CHAPTER 3: THE INTEGERS $\mathbb{Z}$

MATH 378, CSUSM. SPRING 2009. AITKEN

1. Introduction

The natural numbers are designed for measuring the size of finite sets, but what if you want to compare the sizes of two sets? For example, you might want to compare the number of of chairs in a classroom with the number of students to determine the number of free chairs. If there are more students than chairs, you would use *negative integers* to indicate the absence of free chairs.

Again, natural numbers are good for indicating the number of times you want to iterate a function $f : S \to S$. But what if you want to allow iterations of the inverse function: these are indicated by writing f^a where a a negative integer.

What if you want to subtract $m, n \in \mathbb{N}$ and you want $m-n$ to make sense even if $m < n$? Then you also need negative integers.

Finally, you might need negative numbers when you solve even the most basic types of algebraic equations. For instance, if you allow negative numbers you can always solve $x + b = c$ for x regardless of the sizes of b and c.

For these reasons and others the negative integers were introduced into mathematics. In this chapter we will construct and study the set $\mathbb{Z}$ of all integers, including negative integers. The amazing thing is that most of our algebraic laws that we developed for the natural numbers $\mathbb{N}$ continue to hold, and many new ones besides. Three modern ways of saying this is to say that $\mathbb{Z}$ is an *abelian group* under addition, $\mathbb{Z}$ is a *commutative ring*, and $\mathbb{Z}$ is an *integral domain*.

Our method of constructing $\mathbb{Z}$ will be a bit more involved than you might at first expect. You might expect a construction where you make a copy $\mathbb{N}^-$ of the positive integers $\mathbb{N}^+$ that you distinguish from the original set $\mathbb{N}^+$ somehow. For example, you could indicate the negative copy of 7 by writing -7. Then you take the (disjoint) union of $\mathbb{N}^-$ and $\mathbb{N}$ and call that $\mathbb{Z}$. Call this approach the *naive approach*. This is *not* the approach we will take.

One problem with the naive approach is that it requires a highly non-unified approach. For example, to define $x + y$ you need to consider six cases. Case i: if $x \geq 0$ and $y \geq 0$ then $x + y$ is defined as in Chapter 1. Case ii: if $x \geq 0$ and $y < 0$ with $y = -n$, and if $x \geq n$ then $x + y$ is defined as $x - n$. Case iii: if $x \geq 0$ and $y < 0$ with $y = -n$, and $x \leq n$ then $x + y$ is defined as $-(n - x)$. And so on. If you want to prove a law, such as the

Date: May 19, 2009.

associative law $x + (y + z) = (x + y) + z$, you must allow for a very large number of cases. Our approach, adopted in this chapter, will require many fewer separate cases by treating $\mathbb{Z}$ in a more unified manner.

Our approach is closely tied to the idea that elements of $\mathbb{Z}$ are used to measure the *net difference* between two finite sets. Just as elements of $\mathbb{N}$ have as one of their main applications the ability to describe the size of a finite set A, the integers $\mathbb{Z}$ can be used to describe the net difference of the size of A over the size of B, even if B is bigger than A. For example, A can represent how many dollars you have, and B how many dollars you owe. Or A can represent the number of protons in a charged particle, and B the number of electrons. There can be a temporal aspect: A can be the number of sheep that a farmer has this year, and B the number he or she had last year.

If we write (m, n) for the sizes of two sets, A and B respectively, we want to describe the net difference between m and n. By removing one from each side until we reach 0, the pair (m, n) can be reduced to either the form $(m', 0)$ or the form $(0, n')$ depending on whether A is larger or smaller than B. You can thing of $(m', 0)$ as representing a positive net difference if $m' \neq 0$, and you can think of $(0, n')$ as representing a negative net difference if $n' > 0$. For example, the pair $(19, 15)$ corresponds with $(4, 0)$, which describes a positive net difference, and $(8, 10)$ corresponds with $(0, 2)$, which describes a negative net difference.[1]

Roughly speaking, -2 can be thought of as the pair $(0, 2)$, and positive 4 as the pair $(4, 0)$. This is not quite what we will do in this chapter: we will define -2 as a certain type of *equivalence class* containing $(0, 2)$, and positive 4 as a certain type of equivalence class containing $(4, 0)$. Each equivalence class will be composed of pairs with the same net difference.

There are two reasons for using equivalence classes. First, the proofs of many of the theorems are easier using such equivalence classes. Second, the idea of equivalence class is used in many branches of modern mathematics to construct new objects, and it is good for you to get used to the idea in a relatively simple situation. We will use the equivalence class approach later when we define the integers modulo n, the rational numbers $\mathbb{Q}$, and the real numbers $\mathbb{R}$. In group theory, equivalence classes are used to construct quotient groups, and so on.

There is a pleasant symmetry between positive and negative when we study only addition.[2] Something strange happens when we introduce multiplication. For example, the product of positive integers is positive: positive integers are closed under multiplication. However, the product of negative integers is not negative, it is positive: the negative integers are not closed

[1] Of course this is for the difference of A over B. If our focus was on the difference of B over A, then $(m', 0)$ would be regarded as negative and $(0, n')$ as positive. In this chapter we will consistently measure the difference of the first set over the second.

[2] A fancy way of saying this is that the change of sign function yields an automorphism of the additive group of $\mathbb{Z}$.

under multiplication. What is the source of this asymmetry. *Why is the product of two negative integers positive?* This is probably the most mysterious question arising with the introduction of negative numbers.

The simplest answer to this question is probably one that involves negative iterations and inverse functions. We will discuss this explanation and others, including those involving algebraic laws that we expect $\mathbb{Z}$ to possess.

2. The net difference

Before introducing the integers $\mathbb{Z}$, we will study a motivating concept:

Definition 1. The *net difference function* $\Delta : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ is designed to measure the difference in sizes between two finite sets (of size m and n respectively). It is defined by the rule

$$\Delta(m,n) = \begin{cases} (m-n,0) & \text{if } m > n \\ (0,n-m) & \text{if } n > m \\ (0,0) & \text{if } m = n \end{cases}$$

This is well-defined by the trichotomy law for $\mathbb{N}$.

Informal Exercise 1. What is $\Delta(19,15)$? What is $\Delta(14,16)$?

Remark 1. Roughly speaking, you can think of $(x,0)$ as a positive difference, and $(0,x)$ as a negative difference (if $x \neq 0$). Later we will use this idea to define positive and negative integers in $\mathbb{Z}$, but we will work with equivalence classes of pairs, not the pairs themselves.

Exercise 2. Use the basic law of subtraction (Chapter 2) to show $m-0=m$. Use this to show that $\Delta(m,0) = (m,0)$ for all $m \in \mathbb{N}$. Don't forget to separate the case $m > 0$ from the case $m = 0$. Show that $\Delta(0,n) = (0,n)$.

Exercise 3. Use the above exercise to show that the second iteration of Δ is itself. In other words,

$$\Delta^2 = \Delta.$$

Lemma 1. *Let $m,n \in \mathbb{N}$. Then at least one of the coordinates of $\Delta(m,n)$ is zero. Furthermore,*
if $\Delta(m,n) = (x,0)$ with $x > 0$ then $m > n$,
if $\Delta(m,n) = (0,x)$ with $x > 0$ then $n > m$, and
if $\Delta(m,n) = (0,0)$ then $n = m$.

Proof. All the claims but the last follow directly from the definition. Recall from Chapter 2 that $n - m = 0$ implies $n = m$. So $\Delta(m,n) = (0,0)$ is impossible if $m > n$ or if $n > m$. Thus $\Delta(m,n) = (0,0)$ implies $m = n$. □

Definition 2 (Net-difference equivalence)**.** If $\Delta(m,n) = \Delta(m',n')$ we say that (m,n) and (m',n') are *net-difference equivalent*. In that case we write $(m,n) \sim (m',n')$. The relation $\sim$ is called *net-difference equivalence*.

Warning. The notation $\sim$ for net-difference equivalence is only really used in this chapter. The symbol $\sim$ will be used for other equivalence relations in other chapters.

Theorem 2. *Net-difference equivalence is an equivalence relation: it is reflexive, symmetric, and transitive.*

Exercise 4. Prove the above theorem.

We now discuss several lemmas in order to develop a variety of criteria to show that pairs are net-difference equivalent. These are summarized in Theorem 6 below.

Lemma 3. *For all* $m, n, x \in \mathbb{N}$, $\Delta(m, n) = \Delta(m + x, n + x)$

Proof. We divide into cases: $m > n$, $n > m$, $m = n$. First suppose that $m > n$. Then $m+x > n+x$ by a result of Chapter 1. So $\Delta(m, n) = (m-n, 0)$ and $\Delta(m + x, n + x) = \big((m + x) - (n + x), 0\big)$. The result follows from the equality $(m + x) - (n + x) = n - m$ established in Chapter 2.

The proof in the other cases is similar. □

Lemma 4. *If* $\Delta(m, n) = \Delta(m', n')$ *then* $m + n' = n + m'$.

Proof. We divide into cases: $m > n$, $n > m$, $m = n$. First suppose that $m > n$. Then $\Delta(m, n) = (x, 0)$ with $x > 0$ (since $m - n \neq 0$ by a result of Chapter 2). Thus $\Delta(m', n') = (x, 0)$ with $x > 0$. By Lemma 1, $m' > n'$. Also, $m - n = x = m' - n'$.

By the Basic Law of Subtraction (Chapter 2), $m = n+x$ and $m' = n'+x$. Thus, using arithmetic laws of Chapter 1,

$$m + n' = (n + x) + n' = n + (x + n') = n + (n' + x) = n + m'.$$

The cases where $n > m$ and $m = n$ are similar. □

Lemma 5. *Suppose* $(m, n), (m', n') \in \mathbb{N} \times \mathbb{N}$ *are such that* $m + n' = n + m'$ *and* $n' \geq n$. *Then there is an* $x \in \mathbb{N}$ *such that* $n' = n + x$ *and* $m' = m + x$.

