CHAPTER 2: EXPLORING $\mathbb{N}$

MATH 378, CSUSM. SPRING 2009. AITKEN

1. Introduction

In this chapter we continue the study of the set $\mathbb{N}$. We begin with subtraction $n-m$ where we assume $n \geq m$. Then we consider the well-ordering property of $\mathbb{N}$ and the related maximum principle.

Most of the remainder of the chapter is devoted to idea of *counting* and *cardinality*, which are arguably the most important applications of the natural numbers. An important result is the invariance of counting: it does not matter what order you count a given finite set, the answer will be the same. We also consider cardinality properties of the following: subsets, bijections, injections, surjections, addition, multiplication, subtraction, and exponentiation. We use these ideas to give alternative, set-based proofs of some of the basic laws of arithmetic. These proofs are more insightful than the induction proofs from Chapter 1. Counting principles, such as the pigeonhole principle and the inclusion-exclusion principle, will be discussed.

We end with a short discussion of how iteration is related to addition and multiplication. This illustrates an important application for the operations of addition and multiplication, and prepares us for Chapter 3 where multiplication in $\mathbb{Z}$ is developed in terms of iteration.

By the end of the chapter we will have seen three characterizations each of addition and multiplication.
Addition is
(i) iterated successor (Chapter 1),
(ii) what is needed to count finite disjoint unions,
(iii) what is needed to describe the composition of two iterations.
Multiplication is
(i) iterated addition (Chapter 1),
(ii) what is needed to count finite Cartesian products,
(iii) what is needed to describe the iteration of an iteration.

Remark 1. Our focus on counting and cardinality explains why we include 0 as an element of $\mathbb{N}$. It is common, in other places, to adopt the convention that 1 is the first natural number. This is a reflection of the historical fact that 0 was developed much later than the positive integers. However, the empty set is very common in modern mathematics, and we want to be able

Date: May 19, 2009.

to count all finite sets including the empty set. We need 0 as a natural number in order to define the size (cardinality) of the empty set.

2. Subtraction

In Chapter 1 we considered addition and multiplication for the natural numbers. Another fundamental operation is subtraction, but $n - m$ is not defined (as a natural number) for all $n, m \in \mathbb{N}$. Obviously we want to restrict the definition of $n - m$ to natural numbers such that $n \geq m$. In Chapter 3 we will introduce negative integers, and then we will be able to define $n - m$ for all integers n and m.

Recall, from Chapter 1, that $n \geq m$ if and only if there is a $b \in \mathbb{N}$ such that $n = m + b$. It turns out that this b is unique:

Lemma 1. *Let $n, m \in \mathbb{N}$. If $n \geq m$ then there is a unique $b \in \mathbb{N}$ such that $n = m + b$.*

Exercise 1. Justify the above claim that b is unique.

To define a new term, such as $n - m$, we need to identify a specific object that the term will reference. Both existence and uniqueness are important in identifying a specific object with a given property. Now that we know that a number b with the property $n = m + b$ exists and is unique (when $n \geq m$) we can use this property to define subtraction.

Definition 1. Let $m, n \in \mathbb{N}$ be such that $n \geq m$. Then $n - m$ is defined to be the $b \in \mathbb{N}$ such that $n = m + b$. We call $n - m$ the *difference* of n and m, and call $-$ the *subtraction operation.*

The subtraction operation is not defined for all $(n, m) \in \mathbb{N} \times \mathbb{N}$, but only for the subset consisting of pairs where $n \geq m$. (In Chapter 3 we will define $n - m$ without assuming $n \geq m$, but the result will not always be in $\mathbb{N}$.)

Directly from the definition we have the following.

Theorem 2 (Basic law of subtraction)**.** *Suppose $m, n \in \mathbb{N}$ are such that $n \geq m$. Then $n = m + b$ if and only if $b = n - m$.*

Theorem 3. *Let $n \in \mathbb{N}$. Then $n - n = 0$.*

Proof. Since $n = n + 0$, the conclusion $n - n = 0$ follows from Theorem 2. □

Here is a converse that follows easily from the basic law of subtraction:

Theorem 4. *Given $n, m \in \mathbb{N}$ with $n \geq m$, if $n - m = 0$ then $n = m$*

Theorem 5. *Suppose $m, n \in \mathbb{N}$ with $n \geq m$. Then $m + (n - m) = n$.*

Theorem 6. *Suppose $x, y, z \in \mathbb{N}$ are such that $y \leq x$ and $z \leq x$. Then $x - y = z$ if and only if $x - z = y$.*

Exercise 2. Prove the above three theorems as consequences of Theorem 2.

Informal Exercise 3. Give a counter-example showing that subtraction is not associative. Is subtraction commutative? Hint: $0 - 2$ is not even defined.

Remark 2. Since subtraction is not associative, parentheses are often required to determine the meaning of an expression involving subtraction. When parentheses are not explicitly written, we follow the usual rules for grouping. One rule we will adopt is that when we are given terms linked by $+$ and $-$, we perform our operations left to right. For example

$$a + b + c - d + e - f + (g + h) - (i - j) + k.$$

is really

$$\Big(\Big(\big(\big(\big((((a + b) + c) - d) + e\big) - f\big) + (g + h)\big) - (i - j)\Big) + k.$$

Even though subtraction itself is not associative, the following shows a situation where parentheses can be moved.

Theorem 7. *Suppose $x, y, z \in \mathbb{N}$ are such that $z \leq y$. Then*

$$(x + y) - z = x + (y - z).$$

Proof. Let $c = x + (y - z)$. Observe that

$$c + z = \big(x + (y - z)\big) + z = x + \big((y - z) + z\big) = x + y$$

by the associative and commutative laws of addition (Chapter 1) and Theorem 5. Thus $z + c = x + y$ by the commutative law. By the basic law of subtraction $c = (x + y) - z$. The result follows. □

Here is an application of the above associative law:

Theorem 8. *Suppose $m, n, c \in \mathbb{N}$. If $n \geq m$ then $n + c \geq m + c$ and*

$$n - m = (n + c) - (m + c).$$

Proof. The first part follows from a result of Chapter 1. For the second part:

$$\begin{aligned}
(m + c) + (n - m) &= ((m + c) + n) - m && \text{(Theorem 7)} \\
&= (n + (c + m)) - m && \text{(Comm law: Ch.1, twice)} \\
&= ((n + c) + m) - m && \text{(Assoc law: Ch.1)} \\
&= (n + c) + (m - m) && \text{(Theorem 7)} \\
&= (n + c) + 0 && \text{(Theorem 3)} \\
&= n + c && \text{(Rule from Ch.1)}
\end{aligned}$$

The result now follows from the basic law of subtraction. □

3. The well-ordering property

In Chapter 1 we established that $\mathbb{N}$ is ordered by $<$. Several other number systems ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}$) are also ordered. We now consider a general definition of ordered set in order to describe the concepts of *minimum* and *maximum*:

Definition 2 (Ordered Set)**.** An *ordered set* is a set U with a designated relation, typically written $<$, that is transitive and satisfies the trichotomy law. In other words (i) if $x, y, z \in U$ are such that $x < y$ and $y < z$, then $x < z$, and (ii) if $x, y \in U$ then exactly one of the following holds: $x < y$, $x = y$, or $y < x$.

