to the equations (1).

- Looking ahead, we have to come up with a reasonable way to define an ordering of integers which is compatible with the ordering of the natural numbers.
- Finally, we need to define a suitable notion of multiplication of integers.

The first of these gaps can be filled by part (a) of the following exercise, as we explain below.

**Exercise 4.** Prove each of the following.

- For any natural numbers  $a, b$ ,  $[0, a] = [0, b] \iff a = b$ .
- For any natural numbers  $a, b$ ,  $[a, 0] = [b, 0] \iff a = b$ .
- For any natural numbers  $a, b$ ,  $[a + b, a] = [b, 0]$  and  $[a, a + b] = [0, b]$ .

Notice that if we choose  $b = 0$  in part (c), we may conclude that for any  $a$ ,  $[a, a] = [0, 0]$ . This fact will be useful for later computations.

Part (a) of this exercise shows us how we may consider  $\mathbb{N}$  to be a subset of  $\mathbb{Z}$ . Namely, we define the function  $\iota : \mathbb{N} \rightarrow \mathbb{Z}$  by the rule

$$\iota(n) = [0, n],$$

for each  $n \in \mathbb{N}$ . Part (a) tells us that  $\iota$  is injective. This means that  $\iota$  maps  $\mathbb{N}$  injectively into  $\mathbb{Z}$ , specifically onto the subset of  $\mathbb{Z}$  consisting of all integers of the form  $[0, n]$ . This suggests that we should *identify* each natural number  $n$  with the corresponding integer  $\iota(n)$ , that is with  $[0, n]$ . (The word “identify” here is mathematical parlance for “consider to be identical with.”) In fact, we shall be doing this shortly. But before we do, we need to be sure that all the structure we have built for  $\mathbb{N}$  (e.g.,

addition) carries over to  $\mathbb{Z}$  in such a way that the identification we wish to make preserves this structure. Therefore, we are now led to consider the definition of addition for integers.

## 2.2 Adding integers

We want to define an addition operation for integers  $[a, b]$  which reflects our idea of adding solutions to equations (1). So, again, we perform a mental experiment. Suppose that  $r$  is a hypothetical solution of  $E_{a,b}$  and  $s$  is a hypothetical solution of  $E_{c,d}$ . Then, what should  $r + s$  be a solution of? Well, maybe this is so obvious as to be rhetorical, the answer being, of course, the sum of the two equations. But, even though it's obvious, let's work it out. We have

$$\begin{aligned} a + r &= b, \text{ and} \\ c + s &= d, \end{aligned}$$

so, clearly, this gives

$$(a + c) + (r + s) = (b + d).$$

In other words, the sum  $r + s$  should be the hypothetical solution for  $E_{a+c, b+d}$ . This conclusion, then, motivates the following definition:

**Definition 3.** For any integers  $[a, b]$  and  $[c, d]$ , we define the sum  $[a, b] \oplus [c, d]$  by the equation

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

Adding  
integers

We use the unusual sum symbol  $\oplus$  instead of  $+$  for the time being to distinguish it from the addition of natural numbers that we defined earlier and for which we used the symbol  $+$ . The definition of  $\oplus$  has been well-motivated (we hope), but is it well-posed? Recall what this means (cf. the section on equivalence relations in the *Set Theory* notes): We are using the representatives  $(a, b)$  and  $(c, d)$  of the equivalence classes  $[a, b]$  and  $[c, d]$ , respectively, to write the defining expression on the right-hand side of the equation. One must check that different choices of representatives will not affect the value of this right-hand side. The following exercise insures this:

**Exercise 5.** Suppose that  $(a_1, b_1) \sim (a_2, b_2)$  and  $(c_1, d_1) \sim (c_2, d_2)$ . Then prove that  $(a_1 + c_1, b_1 + d_1) \sim (a_2 + c_2, b_2 + d_2)$ .

Make sure you understand how this exercise shows that the foregoing definition is well-posed.

We shall now use the definition to derive some key properties of the operation  $\oplus$ .

**Theorem 1.** *Let  $a, b, c, d, e, f$  be any natural numbers. Then the following hold:*

$$a. [a, b] \oplus ([c, d] \oplus [e, f]) = ([a, b] \oplus [c, d]) \oplus [e, f] \quad (\text{associative law}).$$

$$b. [a, b] \oplus [0, 0] = [a, b] = [0, 0] \oplus [a, b] \quad (\text{identity law}).$$

$$c. [a, b] \oplus [b, a] = [0, 0] = [b, a] \oplus [a, b] \quad (\text{inverse law}).$$

$$d. [a, b] \oplus [c, d] = [c, d] \oplus [a, b] \quad (\text{commutative law}).$$

The first three properties listed are precisely the defining axioms in the definition of a mathematical structure called a *group*. The fourth property is the additional axiom needed to define a *commutative group*. We shall discuss groups further in an exercise at the end of this subsection.