Proof. Since $n' \geq n$, there is an $x \in \mathbb{N}$ such that $n' = n + x$ (Chapter 1). Our goal is to show $m' = m + x$ as well. Observe

$$n + m' = m + n' = m + (n + x) = n + (m + x).$$

The first equality is an assumption, the second is a substitution, and the last is a combination of the associative and commutative laws. The desired equation $m' = x + m$ follows from the cancellation law. □

Theorem 6. *Let* $(m, n), (m', n') \in \mathbb{N}\times\mathbb{N}$. *Then the following are equivalent:*

(i) $\Delta(m, n) = \Delta(m', n')$.

(ii) $m + n' = n + m'$.

(iii) Either $n' = n + x$ *and* $m' = m + x$ *for some* $x \in \mathbb{N}$, *or* $n = n' + x$ *and* $m = m' + x$ *for some* $x \in \mathbb{N}$.

Proof. We use the above lemmas to make an "implication circle".

For example (i) implies (ii) by Lemma 4.

Now if (ii) holds then divide into two cases: $n' \geq n$ and $n \geq n'$. In either case, Lemma 5 gives the result (with role reversal in the second case). So (ii) implies (iii).

Finally, (iii) implies (i) by Lemma 3. □

Remark 2. The above theorem gives us three different ways to check for net-difference equivalence. In other words, the above theorem gives three characterizations for net-difference equivalence. To prove theorems about net-difference equivalence, one strategically uses the condition that makes the proof the easiest.

3. The integers $\mathbb{Z}$

Informally, if $n \neq 0$ then positive n is the equivalence class containing $(n, 0)$ and negative n is the equivalence class containing $(0, n)$.

Definition 3. Let $[m, n]$ be the equivalence class of (m, n) under net-difference equivalence.

Theorem 7. *For all $m, n, m', n' \in \mathbb{N}$,*

$$[m, n] = [m', n'] \quad \Leftrightarrow \quad \Delta(m, n) = \Delta(m', n') \quad \Leftrightarrow \quad m + n' = n + m'$$

and

$$[m, n] = [\Delta(m, n)]$$

Exercise 5. Prove the above theorem. Hint: you might need to review equivalence classes from your set theory course. Also, use Theorem 6 and Exercise 3.

Definition 4 (Set of integers)**.** The *set of integers* $\mathbb{Z}$ is defined to be the set of equivalence classes under net-difference equivalence. In other words,

$$\mathbb{Z} = \{a \mid a = [m, n] \text{ for some } (m, n) \in \mathbb{N} \times \mathbb{N}\}.$$

Theorem 8. *If $a \in \mathbb{Z}$ then exactly one of the following hold:*

(i) $a = [0, 0]$.

(ii) $a = [n, 0]$ *for some* $n \in \mathbb{N}^+$.

(iii) $a = [0, n]$ *for some* $n \in \mathbb{N}^+$.

In addition, the integer n in (ii) or (iii) is unique.

Proof. By definition of $\mathbb{Z}$ we have $a = [m, n]$ for some $m, n \in \mathbb{N}$. By theorem 7 we have $a = [\Delta(m, n)]$. From the definition of Δ we have that $\Delta(m, n)$ has at least one coordinate equal to zero. Thus at least one of (i), (ii), (iii) holds since $a = [\Delta(m, n)]$.

We will show that (i) and (ii) cannot both hold. Suppose otherwise that $[0, 0] = a = [n, 0]$ for some $n \in \mathbb{N}^+$. This implies $0+0 = 0+n$ by Theorem 7. By results of Chapter 1, we can simplify $0+0 = 0+n$ to the equation $0 = n$. This contradicts $n \in \mathbb{N}^+$.

The proof that (i) and (iii) cannot both hold, and that (ii) and (iii) cannot both hold is similar. The proof that n is unique in case (ii) or case (iii) is also similar. □

Exercise 6. Show that (ii) and (iii) cannot both be true (even with different choices of n for (i) and (ii)). Show that n is unique in case (ii).

Definition 5. Let $a \in \mathbb{Z}$. If a is $[0,0]$ then a is called the *zero integer*. If a is $[n,0]$ for $n \in \mathbb{N}^+$ then a is said to be *positive*. If a is $[0,n]$ for $n \in \mathbb{N}^+$ then a is said to be *negative*. From the above theorem, exactly one of these applies to each $a \in \mathbb{Z}$.

Remark 3. The symbol $\mathbb{Z}$ is based on the German word *Zahlen* meaning 'numbers'. Some books write $\mathbf{Z}$ instead of $\mathbb{Z}$. In fact, the variant $\mathbb{Z}$ originated as a way to write a bold $\mathbf{Z}$ on the blackboard (without having to smash the chalk into the board to make the letter look bold). The letters $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are in a font style called *blackboard bold*.

4. Addition in $\mathbb{Z}$

In Chapter 2, addition in $\mathbb{N}$ is characterized by its ability to measure the size of a disjoint union of finite sets. We want to define an addition for $\mathbb{Z}$ with a similar capability. Now, individual elements of $\mathbb{Z}$ are used to measure the net difference resulting from the comparision of *two* sets A and B. We want addition in $\mathbb{Z}$ to measure the result of taking the disjoint union (in some sense) of one comparison A and B with another comparison A' and B'.

More specifically, if A is a set with m elements and if B is a set of n elements, then the integer $a = [m,n] = [\Delta(m,n)]$ measures the net difference of the size of A over B. It is positive when A is larger than B, it is negative when B is larger than A.

What happens if we simultaneously add m' elements to A, and n' elements to B where the new elements are in sets A' and B' disjoint from A and B respectively? Then we have added a net difference of $b = [m', n']$ to the sets A and B. We want our definition of $a + b$ in $\mathbb{Z}$ to represent the net differences of the sizes *after* adding the new elements. Since the first set has $m + m'$ elements after the addition, and the second has $n + n'$ elements, the resulting net difference is represented by $[m + m', n + n']$. This suggests that we define $a + b$ to be $[m + m', n + n']$.

Definition 6. Suppose $a, b \in \mathbb{Z}$ are integers such that $a = [m,n]$ and $b = [m', n']$. Then $a + b$ is defined to be $[m + m', n + n']$. The following lemma assures us that this definition is well-defined.

Remark 4. This definition brings up the subtle issue of "well-definedness". *Whenever you define a function or relation for equivalence classes, you must always check that the result depends only on the equivalence classes and not how they are represented.* For example, if $a = [14, 13]$ then we can describe a as $[11, 10]$, or $[101, 100]$ or in an infinite number of different ways. You want

to make sure that any definition involving a depends only on a and not on the arbitrary numbers, 14 and 13 say, used to describe it. The above formula $[m + m', n + n']$ for addition seems to depend on the particular numbers! The following lemma shows that it does not.

Lemma 9. *If* $[m_1, n_1] = [m_2, n_2]$ *and* $[m_1', n_1'] = [m_2', n_2']$ *then*

$$[m_1 + m_1', n_1 + n_1'] = [m_2 + m_2', n_2 + n_2'].$$

Proof. By Theorem 7, $m_1 + n_2 = n_1 + m_2$ and $m_1' + n_2' = n_1' + m_2'$. So

$$\begin{aligned}(m_1 + m_1') + (n_2 + n_2') &= (m_1 + n_2) + (m_1' + n_2') \\ &= (n_1 + m_2) + (n_1' + m_2') \\ &= (n_1 + n_1') + (m_2 + m_2').\end{aligned}$$

□

5. $\mathbb{Z}$ AS AN ABELIAN GROUP

The first main result concerning $\mathbb{Z}$ is that it is an *abelian group* under addition. This is just a fancy way of saying that (i) $\mathbb{Z}$ has an addition $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ that is associative, (ii) that there is an additive identity (zero) element in $\mathbb{Z}$, and (iii) that every element $a \in \mathbb{Z}$ has an additive inverse.

The combination of properties mentioned above (associativity, identity, and inverse) is so common in mathematics, that there is a name for something that possesses them, a *group*. Forget the informal meaning of the word *group* used in everyday life; from now on it will be a technical term referring to a set with the combination of properties mentioned above.[3] If we throw the commutative law into the mix, we call the group *abelian* (after the famous mathematician Abel).

Definition 7. A group G is a set together with a binary operation

$$* : G \times G \to G$$

such that

(i) $*$ is associative: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

(ii) G has an identity element. In other words, there is an element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. (It is easy to prove that the identity is unique).

(iii) Every element of G has an inverse. In other words, if $a \in G$ then there is a $b \in G$ such that $a * b = b * a = e$ where e is an identity for G. (It is easy to prove that the inverse of a is unique).

Informal Exercise 7. In many examples, $*$ is written $+$. Is $\mathbb{N}$ a group under $+$? What about $\mathbb{R}$ and $\mathbb{Q}$?

Definition 8. A group G is said to be *abelian* if the commutative law holds: $a * b = b * a$ for all $a, b \in G$.

[3]Mathematics majors typically study groups in more detail in an upper-division (abstract) algebra course.

In the previous section, we defined a binary operation $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. In an effort to show that $\mathbb{Z}$ is a group under $+$, we investigate some of the properties of $+$. The fact that the following proofs are so easy is due to our decision to define addition with equivalence classes. The naive definition of $\mathbb{Z}$ would result in lots of special cases.

Theorem 10 (Associative law)**.** *If $a, b, c \in \mathbb{Z}$ then $(a+b)+c = a+(b+c)$.*

Proof. Write $a = [m_1, n_1], b = [m_2, n_2]$, and $c = [m_3, n_3]$. Since each m_i and n_i is in $\mathbb{N}$, we can use the associative law of Chapter 1: $(m_1 + m_2) + m_3 = m_1 + (m_2 + m_3)$ and $(n_1 + n_2) + n_3 = n_1 + (n_2 + n_3)$. Thus, by substitution,

$$\big[(m_1 + m_2) + m_3, (n_1 + n_2) + n_3\big] = \big[m_1 + (m_2 + m_3), n_1 + (n_2 + n_3)\big].$$

So, using the above and applying the definition of addition several times,

$$\begin{aligned}
(a+b)+c &= \big([m_1, n_1] + [m_2, n_2]\big) + c \\
&= [m_1 + m_2, n_1 + n_2] + c \\
&= \big[(m_1 + m_2), (n_1 + n_2)\big] + \big[m_3, n_3\big] \\
&= \big[(m_1 + m_2) + m_3, (n_1 + n_2) + n_3\big] \\
&= \big[m_1 + (m_2 + m_3), n_1 + (n_2 + n_3)\big] \\
&= [m_1, n_1] + \big[(m_2 + m_3), (n_2 + n_3)\big] \\
&= a + [m_2 + m_3, n_2 + n_3] \\
&= a + \big([m_2, n_2] + [m_3, n_3]\big) = a + (b + c).
\end{aligned}$$

□

Theorem 11 (Commutative law)**.** *If $a, b \in \mathbb{Z}$ then $a + b = b + a$.*

Exercise 8. Prove the commutative law using the previous proof as a model.