We follow the conventions of Chapter 1 in defining $>, \leq, \geq$. If U is an ordered set and if $x, y \in U$, then $x \leq y$ is defined as $(x < y) \vee (x = y)$. Also $x > y$ is defined as $y < x$, and $x \geq y$ is defined as $y \leq x$.

Remark 3. If S is a subset of an ordered set, then S is itself an ordered set. Thus any subset of $\mathbb{N}$ is an ordered set.

Exercise 4. Suppose U is an ordered set. Show that $\leq$ is transitive using cases.

The trichotomy law does not hold for $\leq$, but the next theorem follows easily from the trichotomy law for $<$.

Theorem 9. *Let $x, y \in U$ where U is an ordered set. Then $x < y$ is the negation of $y \leq x$. Likewise $x \leq y$ is the negation of $y < x$. Finally, if $x \leq y$ and $y \leq x$ then $x = y$.*

Definition 3. Let U be an ordered set. An element $m \in U$ is called a *minimum* if $m \leq x$ holds for all $x \in U$. An element $M \in U$ is called a *maximum* if $x \leq M$ holds for all $x \in U$.

Warning. Suppose U is a subset of another ordered set such as $\mathbb{N}$. *The elements m and M in the above must be in U.* If the requirement $m, M \in U$ is dropped then we call m a *lower bound* for U and M an *upper bound* for U.

Warning. Not all ordered sets have a minimum and a maximum. For example, if $U = \mathbb{N}$ then U has no maximum. In a later chapter we will describe intervals such as $U = (0, 1]$ in $\mathbb{Q}$ that have no minimum. The number 0 is not a minimum of $(0, 1]$ since it is not in U, but 0 is a lower bound for U.

Existence may fail, but if existence holds then uniqueness must as well:

Theorem 10. *The minimum of U, if it exists, is unique. The maximum of U, if it exists, is unique.*

Exercise 5. Prove the above theorem.

Warning. In contrast, upper and lower bounds are not necessarily unique.

Exercise 6. What is the minimum of $\mathbb{N}$? Show that $\mathbb{N}$ has no maximum.

We now come to the key concept of this section:

Definition 4. An ordered set U is said to be *well-ordered* if every non-empty subset $A \subseteq U$ has a minimum.

Warning. Showing that $\mathbb{N}$ has a minimum is not enough to prove it is well-ordered. You must show that every nonempty subset of $\mathbb{N}$ has a minimum. Of course, different subsets can have different minima.

Theorem 11. *The set of natural numbers $\mathbb{N}$ is well-ordered.*

Proof. We begin with an induction. Consider the following set

$$S = \{x \in \mathbb{N} \mid \text{every subset } A \subseteq \mathbb{N} \text{ containing } x \text{ has a minimum}\}$$

Our first goal is to show that all natural numbers are in S. Once we have done this, proving the theorem is much easier.

First observe that $0 \in S$ since any subset A containing 0 has as a minimum $m = 0$ (recall $0 \leq n$ for all natural numbers n).

Now suppose $n \in S$. We wish to show that $n + 1 \in S$. In other words, if A is a subset containing $n + 1$, we want to show it has a minimum. Let $A' = A \cup \{n\}$. Let m' be the minimum of A', which exists by the inductive hypothesis and the fact that $n \in A'$.

Case 1. Suppose $m' \in A$. Observe that $m' \leq x$ for all $x \in A$ since m' is a minimum of A' and A is a subset. Thus A has m' for its minimum.

Case 2. Suppose $m' \notin A$. Since m' is in A' but not in A, then $m' = n$ by the definition of A'. Let $m = m' + 1$. Claim: m is the minimum of A. Suppose otherwise, that $x < m' + 1$ for some $x \in A$. We have $m' \leq x$ since m' is the minimum of A' and A is a subset. Actually $m' < x$ since $m' \neq x$ (because $m' \notin A$). So $m' < x < m' + 1$, contradicting a result of Chapter 1.

In each case, A has a minimum. We have established that $n + 1 \in S$.

By the induction axiom, $S = \mathbb{N}$. We now use this fact to prove the result. Let A be any non-empty subset of $\mathbb{N}$. Let $x \in A$ (which exists since A is non-empty). Since $x \in \mathbb{N}$ we have $x \in S$. By definition of S, the set A has a minimum. □

Informal Exercise 7. Is the set of nonnegative rational numbers well-ordered? Is the set of integers $\mathbb{Z}$ well-ordered?

Not every non-empty subset of $\mathbb{N}$ has a maximum. However, every *bounded* non-empty subset of $\mathbb{N}$ has a maximum.

Theorem 12 (Maximum Principle)**.** *Suppose A is a non-empty subset of $\mathbb{N}$ with an upper bound. In other words, suppose there is a $b \in \mathbb{N}$ such that every $y \in A$ satisfies $y \leq b$. Then A has a maximum.*

Exercise 8. Study the proof that $\mathbb{N}$ is well-ordered. Use the ideas in the proof to prove Theorem 12. Hint: let S be the set

$$\{x \in \mathbb{N} \mid \text{every non-empty } A \subseteq \mathbb{N} \text{ with upper bound } x \text{ has a maximum}\}.$$

Divide the main step into two cases as before (but there is no need to form a set A' from A).

4. The set $\{1, \ldots, n\}$

A main purpose of this chapter is to develop the theory of counting for finite sets. Informally, a non-empty set is said to be finite if its elements can be counted by integers $1, \ldots, n$ for some $n \geq 1$. In order to make this precise and prove theorems about counting, we need to understand the set $\{1, \ldots, n\}$. The purpose of this preliminary section is to define and develop basic properties of this set.