**Exercise 6.** Prove each of the following:

- a. Suppose that  $[x, y]$  is an integer such that, for every integer  $[a, b]$ , we have  $[a, b] \oplus [x, y] = [a, b]$ . (In other words, assume that  $[x, y]$  satisfies the same property that  $[0, 0]$  does in part (b) of the above theorem.) Then  $[x, y] = [0, 0]$ .
- b. Suppose that  $[a, b]$  is any given integer and  $[x, y]$  is an integer that satisfies  $[a, b] \oplus [x, y] = [0, 0]$ . Then,  $[x, y] = [b, a]$ .
- c. Suppose that  $a$  and  $b$  are natural numbers satisfying  $[a + b, a] = [a, a + b]$ . Then  $b = 0$ . Conclude that if  $c$  and  $d$  are natural numbers satisfying  $[c, d] = [d, c]$ , then  $[c, d] = [0, 0]$ .
- d. Suppose  $[a, b] \oplus [e, f] = [c, d] \oplus [e, f]$ . Then  $[a, b] = [c, d]$ . (cancellation law)
- e. Suppose that  $[a, b]$  and  $[c, d]$  are any integers. Construct an integer  $[x, y]$  such that  $[a, b] \oplus [x, y] = [c, d]$ , and show that there is only one such integer.

There are a number of important comments to make about the items in Exercise 6:

- The identity law of Theorem 1 tells us that there exists *at least* one additive identity in  $\mathbb{Z}$ . Item (a) of Exercise 6 tells us that there is *at most* one additive identity. So, there is exactly one additive identity in the set of integers. One practical consequence of this is that we can prove an integer  $[a, b]$  is equal to  $[0, 0]$  by showing that  $[a, b]$  satisfies the defining property of an additive identity.
- The inverse law of Theorem 1 tells us that each integer has *at least* one additive inverse. Item (b) of the Exercise tells us that each integer has *at most one* inverse. So, each integer  $[a, b]$  has exactly one additive inverse. One practical

Uniqueness  
of  
identity

Uniqueness  
of  
inverses

consequence of this is that to prove two integers are equal, it is sufficient to prove that each is the additive inverse of some single integer. Sometimes this is a useful proof technique (cf. Exercise 7 below).

We shall use the notation  $-[a, b]$  to denote the additive inverse of  $[a, b]$ . Since the inverse law of Theorem 1 tells us that  $[b, a]$  is the additive inverse of  $[a, b]$ , we must have  $-[a, b] = [b, a]$ .

Once we have introduced this  $-$  symbol, expressions such as  $[a, b] \oplus (-[c, d])$  make perfectly good sense. However, it becomes unwieldy to write these out, so we introduce the standard shorthand

—  
notation

$$[a, b] - [c, d] \quad \text{to stand for} \quad [a, b] \oplus (-[c, d]).$$

Finally, once we use expressions like  $[a, b] - [c, d]$ , we are led to think of  $-$  as representing a binary operation on integers. (See Exercise 11 below.)

- Item (e) in the above exercise shows that every equation of the type that began this discussion of integers has a unique solution in  $\mathbb{Z}$ . We elaborate on this below.

**Exercise 7.** Prove that  $-(-[a, b]) = [a, b]$  by showing that each side of the equation is the additive inverse of  $-[a, b]$ . (Note: There is a more direct proof in this special case: namely,  $-(-[a, b]) = -[b, a] = [a, b]$ . The point of the exercise is to illustrate the described method, which also applies to a wide variety of other cases, as we may have occasion to see later.)

**Exercise 8.** Verify that  $\iota$  preserves addition. That is, prove that, for any natural numbers  $a$  and  $b$ ,  $\iota(a + b) = \iota(a) \oplus \iota(b)$ . (Recall that  $\iota(a) = [0, a]$ .)

This means that whether we consider  $a$  and  $b$  as natural numbers as before and add them using the definition of the previous section (getting  $a + b$ ), or whether we think of them as integers and use the new addition operation of integers (getting  $a \oplus b$ ), the result will be the same.