Theorem 12 (Identity law)**.** *If $a \in \mathbb{Z}$ then $a + [0, 0] = a$.*

This shows that $[0, 0]$ is an identity for $\mathbb{Z}$. (Because of the commutative law, we don't have to show $[0, 0] + a = a$).

Definition 9. If $a = [m, n]$ is an element of $\mathbb{Z}$ then $-a$ is defined as $[n, m]$.

Actually, we cannot use this definition until we prove that is is well-defined.

Lemma 13. *If $[m, n] = [m', n']$ then $[n, m] = [n', m']$.*

Proof. If $[m, n] = [m', n']$ then $m + n' = n + m'$. So $n + m' = m + n'$. Thus $[n, m] = [n', m']$. (Theorem 7). □

Theorem 14 (Inverse Law)**.** *If $a \in \mathbb{Z}$ then $a + (-a) = [0, 0]$.*

Exercise 9. Show that $[n, n] = [0, 0]$ for all $n \in \mathbb{N}$. Prove the identity and the inverse law.

The above theorems combine to give us the following. (Because of the commutative law, we don't have show $a + (-a) = (-a) + a$.)

Theorem 15. *The set $\mathbb{Z}$ is an abelian group under addition $+$.*

Definition 10. If $a, b \in \mathbb{Z}$ then $a-b$ is shorthand for $a+(-b)$. In particular $a - a = [0, 0]$. This $-$ should not be confused with subtraction defined in Chapter 2. We will discuss the compatibility in the two types of $-$ in the next section.

Remark 5. If G is a group, then the notation g^{-1} and $-g$ are both used for the inverse of $g \in G$. If the operation for G written '$+$', then $-g$ is usually used to signify the inverse (as we did in $\mathbb{Z}$ above).

Every abelian group satisfies the cancellation law.

Theorem 16. *Suppose $a, b, c \in \mathbb{Z}$, or more generally suppose $a, b, c \in G$ where G is a group under addition $+$. Then, if $a + c = b + c$ then $a = b$.*

Exercise 10. Use the inverse of c to prove the above theorem.

Theorem 17. *Suppose $a \in \mathbb{Z}$, or more generally suppose $a \in G$ where G is a group under addition $+$. Then $-(-a) = a$.*

Proof. Observe that $a + (-a)$ and $(-(-a)) + (-a)$ are both equal to the identity by the definition of inverse. Hence they are equal to each other:

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

Now use the cancellation law. □

One advantage of using integers is that you can always solve equations of the form $x + a = b$.

Theorem 18. *Suppose $a, b \in G$ where G is a group under addition $+$ (for example $G = \mathbb{Z}$). Then, the equation $x + a = b$ has a unique solution in G. The solution is $x = b - a$.*

Exercise 11. Prove the above theorem.

Informal Exercise 12. If $m, n \in \mathbb{N}$ does the equation $x + m = n$ always have a solution for x in $\mathbb{N}$? Give necessary and sufficient conditions for the solution to exist.

Exercise 13. Suppose $a, b \in G$ where G is an abelian group under addition $+$. Show that $-(a+b) = (-a)+(-b)$. We often write this with the parentheses removed as

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

(Use parentheses in your proof)

Exercise 14. Show that if e is the identity element of a group, then e is its own inverse.

6. The canonical embedding

According to our formal definition, $\mathbb{N}$ is not a subset of $\mathbb{Z}$. However, we would like to think of $\mathbb{N}$ as a subset of $\mathbb{Z}$. What we do is define an injection of $\mathbb{N}$ into $\mathbb{Z}$, and then "identify" a natural number with its image in $\mathbb{Z}$.

Definition 11. Consider the function $\mathbb{N} \to \mathbb{Z}$ defined by the rule $n \mapsto [n, 0]$. Call this the *canonical embedding* of the natural numbers into the integers.

Theorem 19. *The canonical embedding $\mathbb{N} \to \mathbb{Z}$ is injective.*

Proof. If $[n_1, 0] = [n_2, 0]$ then $n_1 + 0 = 0 + n_2$ by Theorem 7. □

Whenever we have an injective function $f : A \to B$, the image $A' = f[A]$ is a subset of B and the function f gives a bijection $A \to A'$ (using restriction of codomain). We can use this bijection to match each element $a \in A$ with an element $a' \in A'$. We can go further, and *identify* the element a with its image a'. When we do this, we think of a' as a copy or "clone" of a. This allows us to think of A as being in some sense equal to A', and allows us to think of A as a subset of B.

We apply this idea to the canonical embedding $\mathbb{N} \to \mathbb{Z}$. We identify $n \in \mathbb{N}$ with its image $[n, 0]$ in $\mathbb{Z}$. We treat n and $[n, 0]$ as the same object, and we think of $\mathbb{N}$ as a subset of $\mathbb{Z}$.

Warning. When we identify the elements of $\mathbb{N}$ with elements of $\mathbb{Z}$ we risk ambiguous definitions and notation. For example, $m + n$ can mean two things if $m, n \in \mathbb{N}$. First, it can mean $m + n$ as defined in Chapter 1: we write $m +_{\mathbb{N}} n$ in this case. Second, it can mean $m + n$, or rather $[m, 0] + [n, 0]$ as defined in the current chapter: we write $m +_{\mathbb{Z}} n$ in this case.

It turns out that both types of addition are equal if $m, n \in \mathbb{N}$ and so we do not really need to make a distinction. This is shown by the following:

Theorem 20 (Extension of addition)**.** *If we consider $\mathbb{N}$ as a subset of $\mathbb{Z}$, and if $m, n \in \mathbb{N}$, then $m +_{\mathbb{N}} n$ and $m +_{\mathbb{Z}} n$ define the same element of $\mathbb{Z}$.*

Proof. The definition of addition for $\mathbb{Z}$ (Definition 6) implies

$$[m, 0] +_{\mathbb{Z}} [n, 0] = [m +_{\mathbb{N}} n,\ 0 +_{\mathbb{N}} 0] = [m +_{\mathbb{N}} n,\ 0].$$

Since m is identified with $[m, 0]$ and n with $[n, 0]$, and furthermore $m +_{\mathbb{N}} n$ with $[m +_{\mathbb{N}} n, 0]$, we can rewrite this equation as

$$m +_{\mathbb{Z}} n = m +_{\mathbb{N}} n.$$

□

When thinking of $\mathbb{N}$ as a subset of $\mathbb{Z}$, we call $+_{\mathbb{Z}}$ an *extension* of $+_{\mathbb{N}}$ since we originally only had an addition on $\mathbb{N}$ (Chapter 1), but we defined this addition to the larger set $\mathbb{Z}$ without changing the values on the subset $\mathbb{N}$. From now on we will not make a difference between the two types of additions since they agree whenever both are defined.

Theorem 21 (Extension of subtraction)**.** *The definition of subtraction for $\mathbb{Z}$ extends the definition of subtraction for $\mathbb{N}$. In other words, if $m, n \in \mathbb{N}$ with $m \leq n$, then $n-m$, as defined in Chapter 2, agrees with $n+(-m)$ as defined in the current chapter.*

Proof. By the definition of subtraction in Chapter 2, $n - m = b$ where $n = m + b$. To show that the two definitions of subtraction agree, we must show that $[n, 0] + (-[m, 0]) = [b, 0]$. Observe that

$$\begin{aligned} [n,0] + (-[m,0]) &= [n,0] + [0,m] && \text{(Def. of add. inverse)} \\ &= [n,m] && \text{(Def. of addition)} \\ &= [m+b,m] && (n = m+b) \\ &= [b,0] && \text{(Theorem 7)} \end{aligned}$$

The last step can be justified by the equation $(m + b) + 0 = m + b$. □

Multiplication for $\mathbb{Z}$ has not been defined yet, but when it is we will check that it extends the multiplication for $\mathbb{N}$.

Remark 6. Since we identify $0 \in \mathbb{N}$ with $[0, 0] \in \mathbb{Z}$, we can use the symbol '0' for both. In particular, by Theorem 12 (the identity law),

$$a + 0 = a \qquad \text{for all } a \in \mathbb{Z}.$$

Similarly, by Theorem 14 (inverse law),

$$a + (-a) = 0 \qquad \text{for all } a \in \mathbb{Z}.$$

Finally, by Exercise 14,

$$-0 = 0.$$

In the following two theorems we use the the canonical embedding to view $\mathbb{N}$ as a subset of $\mathbb{Z}$.

Theorem 22. *If $a \in \mathbb{Z}$ then exactly one of the following occurs: (i) $a = 0$, (ii) $a = n$ for $n \in \mathbb{N}^+$, or (iii) $a = -n$ for $n \in \mathbb{N}^+$. Furthermore, the n occurring in case (ii) or (iii) is unique.*

Proof. Let $a \in \mathbb{Z}$. By Theorem 8 either (i) $a = [0, 0]$, (ii) $a = [n, 0]$ where $n \in \mathbb{N}^+$, or (iii) $a = [0, n]$ where $n \in \mathbb{N}^+$. In case (i), $[0, 0]$ is identified with 0, so $a = 0$. In case (ii), $[n, 0]$ is identified with n, so $a = n$. In case (iii), $a = [0, n] = -[n, 0]$ and $[n, 0]$ is identified with n, so $a = -n$.