Informally, we are comfortable with an expressions such as $1, \ldots, n$ which make use of ellipses (three dots: $\ldots$), but we will not use such expressions without formal definitions.

Definition 5. Define $\{1, \ldots, n\}$ to be the set

$$\{x \in \mathbb{N} \mid 1 \leq x \leq n\}.$$

More generally, $\{m, \ldots, n\}$ is defined as $\{x \in \mathbb{N} \mid m \leq x \leq n\}$. Warning: this is the empty set if $m > n$.

We allow common variants. For example, $\{1, 2, \ldots, n\}$ is also defined as $\{x \in \mathbb{N} \mid 1 \leq x \leq n\}$.[1]

Here are facts from set theory, repeated for convenience:

$$\{a\} = \big\{x \mid x = a\big\}$$

$$\{a, b\} = \big\{x \mid (x = a) \vee (x = b)\big\}.$$

$$\{a, b, c\} = \big\{x \mid (x = a) \vee (x = b) \vee (x = c)\big\}.$$

Theorem 13. *Let $m \in \mathbb{N}$. The set $\{m, \ldots, m\}$ is equal to $\{m\}$.*

Proof. Suppose $x \in \{m, \ldots, m\}$. By Definition 5, $m \leq x \leq m$. However, $m \leq x$ and $x \leq m$ imply $x = m$. From set theory we know that $x = m$ implies $x \in \{m\}$. We conclude that $\{m, \ldots, m\} \subseteq \{m\}$.

Suppose $x \in \{m\}$. By basic set theory, this means $x = m$. Since $x = m$ we have both $m \leq x$ and $x \leq m$. In other words, $m \leq x \leq m$. So, by Definition 5, $x \in \{m, \ldots, m\}$. Thus $\{m\} \subseteq \{m, \ldots, m\}$. □

Theorem 14. *Let $n \in \mathbb{N}$. The set $\{n, \ldots, n+1\}$ is equal to $\{n, n+1\}$.*

Exercise 9. Prove the above theorem.

The next theorem one might want to show is that

$$\{n, \ldots, n+2\} = \{n, n+1, n+2\}.$$

After this, one might want a theorem concerning $\{n, \ldots, n+3\}$, and so on. The next theorem shows a key relationship that helps make it easier to prove such results.

[1] Warning: the notation $\{1, 2, \ldots, n\}$ might suggest to the reader that $n > 2$. To be safe, we should always mention any assumptions about the size of n.

Theorem 15. *If $m, n \in \mathbb{N}$ where $m \leq n$, then*

$$\{m, \ldots, n+1\} = \{m, \ldots, n\} \cup \{n+1\}.$$

Furthermore, $n+1 \notin \{m, \ldots, n\}$ so the union is disjoint.

Proof. First we prove $\{m, \ldots, n+1\} \subseteq \{m, \ldots, n\} \cup \{n+1\}$. So suppose that $x \in \{m, \ldots, n+1\}$. Then, by definition, $m \leq x$ and $x \leq n+1$. So either $x = n+1$ or $x < n+1$.

Case 1: $x = n+1$. Then $x \in \{n+1\}$. But $\{n+1\} \subseteq \{m, \ldots, n\} \cup \{n+1\}$ by properties of unions. So $x \in \{m, \ldots, n\} \cup \{n+1\}$.

Case 2: $x < n+1$. Observe that $x > n$ implies $n < x < n+1$ which cannot happen (see Chapter 1). Thus $x \leq n$. We know that $m \leq x$, so $m \leq x \leq n$. Thus $x \in \{m, \ldots, n\}$. Since $\{m, \ldots, n\} \subseteq \{m, \ldots, n\} \cup \{n+1\}$, we have $x \in \{m, \ldots, n\} \cup \{n+1\}$ as well.

So in either case, $x \in \{m, \ldots, n\} \cup \{n+1\}$. Thus

$$\{m, \ldots, n+1\} \subseteq \{m, \ldots, n\} \cup \{n+1\}.$$

Next we will prove that $\{m, \ldots, n\} \cup \{n+1\} \subseteq \{m, \ldots, n+1\}$. So suppose that $x \in \{m, \ldots, n\} \cup \{n+1\}$ By definition of union, we have two cases.

Case 1: $x \in \{m, \ldots, n\}$. In this case $m \leq x \leq n$. But $n < n+1$ by a result of Chapter 1. Thus $x < n+1$ by (mixed) transitivity. This implies $m \leq x \leq n+1$, so $x \in \{m, \ldots, n+1\}$.

Case 2: $x \in \{n+1\}$ In other words, $x = n+1$. Now $n < n+1$, by a result of Chapter 1. In particular, $n \leq x$. By hypothesis, $m \leq n$. Thus $m \leq x$ by transitivity. Trivially $x \leq n+1$, since $x = n+1$. So $m \leq x \leq n+1$. Hence $x \in \{m, \ldots, n+1\}$.

In either case, $x \in \{m, \ldots, n+1\}$. Thus

$$\{m, \ldots, n\} \cup \{n+1\} \subseteq \{m, \ldots, n+1\}.$$

Combining this with the previous inclusion, we conclude the sets are equal.

Finally, we show $n+1 \notin \{m, \ldots, n\}$. Suppose otherwise: $m \leq n+1 \leq n$. Then $n+1 \leq n$. However, by a result of Chapter 1, $n+1 > n$. This contradicts trichotomy. □

Exercise 10. Use the above to give another proof that the set $\{n, \ldots, n+1\}$ is just $\{n, n+1\}$. Hint: $\{a\} \cup \{b\} = \{a, b\}$ by basic set theory.

Exercise 11. Show $\{1, \ldots, 3\} = \{1, 2, 3\}$. Hint: $\{a\} \cup \{b\} \cup \{c\} = \{a, b, c\}$ by basic set theory.

5. The invariance of counting

We count a finite set S by assigning a number to each object in S. We start by picking an object of S and assigning it 1. Then we assign 2 to another object of S (if there are any more). We continue until we have assigned a number, n say, to a final element of S. We then declare that S has n elements. This is a method we all learn as small children counting, say, apples or Halloween candy.

So in the process of counting a set S of n objects, every integer in $\{1, \ldots, n\}$ is assigned to an element of S. In other words, this process defines a function

$$\{1, \ldots, n\} \to S.$$

We assign distinct numbers to distinct objects, so the function is injective (one-to-one). We assign a number to every element of S, so the function is surjective (onto). Thus counting a finite set S is really the same thing as setting up a bijection $\{1, \ldots, n\} \to S$. This informal discussion motivates the following formal definition.