Therefore, it no longer makes much sense to use distinct symbols for each of these addition operations, so we shall replace  $\oplus$  by the simpler  $+$ .

We now tie together some of the notational conventions we have introduced.

- We have identified each natural number  $n$  with  $\iota(n) = [0, n]$ . Accordingly, let us now denote this integer simply by the same symbol  $n$ . Notice that this implies that the additive identity of  $\mathbb{Z}$ , which is  $[0, 0]$ , is then denoted by the usual symbol for additive identities, namely  $0$ . Correspondingly, the additive inverse of  $[0, m]$ , i.e.,  $[m, 0]$ , which was denoted as  $-[0, m]$  will now be called  $-m$ . Since  $-[0, 0] = [0, 0]$ , we have the usual equality  $-0 = 0$ .

Identify  
 $\mathbb{N}$   
with a  
subset  
of  $\mathbb{Z}$

By this notational change, we make it easier to use  $\iota$  to identify  $\mathbb{N}$  with a subset of  $\mathbb{Z}$ . For in the new notation,  $\iota(n) = n$ . So, from now on, we simply consider  $\mathbb{N}$  to be a subset of  $\mathbb{Z}$ .

- By the definition of addition, every integer  $[a, b]$  can be written as follows:

$$[a, b] = [0, b] + [a, 0] = [0, b] + (-[0, a]) = [0, b] - [0, a] = b - a.$$

The nice thing about the notation  $b - a$  in place of  $[a, b]$  is that it shows clearly how every integer is obtained by adding a natural number to the (additive) inverse

of some other natural number. Moreover, we can see that

$$b - a = d - c$$

if and only if  $b + c = a + d$ , either directly from the definition of what it means for  $[a, b]$  to equal  $[c, d]$ , or by using the  $+$  operation of integers and doing the usual algebraic manipulation. Both approaches yield the same thing.

Thus, to summarize, we have constructed a set  $\mathbb{Z}$ , which we call the set of integers, and we have shown that it contains the natural numbers  $\mathbb{N}$  as well as the additive inverses of these. It is useful to have some notation for the set of all additive inverses of the natural numbers (i.e., the negatives of the natural numbers), so we use the notation  $-\mathbb{N}$  for this set.

**Exercise 9.** Show that every integer is either a natural number or the additive inverse of a natural number. Show, moreover, that the only integer that is both a natural number and the additive inverse of a natural number is the additive identity 0.

This can be summarized by the equations  $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$  and  $\{0\} = \mathbb{N} \cap (-\mathbb{N})$ .

For this part of the construction of the integers, it remains only to introduce the standard notation and to summarize the results obtained in terms of that notation.

From now on, *we'll use the usual lower case letters,  $a, b, c, \dots, j, k, \ell, m, n$ , etc. to denote both integers and natural numbers*, specifying which is which when it is important to do so. Thus, Theorem 1 becomes:

**Theorem 2.** *Let  $a, b, c$  be any integers. Then the following hold:*

$$a. \quad a + (b + c) = (a + b) + c \qquad \text{(associative law).}$$

b.  $a + 0 = a = 0 + a$  *(identity law)*.

c. *Given  $a$ , there exists an integer  $\tilde{a}$  such that  $a + \tilde{a} = 0 = \tilde{a} + a$*  *(inverse law)*.

d.  $a + b = b + a$  *(commutative law)*.

Of course, as we have already said,  $\tilde{a}$  is uniquely determined by  $a$ , and we write  $\tilde{a} = -a$ . (Recall that we have already defined  $-$  for all integers:  $b - a = b + (-a)$ , for all integers  $a$ , and  $b$ .)

**Exercise 10.** Verify the following, for all integers  $a$  and  $b$ :

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

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

Now reconsider part (e) of Exercise 6. We shall rewrite this in terms of our new notational conventions: Let  $a$  and  $b$  be any integers. Then, part (e) of Exercise 6 asserts that the equation

$$a + x = b \tag{4}$$

has a unique solution in  $\mathbb{Z}$ . Here  $x$  represents a variable ranging over  $\mathbb{Z}$ . Compare equation (4) with equation (1). The equations look identical. In the earlier equation, we use only natural numbers. The  $+$  is the addition operation defined for the natural numbers, and the variable  $x$  is assumed to vary over  $\mathbb{N}$ . In each of these particulars, the new equation represents an extension of the old. In equation (4),  $a$  and  $b$  represent any integers, including natural numbers. The  $+$  operation is the addition defined for integers, which we have seen extends the addition operation defined for natural numbers. And, finally, the variable  $x$  ranges over the set  $\mathbb{Z}$  which contains the set  $\mathbb{N}$ .