To show at most one case occurs, and to show uniqueness of n, use Theorem 8 together with the fact that $-n$ is identified with $-[n, 0] = [0, n]$. □

Remark 7. We can use this theorem to rephrase Definition 5 as follows. Integers of the form $a = n$ with $n \in \mathbb{N}^+$ are called *positive integers*. Integers of the form $a = -n$ with $n \in \mathbb{N}^+$ are called *negative integers*. Every integer is either zero, positive, or negative.

Remark 8. Theorem 22 shows that the integers, as we have formally constructed them, give the same integers as the informal definition mentioned in the introductory section of this chapter.

Corollary 23. *If $a \in \mathbb{Z}$ then exactly one of the following occurs:* (i) $a \in \mathbb{N}$, *or* (ii) $a = -n$ *for a unique* $n \in \mathbb{N}^+$.

Theorem 24. *Suppose $a, b \in \mathbb{Z}$. Then $a - b = 0$ if and only if $a = b$.*

Proof. Suppose that $a + (-b) = 0$. Then $\big(a + (-b)\big) + b = 0 + b$. Thus

$$\begin{aligned} b &= b + 0 && \text{(Identity Law)} \\ &= 0 + b && \text{(Commutative Law)} \\ &= \big(a + (-b)\big) + b && \text{(as above)} \\ &= a + \big((-b) + b\big) && \text{(Associative law)} \\ &= a + \big(b + (-b)\big) && \text{(Commutative law)} \\ &= a + 0 && \text{(Inverse Law)} \\ &= a && \text{(Identity law)} \end{aligned}$$

Conversely, if $a = b$, then $a + (-b) = b + (-b) = 0$. □

7. Order

From now one we will view $\mathbb{N}$ as a subset of $\mathbb{Z}$. Thus the positive integers $\mathbb{N}^+$ form a subset of $\mathbb{Z}$ as well. We can use positive integers to define the concept of *order* just as we did in Chapter 1.

Definition 12. Suppose $a, b \in \mathbb{Z}$. Then $a < b$ is defined to mean that there is an element $x \in \mathbb{N}^+$ such that $b = a + x$.

Remark 9. Since this is essentially the same definition as in Chapter 1, we observe that the order relation $<$ on $\mathbb{Z}$ extends the order $<$ on $\mathbb{N}$.

Theorem 25. *Suppose $a, b \in \mathbb{Z}$. Then $a < b$ if and only if $b - a \in \mathbb{N}^+$.*

Exercise 15. Prove the above theorem. Do not use subtraction as presented in Chapter 2, but use additive inverses instead.

Definition 13. Suppose $a, b \in \mathbb{Z}$. Then $a \leq b$ means either $a < b$ or $a = b$.

Theorem 26. *Suppose $a, b \in \mathbb{Z}$. Then $a \leq b$ if and only if $b - a \in \mathbb{N}$.*

Theorem 27. *Suppose $a, b, c \in \mathbb{Z}$. If $a < b$ then $a + c < b + c$. If $a \leq b$ then $a + c \leq b + c$.*

Theorem 28. *Let $a \in \mathbb{Z}$. Then $a \in \mathbb{N}$ if and only if $a \geq 0$. Also, a is positive if and only if $a > 0$, and a is negative if and only if $a < 0$.*

Theorem 29. *Transitivity for $<$ holds.*

Theorem 30. *Transitivity for $\leq$ hold. Mixed transitivity for $<$ and $\leq$ hold.*

Theorem 31. *Trichotomy for $<$ holds.*

Remark 10. Since trichotomy and transitivity hold for $<$, it is a linear order.

Exercise 16. Write up three proofs for the above six theorems. (You should be able to do all of them, but write up three of them.)

Theorem 32. *Let $a, b \in \mathbb{Z}$. If $a < b$ then $-b < -a$. If $a \leq b$ then $-b \leq -a$.*

Proof. (sketch) Suppose $a < b$. Then $a + \big((-a) + (-b)\big) < b + \big((-a) + (-b)\big)$ by Theorem 27. Using the laws proved so far, the left-hand side simplifies to $-b$ and the right-hand side simplifies to $-a$.

A similar argument holds for $\leq$. □

Corollary 33. *Let $c \in \mathbb{Z}$. If $c > 0$ then $-c < 0$. If $c < 0$ then $-c > 0$. If $c \geq 0$ then $-c \leq 0$. If $c \leq 0$ then $-c \geq 0$.*

Proof. This makes use of the fact that $-0 = 0$ (see Remark 6). □

Theorem 34. *Let $a \in \mathbb{Z}$. There is no integer x with $a < x < a + 1$.*

Proof. Suppose $a < x < a + 1$. Then

$$a + (-a) < x + (-a) < (a + 1) + (-a).$$

Thus $0 < x - a < 1$. In particular, $x - a \in \mathbb{N}$, but we showed in Chapter 1 that there is no natural number between 0 and 1. □

8. Iteration by $a \in \mathbb{Z}$

We now investigate the concept of negative iteration. An example where iteration is useful is in the definition of multiplication. Recall that in Chapter 1 multiplication is defined in terms of iteration of addition. If we can figure out a way to define negative iteration then we can explain what it means to multiply by a negative number.

We developed properties of f^n in Chapter 1 for $n \geq 0$. In this section and the next we will define f^a for all $a \in \mathbb{Z}$, and show that the properties of Chapter 1 extend to this more general situation.

We already know how to define f^{-1}. It is just the inverse function. How do we define f^a for other negative a? Informally, think of f^{-n} as the nth iterate of the inverse function f^{-1}. Recall that only bijective functions have inverses, so we will not try to define f^{-n} for functions that are not bijections.

Informal Definition 14. Suppose $f : S \to S$ is a bijection. If $a = n$ is a positive integer, then f^n is the nth iterate of f. If $a = -n$ is a negative integer, then $f^a = f^{-n}$ is the nth iterate of the inverse f^{-1}. If $a = 0$ then f^a is the identity function $id : S \to S$.

Warning. We use f^{-1} to refer to the inverse of f, *not* to $1/f$. Similarly, f^2 refers to $f \circ f$, *not* to the product $f \cdot f$ of the function with itself.

The above definition is informal. Our formal definition will use equivalence classes to give a common definition for all cases at once. It may seem more elaborate, but it will be more convenient for proving theorems. Before giving the formal definition, we give a preliminary theorem.

Theorem 35. *If $n \in \mathbb{N}$ and if $f : S \to S$ is a bijection, then f^n and $\left(f^{-1}\right)^n$ are also bijections. Furthermore, the inverse of f^n is $(f^{-1})^n$. So*

$$(f^n)^{-1} = \left(f^{-1}\right)^n.$$

Proof. First we will show that $f^n \circ \left(f^{-1}\right)^n = id$ where $id : S \to S$ is the identity function. Let A be the set of $n \in \mathbb{N}$ such that $f^n \circ \left(f^{-1}\right)^n = id$.

First we show $0 \in A$. Observe that f^0 and $\left(f^{-1}\right)^0$ are both the identity function, and the composition of the identity function with itself is just the identity function. So $0 \in A$.

Now suppose $u \in A$. We must show that $u + 1 \in A$. By a result of Chapter 2,

$$f^{u+1} = f^u \circ f^1 = f^u \circ f.$$

Similarly,

$$\left(f^{-1}\right)^{u+1} = \left(f^{-1}\right)^{1+u} = \left(f^{-1}\right)^1 \circ \left(f^{-1}\right)^u = f^{-1} \circ \left(f^{-1}\right)^u.$$

So

$$\begin{aligned} f^{u+1} \circ \left(f^{-1}\right)^{u+1} &= \left(f^u \circ f\right) \circ \left(f^{-1} \circ \left(f^{-1}\right)^u\right) \\ &= \left(\left(f^u \circ f\right) \circ f^{-1}\right) \circ \left(f^{-1}\right)^u \\ &= \left(f^u \circ \left(f \circ f^{-1}\right)\right) \circ \left(f^{-1}\right)^u \\ &= \left(f^u \circ id\right) \circ \left(f^{-1}\right)^u \\ &= f^u \circ \left(f^{-1}\right)^u. \end{aligned}$$

In the second and third equalities we used the fact that function composition is associative (Chapter 0). Since $u \in A$, we have $f^u \circ \left(f^{-1}\right)^u = id$. Combining this with the above gives

$$f^{u+1} \circ \left(f^{-1}\right)^{u+1} = id.$$

Thus $u + 1 \in A$.

By the induction axiom, $A = \mathbb{N}$. So $f^n \circ \left(f^{-1}\right)^n = id$ for all $n \in \mathbb{N}$.

A similar argument show that $\left(f^{-1}\right)^n \circ f^n = id$ for all $n \in \mathbb{N}$. By the definition of inverse function, we have that f^n and $\left(f^{-1}\right)^n$ are inverse functions. Finally,, functions that have inverses must be bijections. □

Definition 15 (General iteration)**.** Let $f : S \to S$ be a bijection. Suppose $a \in \mathbb{Z}$, and that $a = [m, n]$. Then

$$f^a \stackrel{\text{def}}{=} f^m \circ \left(f^{-1}\right)^n.$$

The term on the left refers to the new type of iteration, and the terms on the right use the old (Chapter 1) type of iteration.

The following lemma shows that this definition is well-defined: it doesn't matter what pair (m, n) is used to write the same a. Such a lemma is essential whenever we use equivalence classes.

Lemma 36. *Let $m, n, m', n' \in \mathbb{N}$, and let $f : S \to S$ be a bijection. If $[m, n] = [m', n']$ then*

$$f^m \circ \left(f^{-1}\right)^n = f^{m'} \circ \left(f^{-1}\right)^{n'}.$$

Proof. (Sketch) Since $[m,n]=[m',n']$ we have $\Delta(m,n)=\Delta(m',n')$. Without loss of generality, assume $m'\geq m$. So $m'=m+x$ and $n'=n+x$ for some $x\in\mathbb{N}$ (Theorem 6). Thus

$$\begin{aligned} f^{m'}\circ\left(f^{-1}\right)^{n'} &= f^{m+x}\circ\left(f^{-1}\right)^{x+n} \\ &= f^{m}\circ f^{x}\circ\left(f^{-1}\right)^{x}\circ\left(f^{-1}\right)^{n} \quad (f^{m+x}=f^m\circ f^x\text{: see Ch. 2}) \\ &= f^{m}\circ\left(f^{-1}\right)^{n} \qquad\qquad (\text{Thm. 35}). \end{aligned}$$

(We can leave out parentheses since functional composition is associative.) □

Exercise 17. If $f:S\to S$ is bijective, and if $a\in\mathbb{Z}$, show that f^a is also a bijective function $S\to S$ using Definition 15.