Definition 6. A *finite counting* of a nonempty set S is a bijection

$$\{1, \ldots, n\} \to S$$

where $n \neq 0$. If such a finite counting exists, then S is said to be *finite*, and the set S is *counted by* n. We also consider the empty set to be finite, and say that it is *counted by* 0.

If a set is not empty and there is no finite counting, then we say that the set is *infinite*.

We feel free to count the objects of a set S in any order we like. In other words, the particular bijection used in the finite counting does not seem to matter: we instinctively feel like we will get the same result regardless of how we choose to assign the integers. In particular, if we have two countings $f : \{1, \ldots, m\} \to S$ and $g : \{1, \ldots, n\} \to S$ of the same set S, we expect that $m = n$. Why do we expect this to hold? Probably very few people are explicitly taught this principle. Is it based on experience or are we hard-wired to believe it? We will pass over such psychological questions. What is important to our axiomatic approach is that we *not* take it for granted. Instead it is a theorem:

Theorem 16 (Invariance of counting)**.** *Suppose that a set S can be counted by m and n. Then $m = n$.*

Definition 7. Suppose that S is a finite set. Then the *cardinality* or *size* of S is defined to be the element $n \in \mathbb{N}$ such that S can be counted by n. This element is unique by the above theorem, so this definition is well-defined. (In fact, this definition would be nonsense if we did not have the above theorem). We write the cardinality of S as $|S|$ or $\#S$.

We will prove this theorem later. The proof will be by induction, and the key step, Lemma 19, will require the following intuitively obvious principle: given any $a \in S$ we can count a last. In other words, suppose that S can be counted by n and that $a \in S$, then we can find a counting $f : \{1, \ldots, n\} \to S$ with $f(n) = a$. To prove this is possible, we will introduce the idea of a *transposition*:

Definition 8. Suppose $a, b \in S$. Consider the function $\tau_{(a\,b)} : S \to S$ defined by the rule $a \mapsto b$, $b \mapsto a$, and $x \mapsto x$ if x is not equal to a or b.

Obviously if $a = b$ then $\tau_{(a\,b)}$ is the identity map. If $a \neq b$ then $\tau_{(a\,b)}$ is called a *transposition*.

In other words, the function $\tau_{a,b}$ just switches a and b: $\tau_{(a\,b)}(a) = b$ and $\tau_{(a\,b)}(b) = a$, but $\tau_{(a\,b)}(c) = c$ when $c \neq a, c \neq b$. The following lemma is easily proved.

Lemma 17. *Suppose $a, b \in S$. Then $\tau^2_{(a\,b)}$ is the identity function on S. Thus $\tau_{(a\,b)} : S \to S$ is its own inverse, and is a bijection.*

Lemma 18. *Suppose that S is a finite set with element $a \in S$, and suppose that S can be counted by n. Then there is a bijection $f : \{1, \ldots, n\} \to S$ with the property that $f(n) = a$.*

Proof. By Definition 6, there is a bijection $g : \{1, \ldots, n\} \to S$. Form the function $f = \tau_{(a\,b)} \circ g$ where $b = g(n)$. Since $\tau_{(a\,b)}$ and g are bijections, the same is true of the composition f. Finally,

$$f(n) = \tau_{(a\,b)}\big(g(n)\big) = \tau_{(a\,b)}(b) = a.$$

□

The following is critical to the proof of the invariance of counting.

Lemma 19. *Suppose S is a set, and suppose that $S' = S \cup \{a\}$ where $a \notin S$. If S' can be counted by $n + 1$, then S can be counted by n.*

Proof. Case 1: S is the empty set. So $S' = \{a\}$. Claim: $n = 0$. To establish the claim, choose a bijection $f : \{1, \ldots, n+1\} \to \{a\}$ which exists since S' is counted by $n+1$. Since a is the only element of the codomain, $f(1) = a$ and $f(n+1) = a$. Thus $f(1) = f(n+1)$. Since f is injective, we have $1 = n+1$. So $0+1 = 1 = n+1$. By the cancellation law, $0 = n$, establishing the claim. Since S is empty, it can be counted by 0 by Definition 6. Since $n = 0$, it can be counted by n as desired.

Case 2: S is not the empty set. By Lemma 18, there is a bijection $f : \{1, \ldots, n+1\} \to S'$ with $f(n+1) = a$. Since f is injective, $f(x) \neq a$ if $x \neq n+1$. Thus $f(x) \in S$ for all $x \in \{1, \ldots, n\}$ (we showed $n+1$ is not in $\{1, \ldots, n\}$ in Theorem 15). Define $h : \{1, \ldots, n\} \to S$ by the rule $h(x) = f(x)$. In other words, the only difference between f and h is the choice of domain and codomain. Observe that h is injective: $h(x) = h(y)$ implies $f(x) = f(y)$, which in turn implies $x = y$ since f is an injection.

Now we will show h is surjective. If $y \in S$ then, since f is surjective, there is an $x \in \{1, \ldots, n+1\}$ such that $f(x) = y$. Now $x \neq n+1$ because $f(n+1) = a \neq y$. (Note: $a \neq y$ since $y \in S$ and $a \notin S$). Since $x \neq n+1$ and since $\{1, \ldots, n+1\} = \{1, \ldots, n\} \cup \{n+1\}$ (Theorem 15), we have that x is in $\{1, \ldots, n\}$. Thus $h(x) = f(x) = y$. We conclude that h is surjective.

Thus h is a bijection. So S is counted by n. □

Now we prove the main theorem:

Proof. (Theorem 16*).* Let A be the set of all natural numbers u with the property that *any set T that can be counted by u can only be counted by u.*

Consider $u = 0$. Suppose T is a set that can be counted by $u = 0$. Definition 6 only assigns the number 0 to the empty set. Thus T is empty. But the empty set can only be counted by $u = 0$ since there is no function $\{1, \ldots, n\} \to \varnothing$. Thus $u = 0$ is in A.

Now suppose $n \in A$. We want to show that $n + 1 \in A$. Let S' be any set that can be counted by $n+1$. We need to show that S' can only be counted by $n + 1$. In other words, suppose that S' can also be counted by p. We need to show that $p = n + 1$.