So, we have extended our system to  $\mathbb{Z}$  in such a way as to obtain unique solutions for all the desired equations.

It remains to discuss the order properties of the integers and also integer multiplication, which we do in the next two subsections.

**Exercise 11.** A *binary operation* on a set  $S$  is simply a function  $\diamond : S \times S \rightarrow S$ . For such an operation, when we are given  $(s, t) \in S \times S$ , we usually write the function value  $\diamond(s, t)$  as  $s \diamond t$ . (Do not confuse this operation notation with the notation we use for binary relations.) Examples of such binary operations are addition and multiplication of natural numbers, addition of integers (and many similar examples). These examples satisfy nice properties, for instance, like those given by Theorem 2 (and a similar theorem in the section on natural numbers). Subtraction of integers can also be considered as a binary operation: just define  $b - a = b + (-a)$  (as we did when we switched to this notation above). Verify the following for this binary operation on  $\mathbb{Z}$ : (a) Subtraction has a unique identity element, which, in fact, equals 0. (b) For every integer  $b$ , there is an integer  $\hat{b}$ , such that  $b - \hat{b} = 0$ . (c) Subtraction is not commutative. (d) Subtraction is not associative.

We now introduce a concept that plays a very important role in almost every branch of mathematics: the concept of a *group*.

**Definition 4.** A *group* consists of a set  $X$ , together with a binary operation on  $X$ , say,  $\bullet : X \times X \rightarrow X$ , such that  $\bullet$  satisfies an associative law, an identity law, and an inverse law. Sometimes we write the group as a pair  $\langle X, \bullet \rangle$ , if we want to emphasize the role of the operation; sometimes, when the operation is clearly understood, we write the group simply as  $X$ .

Concept  
of a  
group

If  $\langle X, \bullet \rangle$  is a group such that the group operation  $\bullet$  additionally satisfies a commutative law, then we call  $\langle X, \bullet \rangle$  a *commutative group*.

For the reader's convenience, we amplify on the properties that  $\bullet$  must satisfy in order for  $\langle X, \bullet \rangle$  to be a group : (i) for all  $x, y, z \in X$ ,  $x \bullet (y \bullet z) = (x \bullet y) \bullet z$ ; (ii) there exists an element  $e \in X$  such that, for all  $x \in X$ ,  $x \bullet e = x = e \bullet x$ ; this element is called an identity in  $X$ ; (iii) for every  $x \in X$ , there is an element  $x' \in X$  such that  $x \bullet x' = e = x' \bullet x$ ; this element is called an inverse of  $x$ . For  $\langle X, \bullet \rangle$  to be a commutative group,  $\bullet$  must also satisfy the following: (iv) for all  $x, y \in X$ ,  $x \bullet y = y \bullet x$ .

**Exercise 12.** a. Explain why the natural numbers, together with the operation of addition, do *not* form a group.

b. Verify that the integers, together with the operation of addition, *do* form a commutative group.

c. Verify that the set of non-zero real numbers, together with the operation of multiplication, form a commutative group. (You may use the standard facts about real numbers for this exercise.)

d. Verify that the set  $\{0, 1\}$ , together with the operation of mod 2 addition, forms a group.

e. Verify that the set of all  $k \times n$  matrices with real entries, together with the operation of matrix addition, form a commutative group.

f. \* This exercise and the next one are for students familiar with matrix multiplication. Verify that the set of all  $n \times n$  matrices with real entries and non-zero

Examples  
of groups

determinant, together with the operation of matrix *multiplication*, form a group. (In this exercise, as in the ones that follow below, the *first* thing one has to do is to check that the set is *closed* under the given operation. This was pretty obvious in the preceding exercises, but it is less obvious for this one and for those that follow. Thus, given any two elements as described, apply the operation to them, and then verify that what you get is again in the given set.) Is this group commutative? If so, prove it; if not, explain why not.

- g. \* Let  $G$  be the set of all  $2 \times 2$  matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

such that  $a, b, c, d$  are all *integers* and  $ad - bc = \pm 1$ . Verify that  $G$ , together with the operation of matrix multiplication, forms a group.