Warning. We now have two types of iteration: that from Chapter 1, and that defined in Definition 15 (which made use of the earlier type of iteration). We will show that the new type of iteration extends the earlier type.

Lemma 37. *The new type of iteration extends the earlier type of iteration. In other words, if $f:S\to S$ is a bijection and $n\in\mathbb{N}$ then both definitions give the same result for f^n.*

In addition, if we use the new definition for f^{-1}, the result agrees with the old definition. In other words, f^{-1} according to the new definition is just the inverse function.

Proof. Let $n\in\mathbb{N}$. In $\mathbb{Z}$, the integer n is identified with the equivalence class $[n,0]$. Observe

$$f^{[n,0]} \overset{\text{def}}{=} f^n\circ\left(f^{-1}\right)^0 = f^n\circ id = f^n$$

where the right hand side is as in Chapter 1. Thus both types of iteration agree for $n\in\mathbb{N}$.

In $\mathbb{Z}$, the number -1 is identified with the equivalence class $-[1,0]$ which is $[0,1]$. Observe

$$f^{[0,1]} \overset{\text{def}}{=} f^0\circ\left(f^{-1}\right)^1 = id\circ\left(f^{-1}\right)^1 = \left(f^{-1}\right)^1 = f^{-1}.$$

So the new definition of f^{-1} gives the inverse. □

The following shows that f^{-n} is what we expect.

Theorem 38. *Suppose $f:S\to S$ is bijective. If $n\in\mathbb{N}$ then*

$$f^{-n}=\left(f^{-1}\right)^n=\left(f^n\right)^{-1}.$$

Proof. If $n\in\mathbb{N}$ then $-n$ is $[0,n]$. So

$$f^{-n}=f^{[0,n]} \overset{\text{def}}{=} f^0\circ\left(f^{-1}\right)^n = id\circ\left(f^{-1}\right)^n = \left(f^{-1}\right)^n.$$

Note that $\left(f^{-1}\right)^n=\left(f^n\right)^{-1}$ by Theorem 35. □

We will generalize the above result in the next section (Corollary 44 and Corollary 47).

9. Iteration and the commutativity of composition

In this section we will derive several properties concerning iteration, especially those associated with the idea of commutativity of composition. The most significant identity concerning iteration is the additive identity:

$$f^{a+b} = f^a \circ f^b$$

where $a, b \in \mathbb{Z}$ (already proved for $a, b \in \mathbb{N}$ in Chapter 2). This gives an important application for addition in $\mathbb{Z}$: it describes the resulting iteration associated with the composition of two iterations. It gives evidence that our definition of $+$ was "the right one".

Definition 16. Let $f : S \to S$ and $g : S \to S$ be functions. We say that f *and* g *commute* if $f \circ g = g \circ f$. We also say f *commutes with* g and that g *commutes with* f.

Exercise 18. Suppose $f : S \to S$ is a bijection. Verify that f and $g = f^{-1}$ commute. Also, verify that the identity function $id : S \to S$ commutes with all functions $f : S \to S$. (Hint: your proofs should be very short.)

Informal Exercise 19. Find two functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ that do not commute. Hint: try polynomial functions (that are not monomials).

If you know about linear transformations and their matrices you can use matrixes to find examples of non-commuting functions $\mathbb{R}^2 \to \mathbb{R}^2$.

Lemma 39. *Suppose $f : S \to S$ and $g : S \to S$ are functions that commute. Then f^n and g commute for all $n \in \mathbb{N}$.*

Proof. Let A be the set of all $n \in \mathbb{N}$ such that f^n and g commute. We know that $0 \in A$ since f^0 is just the identity function.

Suppose $u \in A$. We must show that $u + 1 \in A$. Observe that

$$\begin{aligned}
f^{u+1} \circ g &= \big(f \circ f^u\big) \circ g && \text{(From Chapter 1)} \\
&= f \circ \big(f^u \circ g\big) && \text{(Set theory: associativity of composition)} \\
&= f \circ \big(g \circ f^u\big) && \text{(Since } u \in A\text{)} \\
&= \big(f \circ g\big) \circ f^u && \text{(Set theory: associativity of composition)} \\
&= \big(g \circ f\big) \circ f^u && \text{(Since } f \text{ and } g \text{ commute)} \\
&= g \circ \big(f \circ f^u\big) && \text{(Set theory: associativity of composition)} \\
&= g \circ f^{u+1} && \text{(From Chapter 1).}
\end{aligned}$$

Thus $u + 1 \in A$.

By the induction axiom, $A = \mathbb{N}$. The result follows. □

Theorem 40. *Suppose $f : S \to S$ and $g : S \to S$ are functions that commute. Then f^m and g^n commute for all $m, n \in \mathbb{N}$.*

Proof. By the above lemma, f^m and g commute. By the above lemma applied to g and f^m, we get that g^n and f^m commute. □

We can extend the above to negative iterations. This is done in the following lemma and theorem.

Lemma 41. *Suppose that $f : S \to S$ and $g : S \to S$ are functions that commute. If f is bijective, then f^{-m} and g^n commute for all $m, n \in \mathbb{N}$.*

Proof. By Theorem 40, $g^n \circ f^m = f^m \circ g^n$. Thus

$$f^{-m} \circ g^n \circ f^m \circ f^{-m} = f^{-m} \circ f^m \circ g^n \circ f^{-m}$$

(parentheses can be left off since function composition is associative). We know that f^m and f^{-m} are inverses by Theorem 38. Thus the above equation simplifies to $f^{-m} \circ g^n = g^n \circ f^{-m}$. □

Theorem 42. *Suppose that $f : S \to S$ and $g : S \to S$ are bijections that commute. Then f^a and g^b commute for all $a, b \in \mathbb{Z}$.*

Proof. If neither a, b are negative use Theorem 40. If one of a, b is negative use Lemma 41.

Suppose that a and b are negative where $a = -m$ and $b = -n$. Lemma 41 shows that f and g^{-1} commute (switching the roles of f and g). Thus, by Lemma 41 again, f^{-m} and $\left(g^{-1}\right)^n$ commute. However, $\left(g^{-1}\right)^n = g^{-n}$ by Theorem 38. □

The following is the key theorem of this section.

Theorem 43. *Suppose $f : S \to S$ is bijective and that $a, b \in \mathbb{Z}$. Then*

$$f^{a+b} = f^a \circ f^b.$$

Proof. Write $a = [m, n]$ and $b = [m', n']$. Thus $a + b = [m + m', n + n']$. Let g be the inverse of f. So

$$\begin{aligned}
f^{a+b} &= f^{[m+m',n+n']} && \text{(Def. 6)} \\
&= f^{m+m'} \circ g^{n+n'} && \text{(Def. 15)} \\
&= \left(f^m \circ f^{m'}\right) \circ \left(g^n \circ g^{n'}\right) && \text{(Chapter 2)} \\
&= \left(f^m \circ \left(f^{m'} \circ g^n\right)\right) \circ g^{n'} && \text{(Assoc. of } \circ\text{.: twice)} \\
&= \left(f^m \circ \left(g^n \circ f^{m'}\right)\right) \circ g^{n'} && \text{(Thm. 40)} \\
&= \left(f^m \circ g^n\right) \circ \left(f^{m'} \circ g^{n'}\right) && \text{(Assoc. of } \circ\text{: twice)} \\
&= f^{[m,n]} \circ f^{[m',n']} = f^a \circ f^b && \text{(Def. 15)}
\end{aligned}$$

□

The following generalizes part of Theorem 38.

Corollary 44. *Suppose $f : S \to S$ is bijective and that $a \in \mathbb{Z}$. Then*

$$f^{-a} = \left(f^a\right)^{-1}.$$

Proof. By Theorem 43,

$$f^{-a} \circ f^a = f^{-a+a} = f^0 \qquad \text{and} \qquad f^a \circ f^{-a} = f^{a-a} = f^0.$$

Since f^0 is the identity function, we see that f^a and f^{-a} are inverse functions. In other words, $(f^a)^{-1} = f^{-a}$. □

Remark 11. Suppose $f : S \to S$ and $g : S \to S$ are bijective functions. We usually do not expect that $(f \circ g)^a = f^a \circ g^a$. However, there is a case where this does indeed happen. We begin (Lemma 45) with the non-negative case.

Informal Exercise 20. Find polynomial functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ such that $(f \circ g)^2$ does not equal $f^2 \circ g^2$.

Lemma 45. *Suppose $f : S \to S$ and $g : S \to S$ commute. Then, for all $n \in \mathbb{N}$,*

$$(f \circ g)^n = f^n \circ g^n.$$

Exercise 21. Prove the above using induction. Where did you use the hypothesis that f and g commute?

Theorem 46. *Suppose $f : S \to S$ and $g : S \to S$ are bijective functions, and suppose $a \in \mathbb{Z}$. If f and g commute, then*

$$(f \circ g)^a = f^a \circ g^a.$$

Proof. If $a \geq 0$ then use Lemma 45. If $a < 0$ then $a = -n$ where $n \in \mathbb{N}$, and

$$\begin{aligned}
(f \circ g)^n \circ (f^a \circ g^a) &= (f^n \circ g^n) \circ (f^a \circ g^a) && \text{(Lemma 45)} \\
&= \left(f^n \circ (g^n \circ f^a)\right) \circ g^a && \text{(by assoc. of } \circ\text{, twice)} \\
&= \left(f^n \circ (f^a \circ g^n)\right) \circ g^a && \text{(Thm. 42)} \\
&= (f^n \circ f^a) \circ (g^n \circ g^a) && \text{(by assoc. of } \circ\text{, twice)} \\
&= f^{n+a} \circ g^{n+a} && \text{(by Thm. 43)} \\
&= f^0 \circ g^0 = id && \text{(since } a = -n\text{)}
\end{aligned}$$

A similar argument show that $(f^a \circ g^a) \circ (f \circ g)^n$ is the identity. So $(f \circ g)^n$ and $(f^a \circ g^a)$ are inverse functions, and

$$(f \circ g)^a = (f \circ g)^{-n} = \left((f \circ g)^n\right)^{-1} = (f^a \circ g^a).$$

□

The following generalizes part of Theorem 38.