We know p is positive since S' is non-empty. Thus $p = m+1$ for some m. So S' can be counted by $m+1$ and $n+1$. Since S' is non-empty, let $a \in S'$. Let S be the set obtained by removing a from S'. By Lemma 19, since S' can be counted by $m + 1$, the set S can be counted by m. Similarly, since S' can be counted by $n + 1$, the set S can be counted by n. Since $n \in A$, the set S can only be counted by n. So $n = m$. Thus $n + 1 = m + 1$.

We conclude that $n + 1 \in A$ if $n \in A$. By the induction axiom, $A = \mathbb{N}$.

Now we are ready to prove the main statement. Suppose that S is a set that can be counted by m and n. Since $\mathbb{N} = A$ we must have $n \in A$. By definition of A, the set S can only be counted by n. Thus $m = n$. □

6. Basic properties of counting

The following theorems state that two finite sets have the same size if and only if there is a bijection between them.

Theorem 20. *Suppose S is finite of cardinality n. If $f : S \to T$ is a bijection, then T is finite and has cardinality n.*

Theorem 21. *Suppose S and T are finite of cardinality n. Then there is a bijection $S \to T$.*

Exercise 12. Prove the above two theorems in the case that $n \neq 0$. (The case $n = 0$ follows from a basic fact about the empty set: for any A there is a unique function $f : \varnothing \to A$. It is injective, and its image is the empty set. It is not surjective unless $A = \varnothing$.)

Theorem 22. *Suppose S is finite of cardinality n. Suppose a is an element outside S. Then the set $S' = S \cup \{a\}$ is finite of cardinality $n + 1$.*

Proof. Suppose $n = 0$. Here S is empty, $S' = \{a\}$, and $\{1, \ldots, n+1\} = \{1\}$. Define a function $g : \{1\} \to S'$ by the rule $g(1) = a$. The function g is bijective since it has an inverse $h : S' \to \{1\}$ defined by the rule $h(a) = 1$. By Definition 6, S' is counted by 1.

Suppose $n > 0$. By Definition 6, there is a bijection $f : \{1, \ldots, n\} \to S$. By Theorem 15, $\{1, \ldots, n+1\} = \{1, \ldots, n\} \cup \{n+1\}$ and $n+1 \notin \{1, \ldots, n\}$. So if we want to extend f to a function $f' : \{1, \ldots, n + 1\} \to S'$ we only have to decide where $n + 1$ maps to.

Define $f' : \{1, \ldots, n+1\} \to S'$ by the following rule: if $1 \leq x \leq n$ then $f'(x) = f(x)$, but $f'(n+1) = a$.

We claim that f' is injective. Suppose that $f'(x) = f'(y)$ where $x, y \in \{1, \ldots, n+1\}$. We wish to show that $x = y$. If $x = y = n+1$ then we are done. If one of the two, x say, is $n+1$, but the other is not then $f'(x) = a$ but $f'(y) = f(y) \in S$ since $1 \leq y \leq n$. Since $a \notin S$, we get a contradiction. The final case is where x and y are both not $n+1$. In this case, $f'(x) = f(x)$ and $f'(y) = f(y)$, so $f(x) = f(y)$. Thus $x = y$ since f is injective.

We claim that f' is surjective. We leave the details to the reader. So $f' : \{1, \ldots, n+1\} \to S'$ is a bijection. By Definition 6, S' is counted by $n+1$. □

Exercise 13. Show that f' in the above proof is surjective.

Exercise 14. Prove the following corollaries.

Corollary 23. *If $S = \{a\}$ then S has cardinality 1.*

Corollary 24. *If $S = \{a, b\}$ where $a \neq b$, then S has cardinality 2.*

Theorem 25. *Let $n \in \mathbb{N}$. The set $\{1, \ldots, n\}$ has cardinality n.*

Exercise 15. Give a very short proof of the above theorem.

Exercise 16. Show that if a set S has size 1 then it has a unique element.

Theorem 26. *If A and B are finite, then so is $A \cup B$.*

Proof. We prove the result by induction on the size of B. So fix a finite set A, and define S as follows

$$S \stackrel{\text{def}}{=} \{x \in \mathbb{N} \mid A \cup B \text{ is finite for all sets } B \text{ of size } x\}$$

Clearly, the theorem will be established once we show that $S = \mathbb{N}$ regardless of A. (Note: S depends on A).

If B has size 0, it is empty. So $A \cup B = A$. Thus $A \cup B$ is finite since A is finite. Hence, $0 \in S$.

Suppose $n \in S$. We must show $n+1 \in S$. Let B be a set of size $n+1$. We must show that $A \cup B$ is finite. Since B has nonzero size, it is not empty. Let $b \in B$. Then $B - \{b\}$ has size n by Lemma 19. Since $n \in S$, we conclude that $A \cup (B - \{b\})$ is finite. If $b \in A$ then $A \cup B = A \cup (B - \{b\})$, so $A \cup B$ is finite. If $b \notin A$, then we use Theorem 22 and the equality

$$A \cup B = A \cup (B - \{b\}) \cup \{b\}$$

to conclude that $A \cup B$ is finite. We have established that $n+1 \in S$.

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

We end this section with two lemmas needed in the next section. These require the concept of ordered pair. Recall from set theory that if A and B are sets, then $A \times B$ is defined to be the set of ordered pairs with first

coordinate in A and second coordinate in B. Also recall from set theory that given (a, b) and (a', b') in $A \times B$, we have $(a, b) = (a', b')$ if and only if both $a = a'$ and $b = b'$.

Lemma 27. *Let $m, n \in \mathbb{N}$. There are disjoint finite sets A and B such that A has cardinality m and B has cardinality n.*

Proof sketch. If $m = 0$ let $A = \varnothing$. Otherwise let

$$A = \{(1, x) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq x \leq m\}.$$

In this case, $x \mapsto (1, x)$ is a function $\{1, \ldots, m\} \to A$ with inverse function $(1, x) \mapsto x$. Thus the function is a bijection, so A has size m.

If $n = 0$ let $B = \varnothing$. Otherwise let

$$B = \{(2, x) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq x \leq n\}.$$

In this case, we define a bijection showing B has size n.

The sets A and B can be shown to be disjoint. □

Exercise 17. Show that A and B in the above proof are disjoint.

A similar proof gives the following.

Lemma 28. *Let $x, y, z \in \mathbb{N}$. There are pairwise disjoint finite sets A, B, C such that A has cardinality x, B has cardinality y, and C has cardinality z.*

7. New perspective on addition

In Chapter 1, addition was defined in terms of iteration of successor. However, there are other ways to characterize addition. For example, one might explain to a child that $m + n$ is the number of apples you have if you combine m apples with n additional apples. In other words, if A is a set of m objects, and if B is a set of n objects, then, as long as A and B are disjoint, $m + n$ is the size of $A \cup B$. We now prove the validity of this alternative characterization of addition. It basically follows the pattern of Theorem 26 but uses a few basic laws of addition (proved in Chapter 1 before the associative and commutative laws).