- h. \* This exercise is for students familiar with complex numbers. Let  $H$  denote the set of all complex numbers  $a + bi$  such that  $a^2 + b^2 = 1$ . (In the usual representation of complex numbers as points in the plane,  $H$  corresponds to all the points on the unit circle.) Verify that  $H$ , together with the operation of complex multiplication, forms a commutative group.

In the following exercise, we consider an arbitrary group  $\langle X, \bullet \rangle$ .

**Exercise 13.** Prove the following:

- a. There is only one identity in  $X$ . (Thus, the element  $e$ , which is described in the definition as *an* identity, is actually *the unique* identity in  $X$ .)

- b. For each  $x \in X$ , there is only one inverse element. (We denote it by  $x^{-1}$ ).
- c. A cancellation law: For all  $x, y, z \in X$ ,  $x \bullet z = y \bullet z \Rightarrow x = y$ .
- d. An equation law: For any  $a, b \in X$ , there is a unique  $x \in X$ , such that

$$a \bullet x = b.$$

The  $\bullet$  notation is slightly annoying visually, so we shall now revert to the more modest  $\cdot$  notation for group operations, or, even more modestly, we may even suppress the  $\cdot$  and just use juxtaposition, as in the case of multiplication of real numbers.

Just as in the case of the integers, the associative law in any group can be extended to cover any number of elements, not just three. This can be derived from the given associative law by an inductive argument: we do not go into this in these notes. As a consequence, we can write the product of any number of elements in a group without having to bother to use parentheses to pair elements. When there are  $n$  elements, and all of them are equal to a single element, say  $x$ , then their product can be written simply as a power,  $x^n$ . Thus, powers are defined for elements in any group, just as they are for, say, real numbers. Further, in any group, one uses the standard convention that  $x^0 = e$ , for any  $x$ . Finally, for any natural number  $n$ , one uses the notation  $x^{-n}$  to stand for  $(x^{-1})^n$ . This defines the expression  $x^m$  for any  $x$  in the group and any integer  $m$ .

With these conventions, the student should have no trouble proving the following exponential laws:

**Exercise 14.** (a)  $(x^m)^n = x^{mn}$ , for all  $x \in X$  and for all integers  $m, n$ ; (b)  $(x^m)(x^n) = x^{m+n}$ . (Prove these results first when  $m$  and  $n$  are natural numbers, either using

induction or using a less formal method of grouping terms and counting. Then extend to the cases in which one or both of the numbers  $m$  and  $n$  is negative.)

**Exercise 15.** \* This exercise assumes that the student has had some familiarity with the elementary theory of numbers (e.g., divisibility properties, prime numbers, division algorithm, Euclidean algorithm). Consider a group  $\langle X, \cdot \rangle$ . If  $x$  is an element of  $X$ , then we say that  $x$  has *finite order* provided (i)  $x \neq e$ , and (ii) there exists a natural number  $n > 0$  such that  $x^n = e$ . If  $x$  has finite order, then we define the *order of  $x$* , written  $\text{ord}(x)$  to be the *minimal* natural number  $n > 0$  such that  $x^n = e$ .

As an example, in the case that  $X$  is the set of non-zero reals and the operation is multiplication, then 1 does not have finite order (because it equals the identity), but  $-1$  does have finite order because  $-1 \neq 1$  and  $(-1)^2 = 1$ . In fact,  $-1$  is the only real number that has finite order.

Back to the general case of a group  $\langle X, \cdot \rangle$ .

(a) Suppose that  $x \in X$  is not equal to  $e$ , and  $x^n = e$ , for some positive natural number  $n$ . Prove that  $n$  must be a multiple of  $\text{ord}(x)$ .

(b) Suppose that  $F$  is the set of all elements of finite order in  $X$ , and assume that  $F$  is not empty. Let  $m$  be the minimum of all natural numbers  $\text{ord}(x)$ , for  $x$  ranging over  $F$ . Prove that  $m$  is a prime number.

## 2.3 Ordering integers

We now want to define an order relation on  $\mathbb{Z}$  that extends the order relation we have already established for  $\mathbb{N}$  and has all the properties we intuitively associate with the usual ordering of the integers. Technically, there is more than one way to proceed

here—as is often the case—but they all amount to the same thing in the end. We'll adopt the following as a definition of the order relation because it simply extends our earlier definition for  $\mathbb{N}$ .

**Definition 5.** Let  $m$  and  $n$  be integers. We say that  $m$  is less than or equal to  $n$ , written  $m \leq n$ , provided there exists a natural number  $k$  such that  $m + k = n$ . In this case, we may also write  $n \geq m$ . We shall also use, without further comment, the strict orderings  $<$  and  $>$  associated with  $\leq$  and  $\geq$ , respectively.