Corollary 47. *Suppose $f : S \to S$ is bijective and that $a \in \mathbb{Z}$. Then*

$$f^{-a} = \left(f^{-1}\right)^a.$$

Proof. Since f and f^{-1} commute, Theorem 46 gives

$$f^a \circ \left(f^{-1}\right)^a = \left(f \circ f^{-1}\right)^a = (id)^a = id.$$

The last step uses Lemma 48 (below). Similarly, $\left(f^{-1}\right)^a \circ f^a$ is the identity. Thus f^a and $\left(f^{-1}\right)^a$ are inverses. In other words,

$$(f^a)^{-1} = \left(f^{-1}\right)^a.$$

But $f^{-a} = (f^a)^{-1}$ (Corollary 44), so $f^{-a} = \left(f^{-1}\right)^a$. □

Lemma 48. *If $id : S \to S$ is the identity, then $id^a = id$ for all $a \in \mathbb{Z}$.*

Exercise 22. Prove the above. First show it by induction for all $a \geq 0$. Next show it for $a < 0$ by appealing to the fact that $a = -n$ for some $n \in \mathbb{N}$, so $id^a = id^{-n} = (id^n)^{-1}$.

10. Translation functions

Recall that in Chapter 1, multiplication was defined as iterated addition. More precisely, if $\alpha_m : \mathbb{N} \to \mathbb{N}$ is the function $x \mapsto x + m$, then $m \cdot n$ was defined to be $\alpha_m^n(0)$. In Section 8 of the current chapter we extended iteration to negative iteration. We can use this idea to define multiplication by a negative integer.

In particular, let $a, b \in \mathbb{Z}$. Define the function $A_a : \mathbb{Z} \to \mathbb{Z}$ by the rule $x \mapsto x + a$. (We use 'A' instead of 'α' to indicate that the domain is $\mathbb{Z}$ and not just $\mathbb{N}$, and that a is allowed to be negative). We propose

$$a \cdot b \stackrel{\text{def}}{=} A_a^b(0).$$

For this definition to make sense we must show that A_a is bijective.

Since the theory of multiplication is so heavily dependent on A_a, we will first prove some properties of A_a, and wait until the next section to formally define multiplication.

Definition 17. Let $a \in \mathbb{Z}$. Then the *translation function* by a is defined to be the function $A_a : \mathbb{Z} \to \mathbb{Z}$ defined by the rule $x \mapsto x + a$.

Theorem 49. *The function $A_0 : \mathbb{Z} \to \mathbb{Z}$ is the identity function.*

Theorem 50. *If $a, b \in \mathbb{Z}$ then $A_a \circ A_b = A_{a+b}$.*

Exercise 23. Prove the above two theorems, and the following corollary.

Corollary 51. *If $a \in \mathbb{Z}$ then $A_a \circ A_{-a}$ and $A_{-a} \circ A_a$ are the identity function. Furthermore, A_a is bijective with inverse $(A_a)^{-1} = A_{-a}$.*

Exercise 24. Show that A_a and A_b commute.

We now discuss some applications of the translation functions. First recall the following definition from Chapter 2, which we extend to all the integers.

Definition 18. If $a, b \in \mathbb{Z}$ then

$$\{a, \ldots, b\} \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid a \leq x \leq b\}.$$

Theorem 52. *Let $a, b, c \in \mathbb{Z}$. There is a bijection*

$$\{a, \ldots, b\} \to \{a + c, \ldots, b + c\}.$$

Proof. By Theorem 27, if $a \leq x \leq b$ then $a+c \leq x+c \leq b+c$. Thus if $x \in \{a, \ldots, b\}$, then $A_c(x) \in \{a+c, \ldots, b+c\}$. So we can restrict A_c to produce a function $\{a, \ldots, b\} \to \{a+c, \ldots, b+c\}$. Similarly, the restriction of A_{-c} gives an inverse. Since these functions are inverses, they are bijective. □

Corollary 53. *Let $a, b \in \mathbb{Z}$. Then the set $\{a, \ldots, b\}$ has $(b-a)+1$ elements. So this set is finite.*

Proof. Apply the previous theorem with $c = -a + 1$. □

Remark 12. This corollary tells us that if you work on a project from the 3rd of November to the 10th of November (inclusive), you have worked on it for $(10-3)+1 = 8$ days. It is a bit counter-intuitive that you don't just subtract: $10 - 3 = 7$ is the wrong answer.

Theorem 54. *Let S be a non-empty subset of $\mathbb{Z}$ that is bounded from above, then $\mathbb{Z}$ has a maximum.*

Proof. First consider the case where S intersects $\mathbb{N}$. Let $T = \mathbb{N} \cap S$. Now T is bounded by the same upper bound as S, and T is not empty. Thus, by a result of Chapter 2, T has a maximum M. Since $M \in \mathbb{N}$, we have $M \geq 0$. Since every negative element of S is less than 0, and since $M \geq 0$, we have that M is a maximum for all of S (transitivity, definition of maximum).

Now suppose that S does not intersect $\mathbb{N}$. Let $-n \in S$, and let S' be the image of S under the translation map A_n. Observe that S' contains $0 = A_n(-n)$. So S' has a maximum M' since it intersects $\mathbb{N}$ (see the first case above). Let $M = M' - n$. Claim: M is a maximum of S. To see this first observe that $A_n(M) = M'$, and that $A_n(x) = M'$ for some $x \in S$ since $M' \in S'$ (def. of image). So $M = x$ by injectivity of A_n. Thus $M \in S$. Suppose that $y \in S$. Then $A_n(y) \leq M'$ (def. of max.), so $y + n \leq M'$. Hence $y \leq M' - n$. So $y \leq M$ as desired. □

Theorem 55. *Let S be a non-empty subset of $\mathbb{Z}$ that is bounded from below, then $\mathbb{Z}$ has a minimum.*

Proof. (sketch) Let c be a lower bound of S. Let S' be the image of the translation map A_{-c}. Then $S' \subseteq \mathbb{N}$. Thus S' has a minimum n. This means that $n + c$ is the minimum of S. □

Exercise 25. Fill in the details of the proof of Theorem 55. Justify all steps.

Now we return to the study of translations. One important fact about translations is that the iteration of a translation is a translation. This follows from the fact that the composition of translations is a translation.

Lemma 56. *If $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ then A_a^n is a translation.*

Proof. Fix $a \in \mathbb{Z}$. Let $S_a = \{x \in \mathbb{N} \mid A_a^x \text{ is a translation}\}$. Observe that $0 \in S_a$ since $A_a^0 = id = A_0$ (Theorem 49) and A_0 is a translation.

Suppose that $k \in S_a$. This means $A_a^k = A_b$ for some $b \in \mathbb{Z}$. Thus

$$A_a^{k+1} = A_a \circ A_a^k = A_a \circ A_b = A_{a+b}. \qquad \text{(Thm. 50)}$$

Since A_{a+b} is a translation, we have that $k+1 \in S_a$.

By induction, $S_a = \mathbb{N}$. Since $n \in \mathbb{N}$, it is in S_a. The result follows. □

This lemma can be generalized:

Theorem 57. *If $a, b \in \mathbb{Z}$ then the iteration A_a^b of A_a is also a translation.*

Proof. If $b \geq 0$ then use Lemma 56. If $b < 0$ then $b = -n$ for some $n \in \mathbb{N}$. So, by Theorem 38 and Corollary 51,

$$A_a^b = A_a^{-n} = \left(A_a^{-1}\right)^n = (A_{-a})^n .$$

But $(A_{-a})^n$ is a translation by Lemma 56. □

The following will be useful in future sections:

Lemma 58. *If $A_a = A_b$ then $a = b$.*

Exercise 26. Prove the above lemma. Hint, apply translations to 0.

Remark 13. A fancy way to say some of the above is is that the set of translations forms an abelian group under composition, and the map $x \mapsto A_x$ is an isomorphism between the additive group $\mathbb{Z}$ and this group of translations.

11. DEFINITION OF MULTIPLICATION

In the previous section we proposed that multiplication be defined using iterated addition. In other words, if A_a is the addition by a map (also called the translation by a map), then the proposal was that $a \cdot b$ be defined as $A_a^b(0)$. Since A_a is a bijection (Corollary 51), iteration A_a^b is defined even if b is negative.

In this section we carry out this proposal. Properties of the map A_a will help us prove theorems about multiplication.

Definition 19. Let $a, b \in \mathbb{Z}$. Then

$$a \cdot b \stackrel{\text{def}}{=} A_a^b(0).$$

The bth iterate is defined since A_a is a bijection $\mathbb{Z} \to \mathbb{Z}$. By definition of iteration, A_a^b is a function $\mathbb{Z} \to \mathbb{Z}$. Thus $a \cdot b = A_a^b(0)$ is in $\mathbb{Z}$.

In particular, multiplication takes pairs of integers a, b to an integer. In other words, multiplication is a binary operation $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Now we develop a few easy consequences of this definition. (None require induction in their proof).

Theorem 59. *If $a \in \mathbb{Z}$ then*

$$a \cdot 0 = 0 \qquad \textit{and} \qquad 0 \cdot a = 0.$$

Exercise 27. Prove Theorem 59. Hint: What is the zeroth iteration A_a^0? You will also need to use Lemma 48 and Theorem 49.

Lemma 60. *If $a \in \mathbb{Z}$ then*

$$a \cdot 1 = a.$$

Exercise 28. Prove Lemma 60.

Theorem 61. *If $a \in \mathbb{Z}$ then*

$$a \cdot (-1) = -a.$$

Exercise 29. Prove Theorem 61. Hint: see Corollary 51. Now apply the function $A_a^{-1} = A_{-a}$ to 0.