Theorem 29. *Suppose that A and B are disjoint finite sets. Let m be the size of A, and let n be the size of B. Then $A \cup B$ has size $m + n$.*

Proof. We prove this by induction on the size of the second set. Let

$$S = \{u \in \mathbb{N} \mid A \cup X \text{ has size } m + u \text{ for all } X \text{ disjoint from } A \text{ of size } u\}$$

We start by showing $0 \in S$. If X has size 0, then X is the empty set, so $A \cup X = A$. Thus

$$|A \cup X| = |A| = m = m + 0.$$

We have established that $0 \in S$.

Suppose $k \in S$. We must show $k + 1 \in S$. Suppose X has size $k + 1$, and that X is disjoint from A. We must show that $A \cup X$ has size $m + (k + 1)$.

Since X has size $k+1$, it is not empty. Let $x \in X$. Then $X - \{x\}$ has size k by Lemma 19. Since $k \in S$, we conclude that $A \cup (X - \{x\})$ has size $m+k$. Now since A and X are disjoint, x is not in $A \cup (X - \{x\})$. So $A \cup X = A \cup (X - \{x\}) \cup \{x\}$ has size $(m+k)+1$ by Theorem 22. By laws of Chapter 1 (before the associative and commutative laws)

$$(m+k)+1 = \sigma(m+k) = m + \sigma(k) = m + (k+1),$$

so $k+1 \in S_m$.

By the induction axiom, $S = \mathbb{N}$. Since $n \in \mathbb{N}$ we have $n \in S$. By definition of S, we have $|A \cup B| = m+n$. □

Remark 4. The above gives a second characterization of addition. See optional Section 14 for an approach where $m+n$ is actually *defined* as the size of $A \cup B$.

We now give new proofs of the commutative and associative laws. For these proofs to be independent of the old proofs, we would have to show that the proofs do not depend on results requiring the commutative and associative laws of Chapter 1. If you are interested, see optional Section 14 for details of an approach to counting that does not use any results about addition from Chapter 1. From the point of view of Section 14, the proofs presented below are independent of the old proofs.

Theorem 30 (Commutative Law)**.** *If $m, n \in \mathbb{N}$, then $m+n = n+m$.*

Proof. Let A be a set of size m and let B be a set of size n. Choose these sets so that they are disjoint (Lemma 27). Now $A \cup B$ has size $m+n$ by the above theorem, and $B \cup A$ has size $n+m$. Since $A \cup B = B \cup A$, we have $m+n = n+m$. □

Theorem 31 (Associative Law)**.** *If $x, y, z \in \mathbb{N}$, then $(x+y)+z = x+(y+z)$.*

Proof. (sketch). This follows from Lemma 28, and the identity

$$A \cup (B \cup C) = (A \cup B) \cup C$$

□

Exercise 18. Write up the above proof. (You do not need to prove the identity $A \cup (B \cup C) = (A \cup B) \cup C$, since it is part of basic set theory.)

8. Subsets and functions

In this section we investigate issues of cardinality for subsets and functions.

It is intuitively obvious that every subset of a finite set is also finite. This intuition is confirmed by the following theorem.

Theorem 32. *Every subset of a finite set is itself finite.*

Proof. This will be proved by induction on the size of the set. Let

$$S = \{x \in \mathbb{N} \mid \text{all sets } C \text{ of size } x \text{ have only finite subsets}\}.$$

Claim: $0 \in S$. To see this, observe that the only set C of size 0 is the empty set, and the only subset of the empty set is again the empty set. The empty set is finite. So $x = 0$ has the desired property.

Suppose $n \in S$. We must show $n+1 \in S$. To do so, let C be a set of size $n+1$. We claim that all subsets $B \subseteq C$ are finite. If $B = C$ we are done since by assumption C is finite. If B is a proper subset, let $a \in C$ be an element not in B. Then B is a subset of $C - \{a\}$. By Lemma 19, $C - \{a\}$ has size n. Since $n \in S$, it follows that subsets of $C - \{a\}$ are finite. Thus B is finite. We have established that $n + 1 \in S$.

By the induction axiom, $S = \mathbb{N}$. This establishes the theorem. □

Theorem 33. *Let C be a finite set of size c. If A is a subset of C of size a then $a \leq c$. If A is a proper subset then $a < c$.*

Proof. Consider the set B defined as follows:

$$B \stackrel{\text{def}}{=} C - A = \{x \in C \mid x \notin A\}.$$

Then B is a subset of C, so is finite by Theorem 32.

By basic set theory, A and B are disjoint and $A \cup B = C$. In particular, if b is the size of B then $c = a + b$ (Theorem 29). By a property of $\leq$ (Chapter 1) we get $a \leq c$.

Now if A is a proper subset of C, there is an element $w \in C$ that is not in A. So $w \in B$. Thus B is not empty, and the size b of B is not zero. Thus $a < c$ by definition of $<$ (Chapter 1). □

Theorem 34. *Let $f : A \to B$ be an injection where B is finite of size b. Then A is also finite and $a \leq b$ where a is the size of A. Finally, if f is not surjective then $a < b$.*

Proof. Let $C = f[A]$ be the image of f. Since B is finite, the same is true of C (Theorem 32). Let $g : A \to C$ be the function obtained by restriction of codomain. In other words, $g(x)$ is defined to be $f(x)$ for all $x \in A$, and f and g differ only in the choice of codomain. Since f is injective, so is g. Since C is the image of f, it is the image of g. Thus the image of g is the codomain of g. This means that g is also surjective.

Thus g is a bijection. Since C is finite, A is finite and C and A have the same size (Theorem 20). Let a be the common size of A and C. Since C is a subset of B, $a \leq b$ (Theorem 33). The proof of the final statement is left to the reader. □

Exercise 19. Complete the above proof by proving the final statement.

Exercise 20. Prove the following two corollaries of Theorem 34.