Clearly this definition extends our earlier notion of  $\leq$  defined exclusively for natural numbers. The following result states that  $\leq$  and  $<$  have all the basic properties that we expect for the ordering of the integers. Each statement either follows from a similar statement about natural numbers or can be derived easily from definitions.

**Theorem 3.** *a. For any  $m, n \in \mathbb{Z}$ , exactly one of the following holds:  $m < n$ ,  $m = n$ , or  $m > n$ .*

*b. For any  $n \in \mathbb{Z}$ , the following are equivalent: (i)  $n \in \mathbb{N}$ , (ii)  $n \geq 0$ ,  $-n \leq 0$ .*

*c. For any  $m, n \in \mathbb{Z}$ ,  $m < n \iff -n < -m$ .*

*d. For any  $m, n, p \in \mathbb{Z}$ ,  $m < n \wedge n < p \implies m < p$ ; (transitivity of  $<$ ).*

*e. For any  $n \in \mathbb{Z}$ ,  $\neg(n < n)$ .*

*f. Every non-empty subset of  $\mathbb{Z}$  that is bounded below contains a smallest element.*

*g. For all  $m, n, p \in \mathbb{Z}$ ,  $m < n \iff m + p < n + p$ .*

**Definition 6.** Let us call an integer *positive* if it is  $> 0$  and *negative* if it is  $< 0$ .

**Exercise 16.** Prove assertions a)-g) of Theorem 3.

This completes our additive picture of the ordered integers. What remains is to introduce multiplication and to check that it interacts appropriately with addition and the order relation.

## 2.4 Multiplying integers

The motivation for the following complicated-looking definition of multiplication goes back to our intuitive view of integers as representing solutions to certain equations. Accordingly, for the moment, we shall revert to our older notation for integers to discuss this. Specifically,  $[a, b]$  is the solution to the equation  $a + x = b$  and  $[c, d]$  is the solution to  $c + y = d$ . Set  $r = [a, b]$  and  $s = [c, d]$ . We again conduct a mental experiment, supposing that multiplication of integers has been defined so as to satisfy the usual properties. We can thus multiply the two equations

$$a + r = b, \quad \text{and}$$

$$c + s = d,$$

and then add  $ac$  to both sides, obtaining

$$ac + rc + as + rs + ac = bd + ac, \quad \text{which becomes}$$

$$(a + r)c + a(c + s) + rs = bd + ac, \quad \text{hence}$$

$$(bc + ad) + rs = bd + ac.$$

The last equation shows that the hypothetical product  $rs$  is a solution to the equa-

Another  
mental  
experiment

tion  $E_{bc+ad, bd+ac}$ . (Notice that the multiplication appearing in the subscripts of this symbol is multiplication of natural numbers, which has already been defined.) Therefore, still using our older notation, we are led to make the following definition for multiplication of integers, for which we temporarily use the symbol  $\otimes$ :

**Definition 7.** Given integers  $[a, b]$  and  $[c, d]$ , we define  $[a, b] \otimes [c, d]$  by the rule

Multi-  
plication

$$[a, b] \otimes [c, d] = [ad + bc, bd + ac] \quad (5)$$

Of course, the first thing one must check, is that this definition of  $\otimes$  is well-posed. This is done via the following exercise:

**Exercise 17.** \* Suppose  $[a, b] = [w, x]$  and  $[c, d] = [y, z]$ , then  $[ad + bc, bd + ac] = [wz + xy, xz + wy]$ . (Hint: First prove the result under the additional assumption that  $w = a$  and  $x = b$ . Then conclude that the result also holds if, instead, one assumes  $y = c$  and  $z = d$ . Finally, prove the general case by combining the two special cases.)

Therefore, assuming the exercise is done, we have a well-defined binary operation  $\otimes$  on  $\mathbb{Z}$ . Let us see how this works for natural numbers. Recall that the natural number  $m$  can also be written as  $[0, m]$ , and the natural number  $n$  can be written as  $[0, n]$ . Applying the definition of  $\otimes$ , we get

$$m \otimes n = [0 \cdot n + m \cdot 0, mn + 0 \cdot 0] = [0, mn] = mn.$$

That is, for natural numbers, the operation  $\otimes$  coincides with the multiplication operation already defined. We can go through a similar computation for negatives of natural numbers, and the product of a negative and a positive, etc. A tally of these computations is easy to list. We do so in the following exercise:

**Exercise 18.** Let  $m$  and  $n$  be natural numbers. Then

a.  $m \otimes n = mn = (-m) \otimes (-n)$ .

b.  $(-m) \otimes n = -(mn) = m \otimes (-n)$ .