Lemma 62. *This definition extends the definition of multiplication given in Chapter 1. In other words, if $m, n \in \mathbb{N}$, then $m \cdot n$ is the same whether you use the definition in Chapter 1 or Definition 19.*

Proof. (Sketch) Let α_m be as in Chapter 1. Observe that $\alpha_m(x) = A_m(x)$ for all $x \in \mathbb{N}$. By induction, one can show that $\alpha_m^n(x) = A_m^n(x)$ for all $x, n \in \mathbb{N}$. In particular, $\alpha_m^n(0) = A_m^n(0)$. □

Remark 14 (Negative times a negative: one answer). Now we are in a position to explain a major puzzle of elementary mathematics: why is a negative times a negative equal to a positive? First we give an informal explanation: a formal proof will follow. For simplicity, this informal explanation will focus on the case $(-n)(-1)$ where $n \in \mathbb{N}$.

First, consider the two functions A_n and A_{-n}. The first of these translates all the integers n units in the positive direction, and the second translates all the integers n units in the negative direction. Clearly these two processes are inverse to each other (see Corollary 51).

Now when we multiply $-n$ by -1 we need to iterate the translation A_{-n} a total of -1 times. But we know that iterating by -1 is the same as taking the inverse. The inverse of A_{-n} is A_n. In short, $(-n)(-1)$ is n.

The same argument applies to multiplying $-n$ by $-m$. Multiplying by $-m$ involves inverting and iterating A_{-n}. After inverting we get A_n, which we then iterate a total of m times. This yields $m \cdot n$.

The above informal discussion is incorporated into the proof of the following.

Theorem 63. *If $m, n \in \mathbb{N}$ then $(-n)(-m) = n \cdot m$. Thus a negative integer times a negative integer is a positive integer.*

Proof.

$$\begin{aligned} A_{-n}^{-m} &= (A_{-n})^{-m} && \text{(rewriting)} \\ &= \left((A_{-n})^{-1}\right)^m && \text{(Thm. 38)} \\ &= (A_n)^m && \text{(Corollary 51)} \\ &= A_n^m && \text{(rewriting)} \end{aligned}$$

Thus, by definition of multiplication (Definition 19),

$$(-n)(-m) = A_{-n}^{-m}(0) = A_n^m(0) = n \cdot m.$$

□

Remark 15. When we discuss rings, we will discuss other reasons why a negative times a negative is a positive. We will see that the axioms for a ring imply that $(-x)(-y) = x \cdot y$ for all elements x, y in the ring.

This answer might beg the question: why should $\mathbb{Z}$ be a ring? The nice thing about the above answer leading to Theorem 63 is that it is a natural consequence of thinking about multiplication as iterated addition.

Remark 16 (Discussion on Symmetry). When we study $\mathbb{Z}$ with no multiplication but only addition ($\mathbb{Z}$ as an abelian group) we get the sense that the positive and the negative integers are analogous. For example, the sum of two positive numbers is positive, and the sum of two negative numbers is negative. The sum of a positive and a negative number depends on the sizes of the two numbers involved in a completely symmetric manner.

The terms "positive" and"negative" seemed like arbitrary labels in a similar manner to what happens with electrical charge. Here one type of charge is called "positive" and the other is "negative", where these terms are purely conventional: there is no inherent reason why a proton's charge should be called "positive" and an electron's charged called "negative".

However, when we move to multiplication ($\mathbb{Z}$ as a ring), we see a stark difference between positive and negative integers. For example, the product of positive integers is positive, but the product of two negative numbers is not negative. Where does this difference between positive and negative emerge? Our point of view is that the difference emerges with the idea of iteration f^a. When $a \in \mathbb{Z}$ is negative there is an element of inversion that is not present when $a \geq 0$. It is this that leads to the loss of symmetry between positive and negative numbers.[4]

Remark 17. We defined $\mathbb{Z}$-multiplication in terms of iteration, but there are a few other common approaches. One way is to simply define it by cases:

$$m \cdot n \stackrel{\text{def}}{=} mn, \qquad m \cdot (-n) \stackrel{\text{def}}{=} -(mn)$$

$$(-m) \cdot n \stackrel{\text{def}}{=} -(mn), \qquad (-m) \cdot (-n) \stackrel{\text{def}}{=} mn$$

where multiplication on the right-hand side of each equation is as in Chapter 1, and where $m, n \in \mathbb{N}$. Proofs have to be done in cases as well. Under this definition, the answer to the question "why is a negative times an negative equal to a positive?" is that we defined it in this way!

A second alternative is to define multiplication by the formula

$$[m, n] \cdot [m', n'] = [mm' + nn', mn' + nm']$$

and show that the formula is well defined. Proving the laws of arithmetic is straightforward, but somewhat messy.

I believe our iteration approach is better motivated than these alternatives since it grows out of the definition of multiplication in Chapter 1. It also

[4]A fancy way of saying the above is that $a \mapsto -a$ is an isomorphism of $\mathbb{Z}$ as a group, but not as a ring.

gives a reasonable answer to the question about a negative times a negative. The downside is it requires more study of negative iteration and translation maps. However, these topics are worth their own study, and so the downside is not too bad.

12. Laws of multiplication

We will prove the laws of multiplication. We begin with another law concerning translation.

Theorem 64. *If $a, b \in \mathbb{Z}$ then*

$$A_a^b = A_{a \cdot b}.$$

Proof. By Theorem 57, A_a^b is a translation. So we can write $A_a^b = A_c$ for some $c \in \mathbb{Z}$. What is c? By the definition of $a \cdot b$ (Definition 19) and the definition of translation (Definition 17),

$$a \cdot b = A_a^b(0) = A_c(0) = 0 + c = c.$$

So $c = ab$. Thus $A_a^b = A_c = A_{ab}$ as desired. □

Theorem 65 (Left distributive law)**.** *If $a, b, c \in \mathbb{Z}$ then*

$$a(b + c) = ab + ac.$$

Proof. Observe that

$$\begin{aligned} A_{a(b+c)} &= A_a^{b+c} && \text{(Thm. 64)} \\ &= A_a^b \circ A_a^c && \text{(Thm. 43)} \\ &= A_{ab} \circ A_{ac} && \text{(Thm. 64)} \\ &= A_{ab+ac} && \text{(Thm 50).} \end{aligned}$$

The result follows from Lemma 58. □

Theorem 66 (Right distributive law)**.** *If $a, b, c \in \mathbb{Z}$ then*

$$(a + b)c = ac + bc.$$

Proof. Recall that A_a and A_b commute (Exercise 24), so we can apply Theorem 46. By this and other results,

$$\begin{aligned} A_{(a+b)c} &= A_{a+b}^c && \text{(Thm. 64)} \\ &= (A_{a+b})^c && \text{(Rewrite)} \\ &= \big(A_a \circ A_b\big)^c && \text{(Thm. 50)} \\ &= A_a^c \circ A_b^c && \text{(Thm. 46)} \\ &= A_{ac} \circ A_{bc} && \text{(Thm. 64)} \\ &= A_{ac+bc} && \text{(Thm. 50).} \end{aligned}$$

The result follows from Lemma 58. □

Theorem 67. *If $a, b \in \mathbb{Z}$ then*

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

Proof. Observe

$$\begin{aligned} A_{(-a)b} &= A_{-a}^{b} && \text{(Thm. 64)} \\ &= (A_{-a})^{b} && \text{(Rewrite)} \\ &= \left(A_{a}^{-1}\right)^{b} && \text{(Cor. 51)} \\ &= A_{a}^{-b} && \text{(Cor. 47)} \\ &= A_{a(-b)} && \text{(Thm. 64).} \end{aligned}$$

So $(-a)b = a(-b)$ by Lemma 58.

Next observe,

$$\begin{aligned} A_{a(-b)} &= A_{a}^{-b} && \text{(Thm. 64)} \\ &= \left(A_{a}^{b}\right)^{-1} && \text{(Cor. 44)} \\ &= (A_{ab})^{-1} && \text{(Thm. 64)} \\ &= A_{-(ab)} && \text{(Cor. 51)} \end{aligned}$$

So $a(-b) = -(ab)$ by Lemma 58. □

Lemma 68. *If $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ then $an = na$.*

Proof. (Using Corollary 23). If $a \in \mathbb{N}$, the result follows from the Commutative law of Chapter 1. If $a = -m$ with $m \in \mathbb{N}^{+}$, then

$$\begin{aligned} (-m)n &= -(mn) && \text{(Theorem 67)} \\ &= -(nm) && \text{(Chapter 1)} \\ &= n(-m) && \text{(Theorem 67)} \end{aligned}$$

□

Theorem 69 (Commutative law)**.** *If $a, b \in \mathbb{Z}$ then*

$$a \cdot b = b \cdot a.$$

Proof. (Using Corollary 23). If $b \in \mathbb{N}$, the result follows from Lemma 68. If $b = -n$ with $n \in \mathbb{N}^{+}$, then

$$\begin{aligned} a(-n) &= -(an) && \text{(Theorem 67)} \\ &= -(na) && \text{Lemma 68} \\ &= (-n)a && \text{(Theorem 67)} \end{aligned}$$

□

Here is an application of the commutative law.

Theorem 70. *If $a \in \mathbb{Z}$ then*

$$1 \cdot a = a \cdot 1 = a.$$

Proof. Combine Lemma 60 with the commutative law (Theorem 69). □

Before proving the associative law, we prove an important result concerning the interaction between iteration and multiplication. It generalizes a result from Chapter 2.