Corollary 35 (Pigeonhole Principle)**.** *Let A be a finite set of size a and B a finite set of size b. If $f : A \to B$ is a function, and if $a > b$, then there are distinct elements of A mapping (via f) to the same element of B.*

Corollary 36. *Let $f : A \to B$ be an injection between two finite sets of the same size. Then f is a bijection.*

Remark 5. Informally, the Pigeonhole principles says that if there are more pigeons than pigeonholes, then there is a pigeon hole with more than one pigeon. Think of A as a set of pigeons, and B as a set of pigeonholes.

Theorem 37. *Let $g : A \to B$ be a surjection. If A is finite of size a then B is also finite, and the size b of B satisfies the inequality $a \geq b$. If, in addition, g is not injective then $a > b$.*

Proof. If $a = 0$ then $A = B = \varnothing$, and the result follows. So assume $a > 0$. Let $h : \{1, \ldots, a\} \to A$ be a finite counting (Definition 6). Then h is a bijection, so it is necessarily a surjection. This implies that the composition $g \circ h : \{1, \ldots, a\} \to B$ is surjective.

Now $g \circ h$ might not be injective: there could be integers $x, y \in \{1, \ldots, a\}$ with $g(h(x)) = g(h(y))$. (In fact, if g is not injective, then $g \circ h$ cannot be). We seek a subset $C \subseteq \{1, \ldots, a\}$ on which $g \circ h$ is injective. To form C, we will want to throw out either x or y whenever $g(h(x)) = g(h(y))$ occurs. Let's agree to always throw out the larger integer. So officially C is defined to be the set of all $x \in \{1, \ldots, a\}$ with the property that, for all $y \in \{1, \ldots, a\}$

$$g(h(x)) = g(h(y)) \;\Rightarrow\; x \leq y.$$

Let f be the restriction of $g \circ h$ to C. We claim that $f : C \to B$ is an injection. To see this, suppose that $f(x) = f(y)$ where $x, y \in C$. Then $g(h(x)) = g(h(y))$. By the definition of C, this implies $x \leq y$ and $y \leq x$. So $x = y$. Thus f is injective.

We claim that $f : C \to B$ is a surjection. Let $b \in B$. Since $g \circ h$ is surjective, there is an integer y with $g(h(y)) = b$. Let x be the smallest such integer (existence by well-ordered property). Then $x \in C$. Thus f is surjective.

So f is a bijection. Since C is a subset of $\{1, \ldots, a\}$, and since $\{1, \ldots, a\}$ has size a, we have that C is finite (Theorem 32) and $|C| \leq a$ (Theorem 33). Since f is a bijection, B is finite and $|B| = |C|$ (Theorem 20). So $|B| \leq a$ as desired.

To establish the second statement, observe that if g is not injective, then C is a proper subset of $\{1, \ldots, m\}$. So $|C| < a$ (Theorem 33), giving us $|B| < a$ as desired. □

Corollary 38. *Let $g : A \to B$ be a surjection between two finite sets of the same size. Then g is a bijection.*

Theorem 39. *If A is a finite set of size n, and if $m \leq n$, then there is a subset $B \subseteq A$ of size m.*

Proof. (sketch). Let $f : \{1, \ldots, n\} \to A$ be a finite counting. Let B be the image of $\{1, \ldots, m\}$ under f. □

In Chapter 1 we showed that $\mathbb{N}$ is well-ordered. In other words, every non-empty subset $S \subseteq \mathbb{N}$ is has a minimum. This leads to a question: which subsets have a maximum?

Theorem 40. *Let S be a non-empty subset of $\mathbb{N}$. Then S has a maximum if and only if S is finite.*

Proof. (sketch). If S has a maximum n, then S is a subset of $T = \{0, \ldots, n\}$. Since $\{0, \ldots, n\} = \{0\} \cup \{1, \ldots, n\}$, T is finite. Thus the subset S is finite.

The converse is proved by induction. Let A be the set consisting of 0 together with the set of all positive $x \in \mathbb{N}$ with the following property: *all finite subsets of $\mathbb{N}$ of size x have a maximum.*

Suppose $n \in A$. We must show $n + 1 \in A$. In other words, if $S \subseteq \mathbb{N}$ has size $n + 1$ we must find a maximum M. If $n = 0$, then S has a single element which is automatically a maximum. If $n \neq 0$, then pick an element $s \in S$ at random. If s is a maximum, we are done. Otherwise, let M be the maximum of $S - \{s\}$ (which exists since $n \in A$). □

Exercise 21. Let $S \subseteq \mathbb{N}$ be a non-empty subset. Suppose that S has an upper bound $B \in \mathbb{N}$ (not necessarily in S). Show that S is finite.

9. New perspective on multiplication

In Chapter 1 multiplication was defined in terms of iteration of addition. However, there are other ways to characterize multiplication. For example, one can count the number of ordered pairs: if there are m choices for the first coordinate of an ordered pair, and if there are n choices for the second coordinate of an ordered pair, then $m \cdot n$ gives the total number of ordered pairs. In other words, if A is finite of size m and B is finite of size n then $m \cdot n$ is the size of $A \times B$. We now prove that this alternative characterization of multiplication is valid.

Theorem 41. *Suppose that A and B are finite sets. Let m be the size of A, and let n be the size of B. Then $A \times B$ is finite with size $m \cdot n$.*

Proof. (Induction) Let

$$S = \{u \in \mathbb{N} \mid \text{the size of } A \times X \text{ is } mu \text{ for all } X \text{ of size } u\}.$$

First we show $0 \in S$. Let X have size 0, so X is empty. Observe that $A \times X$ is also empty since no ordered pair has second coordinate in the empty set. Thus $|A \times X| = 0 = m \cdot 0$. We conclude that $0 \in S$.

Suppose $k \in S$. We must show $k + 1 \in S$. In other words, for any X of size $k + 1$ we must show $|A \times X| = m(k + 1)$.

Since $|X| = k + 1$, the set X is not empty. Let $x \in X$. Then $X - \{x\}$ has size k by Lemma 19. Since $k \in S$, we conclude that $A \times (X - \{x\})$ has size $m \cdot k$. Observe that

$$A \times X \;=\; A \times (X - \{x\}) \;\cup\; A \times \{x\}$$

and that the union is disjoint. Also, there is a bijection $A \to A \times \{x\}$, so A and $A \times \{x\}$ have the same size. So, by Theorem 29, $A \times X$ has size $m \cdot k + m$. From Chapter 1, $m \cdot k + m = m \cdot \sigma k = m(k+1)$. So $k+1 \in S$.