Of course, these computations, each of which can be done in a manner similar to the computation above, yield just what one wants and expects from multiplication of integers. Since every integer is either a natural number or an additive inverse of a natural number (Exercise 9), the above list gives all possible multiplications of two integers in terms of the multiplication of two natural numbers. Using these, together with what we know about multiplication and addition of natural numbers, or using the definition of multiplication directly, we can prove the following theorem.

**Theorem 4.** *Let  $m, n, p$  be any integers. Then:*

a.  $m \otimes (n \otimes p) = (m \otimes n) \otimes p;$  *(associative law)*

b.  $m \otimes n = n \otimes m;$  *(commutative law)*

c.  $m \otimes 1 = 1 \otimes m = m;$  *(identity law)*

d. *If  $m > 0$  and  $n < p$ , then  $m \otimes n < m \otimes p$ .*

e. *If  $m < 0$  and  $n < p$ , then  $m \otimes n > m \otimes p$ .*

f.  $m \otimes (n + p) = m \otimes n + m \otimes p;$  *(distributive law)*

g. *If  $m \otimes n = 0$ , then either  $m = 0$  or  $n = 0$ .* *(no zero divisors)*

h. *Suppose  $m \neq 0$ . Then  $m \otimes n = m \otimes p \Leftrightarrow n = p;$*  *(cancellation law)*

**Exercise 19.** Prove this theorem.

**Exercise 20.** Suppose that  $a$  is an integer  $> 1$ . Show that there is no integer  $b$  such that  $a \otimes b = 1$ . (Hint: First show that no integer  $b < 1$  can satisfy  $a \otimes b = 1$ . Then, show that if  $b \geq 1$ , then  $a \otimes b > 1$ .) Can you come to the same conclusion if  $a$  is an integer  $< -1$ ?

This exercise shows that  $\mathbb{Z}$  is not a group with respect to the operation  $\otimes$ . However, putting together the commutative-group properties of addition of integers together with properties (a), (b), (c), (f) of multiplication in the above theorem, we obtain all of the axioms for what is known as a *commutative ring*. That is,  $\mathbb{Z}$ , together with its two operations of addition and multiplication, is an example of a commutative ring. This concept is important enough to merit a separate definition:

**Definition 8.** A set  $R$ , together with two binary operations, say  $+$  and  $\cdot$ , is known as a *commutative ring* if  $\langle R, + \rangle$  is a commutative group ( i.e.,  $+$  satisfies properties (a)-(d) of Theorem 1) and  $\cdot$  satisfies the associative law, the commutative law, and the identity law ( i.e., properties (a)-(c) of Theorem 4), and finally, the two operations together satisfy the distributive law (property (f) of Theorem 4).

The following aspects of this definition are worth noting:

- The cancellation property (property (h) above) of integer multiplication, which extends the cancellation property of multiplication of natural numbers, can sometimes serve the same purpose as multiplicative inverses do, since we often multiply by multiplicative inverses in order to cancel a number from one side or both sides of an equation.
- For any commutative ring, it is not hard to verify that property (g) above and property (h) are equivalent. Property (g) is sometimes expressed by saying “ $\mathbb{Z}$

has no zero divisors.” Even though the term “zero-divisor” may seem mysterious, the property looks pretty obvious. However, as is often said, looks can be deceiving. Property (g) (or, equivalently, property (h)) does not follow from the other axioms for a commutative ring).

- Property (g) is a special property that only some rings (like the integers) have. In other words, there are many examples of commutative rings that *do* have zero divisors, i.e., they have *non-zero* elements, say  $r$  and  $s$  such that  $rs = 0$ . Students who have had a course in number theory will recall that the ring of integers mod  $n$  is an example of such a ring whenever  $n$  is a composite number (i.e., not a prime). For example, in the ring of integers mod 6, the numbers 2 and 3 are zero divisors, because in that ring,  $2 \neq 0$  and  $3 \neq 0$ , but  $2 \cdot 3 = 0$ . We shall have the occasion to discuss and use the concept of zero-divisor again later.
- Finally, suppose that  $R$ ,  $+$ , and  $\cdot$  satisfy all of the properties of a commutative ring *except* that  $\cdot$  is not commutative. (Note: We still assume that  $+$  is commutative.) Then,  $R$ , together with  $+$  and  $\cdot$  is called, simply, a *ring*. There are many important examples of rings that are not commutative rings. A familiar example is provided by the set of  $n \times n$  real matrices, which we denote by  $\mathcal{M}_n$ , together with the operations  $+$  and  $\cdot$  of matrix addition and matrix multiplication, respectively. Since matrix multiplication is not commutative for  $n \times n$  matrices when  $n > 1$ ,  $\mathcal{M}_n$  is a non-commutative ring for  $n > 1$ .