Lemma 71. *Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$. If $f : S \to S$ is bijection then $(f^a)^n = f^{an}$.*

Proof. (Using Corollary 23). If $a \in \mathbb{N}$, the result follows from a law in Chapter 2. If $a = -m$ with $m \in \mathbb{N}^+$, then

$$\begin{aligned} \left(f^{-m}\right)^n &= \left(\left(f^{-1}\right)^m\right)^n && \text{(Theorem 38)} \\ &= \left(f^{-1}\right)^{mn} && \text{(Law of Ch. 2)} \\ &= f^{-(mn)} && \text{(Theorem 38)} \\ &= f^{(-m)n} && \text{(Theorem 67)} \end{aligned}$$

□

Theorem 72. *Let $f : S \to S$ be a bijection, and $a, b \in \mathbb{Z}$. Then*

$$(f^a)^b = f^{ab}.$$

Proof. (Using Corollary 23). If $b \in \mathbb{N}$, the result follows from a law in Chapter 2. If $b = -n$ with $n \in \mathbb{N}^+$, then

$$\begin{aligned} (f^a)^{-n} &= ((f^a)^n)^{-1} && \text{(Theorem 38)} \\ &= (f^{an})^{-1} && \text{(Lemma 71)} \\ &= f^{-(an)} && \text{(Corollary 44)} \\ &= f^{a(-n)} && \text{(Theorem 67)} \end{aligned}$$

□

Remark 18. This gives an important application for multiplication in $\mathbb{Z}$: multiplication describes the resulting iteration associated with the iteration of an iteration. It gives evidence that our definition was "the right one".

Theorem 73 (Associative law)**.** *If $a, b, c \in \mathbb{Z}$ then*

$$a(bc) = (ab)c.$$

Proof. Observe

$$\begin{aligned} A_{a(bc)} &= A_a^{bc} && \text{(Thm. 64)} \\ &= (A_a)^{bc} && \text{(by rewriting)} \\ &= \left((A_a)^b\right)^c && \text{(Thm. 72)} \\ &= \left(A_a^b\right)^c && \text{(by rewriting)} \\ &= (A_{ab})^c && \text{(Thm. 64)} \\ &= A_{(ab)c} && \text{(Thm. 64).} \end{aligned}$$

The result follows from Lemma 58. □

13. The ring of integers

Definition 20. A *ring* is a set R equipped with *two* binary operations $R \times R \to R$ satisfying the properties listed below. The binary operations are called *addition* and *multiplication*, and are typically written $+ : R \times R \to R$ and $\cdot : R \times R \to R$. Multiplication is also indicated by juxtaposition, and the usual conventions for parentheses are employed. A ring R must satisfy the following:

(i) The set R is an abelian group under addition. In other words,
  (i.1) addition is associative,
  (i.2) addition has an identity, typically written 0,
  (i.3) every element $x \in R$ has an additive inverse, typically written $-x$, and
  (i.4) addition is commutative.

(ii) Multiplication is associative: for all $x, y, z \in R$,

$$(xy)z = x(yz).$$

(iii) There is a multiplicative identity[5], typically written 1: for all $x \in R$,

$$x \cdot 1 = 1 \cdot x = x.$$

(iv) The distributive law holds: for all $x, y, z \in R$

$$x(y + z) = xy + xz,$$

$$(y + z)x = yx + zx.$$

Definition 21. Suppose that R is a ring such that

$$xy = yx$$

for all $x, y \in R$. Then we say that the *commutative law* holds for R, and we call R a *commutative ring*.

Remark 19 (Informal). The set of 2 by 2 matrices with entries in $\mathbb{R}$ forms a non-commutative ring. Thus not all rings are commutative.

Informal Exercise 30. Explain why $\mathbb{N}$ is not a ring.

Theorem 74. *The integers $\mathbb{Z}$ form a commutative ring.*

Proof. This follows from earlier results. □

Exercise 31. List the results needed to prove the above theorem. Hint: start with Theorem 15.

Many results that hold for $\mathbb{Z}$ actually extends to other rings as well. We give four examples.

[5]Some algebra textbooks do not require the multiplicative identity, but many do. Most rings that one considers, however, have a multiplicative identity.

Theorem 75. *If R is a ring, then*

$$x \cdot 0 = 0 \cdot x = 0$$

for all $x \in R$.

Proof. Recall the law $y + 0 = y$ for any additive group. So $0 + 0 = 0$. Thus

$$x \cdot 0 = x(0 + 0) = x \cdot 0 + x \cdot 0$$

by the distributive law. By adding the inverse $-(x \cdot 0)$ to both sides, we get

$$0 = x \cdot 0.$$

A similar argument shows $0 \cdot x = 0$. □

Theorem 76. *If $x, y \in R$ where R is a ring, then*

$$(-x)y = -(xy) = x(-y).$$

Proof. Observe that

$$xy + (-x)y = \big(x + (-x)\big)y = 0 \cdot y = 0$$

by the previous theorem. Thus xy and $(-x)y$ are additive inverses. So

$$(-x)y = -(xy).$$

A similar argument shows $x(-y) = -(xy)$. □

Theorem 77. *If $y \in R$ where R is a ring, then*

$$(-1)y = y(-1) = -y.$$

Proof. This follows from the previous theorem. For example, if $x = 1$ then $(-1)y = -(1y)$ by the previous theorem. □

Theorem 78. *If $x, y \in R$ where R is a ring, then*

$$(-x)(-y) = xy.$$

Proof. By Theorem 76, used twice,

$$(-x)(-y) = -\big(x(-y)\big) = -\big(-(xy)\big).$$

However, $-(-z) = z$ for all z in an additive group (and R is an additive group under addition by the definition of ring). Thus

$$(-x)(-y) = -\big(-(xy)\big) = xy.$$

□

Remark 20. The above theorem gives another explanation to our big question of why a negative times a negative yields a positive: it is just a special case of the above theorem. In other words, once you know that $\mathbb{Z}$ satisfies the properties of a ring, such as the distributive law, then from these properties or laws you can deduce that the product $(-x)(-y)$ is xy. In other words, the equality $(-x)(-y) = xy$ is just a consequence of basic laws of arithmetic, and is so general that it holds for any ring.

This gives a different explanation than that given in Section 11. There we appealed to special properties of $\mathbb{Z}$, but the present explanation works far more generally. The weakness of the present explanation is that it is only compelling once you know that the traditional laws of arithmetic, such that the distributive law, holds of $\mathbb{Z}$. The explanation of Section 11, on the other hand, gives an explanation directly from the definition of multiplication in $\mathbb{Z}$.

We end the section with the so-called "FOIL-rule".[6]

Theorem 79. *Let $a, b, c, d \in R$ where R is a ring then*

$$(a+b)(c+d) = ac + ad + bc + bd.$$

Remark 21. Parentheses are not needed because $+$ is associative.

Exercise 32. Prove Theorem 79 using the distributive law.

14. Other Properties of Multiplication

We end with some important properties of $\mathbb{Z}$.[7]

Theorem 80. *The product of two positive integers is positive, the product of two negative integers is positive, the product of a positive and a negative integer is negative.*

Exercise 33. Prove this theorem. Hint: the first was already proved in Chapter 1, so does not require an additional proof.

Corollary 81. *Suppose $x, y \in \mathbb{Z}$. If $x \neq 0$ and $y \neq 0$, then $xy \neq 0$.*

Corollary 82. *If $x, y \in \mathbb{Z}$ and if $xy = 0$, then $x = 0$ or $y = 0$.*

Exercise 34. Show how the above corollaries follow from Theorem 80.

Definition 22. An *integral domain* is a commutative ring R with the additional properties that (i) $0 \neq 1$, and (ii) for $x, y \in R$,

$$xy = 0 \;\Rightarrow\; x = 0 \;\vee\; y = 0.$$

The name *integral* domain suggests it was inspired by the integers. Needless to say, there are other interesting integral domains that mathematicians study.

Corollary 83. *The ring $\mathbb{Z}$ is an integral domain.*

The cancellation law for $\mathbb{N}$ can be found in Chapter 1. This law also holds in $\mathbb{Z}$. In fact, it doesn't just hold in $\mathbb{Z}$, but it holds in any integral domain. (Warning: it does not hold in every ring though).

Theorem 84 (Cancellation Law for Multiplication)**.** *Let R be $\mathbb{Z}$ or any integral domain. If $a, b, c \in R$ and if $c \neq 0$ then*

$$ac = bc \implies a = b.$$

[6] A favorite mnemonic in HS algebra: "first, outside, inside, last"

[7] These are properties that will extend to $\mathbb{Q}$ and $\mathbb{R}$, but not to rings in general.

Proof. Add $-ac$ to both sides of the equation $ac = bc$:

$$0 = ac + (-ac) = bc + (-ac) = bc + (-a)c = (b - a)c$$

(using Theorem 76, and the Distributive Law). Since R is an integral domain, $b - a = 0$ or $c = 0$. However, $c \neq 0$ by assumption. Thus $b + (-a) = 0$. By adding a to both sides, and using the identity, associative, and inverse laws (valid since R is a ring), we get $b = a$. □

We end with standard laws concerning multiplication and inequalities.

Theorem 85. *Suppose that $x, y, z \in \mathbb{Z}$. Then*

$$x < y \ \wedge \ z > 0 \ \Rightarrow \ xz < yz,$$
$$x < y \ \wedge \ z < 0 \ \Rightarrow \ xz > yz,$$
$$x \leq y \ \wedge \ z \geq 0 \ \Rightarrow \ xz \leq yz,$$

and

$$x \leq y \ \wedge \ z \leq 0 \ \Rightarrow \ xz \geq yz.$$

Proof. Suppose $x < y$ and $z > 0$. Then $y - x$ is positive (Theorem 25). Thus $(y - x)z$ is positive by Theorem 80. But, by Theorem 66 and Theorem 67,

$$(y - x)z = \big(y + (-x)\big)z = yz + (-x)(z) = yz + \big(-(xz)\big).$$

Since $yz - xz$ is positive, we get $xz < yz$ by Theorem 25.

Suppose $x < y$ and $z < 0$. Then $y - x$ is positive (Theorem 25). Thus $(y - x)z$ is negative by Theorem 80. As before, $(y - x)z = yz + \big(-(xz)\big)$. So $yz + \big(-(xz)\big) < 0$. Add xz to both sides (Theorem 27). The result follows.

Suppose $x \leq y$ and $z \geq 0$. If both inequalities are strict, we have proved the result already. If $x = y$ the result $xz = yz$ follows by multiplying both sides of the equation by z. If $z = 0$, then $xz = yz = 0$ (Theorem 59). The result follows.

Suppose $x \leq y$ and $z \leq 0$. If both inequalities are strict, the result follows what we have done. If $x = y$ or $z = 0$ then $xz = yz$ as before. □