The computations listed in Exercise 18 show that  $\otimes$  is simply an extension of the multiplication operation defined earlier on  $\mathbb{N}$ . Moreover, it continues to have the

same basic properties that our earlier-defined multiplication operation in  $\mathbb{N}$  did (i.e., associativity, commutativity, identity). So, we may now drop our insistence on having a separate symbol for this (just as we did earlier in the case of addition). That is, we now write  $mn$  or  $m \cdot n$  instead of  $m \otimes n$  for the product of any two integers  $m$  and  $n$ .

For the reader's convenience, we now rewrite Theorem 4 in terms of the new notation:

**Theorem 5.** *Let  $m, n, p$  be any integers. Then:*

a.  $m(np) = (mn)p;$  *(associative law).*

b.  $mn = nm;$  *(commutative law).*

c.  $m \cdot 1 = 1 \cdot m = m;$  *(identity law)*

d. *If  $m > 0$  and  $n < p$ , then  $mn < mp$ .*

e. *If  $m < 0$  and  $n < p$ , then  $mn > mp$ .*

f.  $m(n + p) = mn + mp;$  *(distributive law).*

g. *If  $mn = 0$ , then either  $m = 0$  or  $n = 0$ .* *(no zero divisors).*

h. *Suppose  $m \neq 0$ . Then  $mn = mp \Leftrightarrow n = p$ ;* *(cancellation law).*

**Exercise 21.** The *definition* of multiplication of integers given in equation (5) can now be written as

$$(b - a) \cdot (d - c) = (bd + ac) - (ad + bc),$$

for all natural numbers  $a, b, c, d$ . Extend the notation by considering  $a, b, c, d$  to be any *integers*, and then use the listed properties in Theorem 5, together with whatever properties of addition that are needed, to *prove* the equality for all integers.

**Exercise 22.** Prove that  $m \cdot 0 = 0 \cdot m = 0$ , for any integer  $m$ .

**Exercise 23.** Let  $a$  and  $b$  be any integers. Prove:

$$ab > 0 \Leftrightarrow (a > 0 \wedge b > 0) \vee (a < 0 \wedge b < 0).$$

Now, the fact that the multiplicative inverse property does not hold for  $\mathbb{Z}$ , is similar to the failure of the additive inverse property in the case of  $\mathbb{N}$ . In that case, the absence of additive inverses was exactly what made some of the equations  $E_{a,b}$  unsolvable when restricting to natural numbers. In the present case, we can look at equations

$$M_{a,b} : ax = b,$$

which are just multiplicative analogs of the  $E_{a,b}$ , and we can ask about their solvability. Here, we are thinking of  $a$  and  $b$  as being arbitrary *integers*.

Our first observation is that when  $a = 0$ , the equation  $M_{a,b}$  almost never has a solution: it follows from Exercise 22 that it only has a solution when  $b = 0$ , and in that case, *every* integer qualifies as a solution. So, if we want *unique* solvability, we'd better stipulate at the outset that we don't want  $a$  to equal 0. So, let's proceed under that restriction from now on.

Our second observation is that even when  $a \neq 0$ , there are still many situations in which the equation  $M_{a,b}$  has no solution in  $\mathbb{Z}$ . Indeed, Exercise 20 tells us that whenever  $a > 1$ , then  $M_{a,1}$  has no solution in  $\mathbb{Z}$ . And the reader can readily supply

other examples.

Analogously to the cases in which equation (1) has no natural-number solution, we regard the unsolvability of some  $M_{a,b}$  as a defect in our system of integers  $\mathbb{Z}$ . So, we proceed by analogy with what we have done earlier in this section: namely, we enlarge  $\mathbb{Z}$  to obtain a number system satisfying all the expected rules but also allowing us to uniquely solve equations  $M_{a,b}$ , for any integers  $a, b$  with  $a \neq 0$ .