By the induction axiom, $S = \mathbb{N}$. Since $n \in \mathbb{N}$ we have $n \in S$. By definition of S we have that $|A \times B| = mn$. □

Remark 6. This result is related to a fundamental counting principle: if you have m choices for one property, and n choices for a second property, then there are mn total combinations given by the two choices. For example, if your computer has five fonts and each font comes in plain, bold, and italic style, then there are 15 total combinations of font and style. To see the connection between this principle and the above theorem, think of the two choices as giving the coordinates of an ordered pair. So the number of combinations is the number of ordered pairs.

Remark 7. We can write the above theorem as

$$|A \times B| = |A| \cdot |B|.$$

This explains why the symbol $\times$ is popular for Cartesian product. Old set theory books sometimes use $+$ for union due to the connection between union and addition, but this notation lost out to $\cup$. If the $+$ notation had survived we would have, for disjoint unions,

$$|A + B| = |A| + |B|.$$

Remark 8. The above theorem gives a new characterization of multiplication. Observe that the above theorem and proof are the first place where we have used multiplication in this chapter. For instance, we have used facts about addition and inequalities from Chapter 1, but the facts we used were not those dependent on multiplication. So everything so far has been "multiplication free".

The above proof uses just two properties about multiplication from Chapter 1: (i) $0 = m \cdot 0$ and (ii) $m \cdot n + m = m \cdot \sigma n$. These two facts occur in Chapter 1 before the commutative, associative, and distributive laws of multiplication.

We will now give new proofs of the commutative, associative and distributive laws of multiplication, which are independent of the old proofs. They give more insight into why these laws are true than the induction proof of Chapter 1. The commutative law is based on the following easy exercise.

Exercise 22. Let A and B be sets. Show that there is a natural bijection between $A \times B$ and $B \times A$. This natural bijection is called a *canonical bijection*.

Theorem 42 (Commutative Law)**.** *If $m, n \in \mathbb{N}$, then $m \cdot n = n \cdot m$.*

Proof. Let $A = \{1, \ldots, m\}$ and $B = \{1, \ldots, n\}$. By Theorem 41, $A \times B$ has size mn and $B \times A$ has size nm. By the previous exercise, there is a bijection $A \times B \to B \times A$. Thus $m \cdot n = n \cdot m$ by Theorem 20. □

Theorem 43 (Associative Law)**.** *If $x, y, z \in \mathbb{N}$, then $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.*

Proof. (sketch). This is similar to the previous proof. The key step is to define a bijection

$$(A \times B) \times C \to A \times (B \times C)$$

by the rule $\big(a, (b, c)\big) \mapsto \big((a, b), c\big)$. □

Theorem 44 (Distributive Law)**.** *If $x, y, z \in \mathbb{N}$, then $(x + y)z = xz + yz$.*

Proof. Let A, B, C be finite sets of size x, y, z respectively, and choose A and B to be disjoint (Lemma 28). Then

$$(A \cup B) \times C = (A \times C) \cup (B \times C).$$

The result follows from Theorem 29 and Theorem 41. □

Exercise 23. In the above proof we used the fact that

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

and the fact that $A \times C$ and $B \times C$ are disjoint. Show these two facts, and show how the statement of the theorem follows from Theorem 29 and Theorem 41.

Remark 9. There is another characterization of multiplication that is commonly used. Suppose A is a set of disjoint finite sets, where each member of A is a set of size n. Suppose A is finite of cardinality m. Then the union of all the sets in A has mn elements.

For example, if you have five apples, and each apple has three worms, then there are 15 worms total (here each member of A is the set of worms on one particular apple). This principle is closely related to the multiplication principle for Cartesian products proved above. See the optional Section 15 for more information.

10. New perspective on subtraction

Above we described set-theoretic characterizations of addition and multiplication. There is also a simple set-theoretic characterization of subtraction. For example, informally one might describe $5-2$ to be the number of apples you have when you start with a set of 5 apples, and remove a subset of 2 apples. The following theorem implements this idea.

Theorem 45. *Let A be a finite set of size n, and let B be a subset of size m. Then the set $A - B = \{a \in A \mid a \notin B\}$ has size $n - m$.*

Proof. (Sketch) Observe that $A = B \cup (A - B)$. □

Exercise 24. Prove the above theorem. Be sure to mention that the subsets on the right-hand side are disjoint. Also refer to Theorem 29 and Theorem 2.

From Section 7 we know that addition gives the size of $A \cup B$ if A and B are finite disjoint sets. What if they are not disjoint? The answer is given by the inclusion-exclusion principle:

Theorem 46 (Inclusion-exclusion principle)**.** *Let A and B be finite sets that are not necessarily disjoint. Then $A \cup B$ is finite, and*

$$|A \cup B| = \big(|A| + |B|\big) - |A \cap B|.$$

In other words

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

Exercise 25. Prove the above theorem. Hint: show

$$A \cup B = A \cup \big(B - (A \cap B)\big).$$

Also use Theorem 7.

Remark 10. The above idea can be extended to three or more sets.[2] For example, if A, B, C are finite sets, then $A \cup B \cup C$ is finite and $|A \cup B \cup C|$ is given by

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

11. New perspective on exponentiation

In Chapter 1 exponentiation was defined in terms of iteration of multiplication. However, there are other ways to characterize exponentiation. For instance, we will see that n^m is the number of functions $A \to B$ where A is finite of size m and where B is finite of size n. Because of this, the set of functions $A \to B$ is written B^A:

Definition 9. Let A and B be sets. Then define B^A to be the set of functions $A \to B$.

Theorem 47. *Suppose that A and B are finite sets. Let m be the size of A, and let n be the size of B. Then B^A is finite with size n^m.*

Proof. (Induction). Let

$$S = \{u \in \mathbb{N} \mid \ B^X \text{ has size } n^u \text{ for every } X \text{ of size } u\}$$

First we show $0 \in S$. So let X have size 0. In other words $X = \varnothing$. Since there is a unique function $\varnothing \to B$, the size of $B^{\varnothing}$ is 1. But $1 = n^0$, so B^X has size n^0. Hence, $0 \in S$.

Suppose $k \in S$. We must show $k + 1 \in S$. In other words, we must show that if $|X| = k + 1$, then $\left|B^X\right| = n^{k+1}$. Since X has size $k + 1$, it is not empty. Let $x \in X$. Then $X - \{x\}$ has size k by Lemma 19. Since $k \in S$ (inductive hypothesis), we conclude that $B^{X-\{x\}}$ has size n^k.

Every function $f : X \to B$ can be obtained by extending a function $g : (X - \{x\}) \to B$ by defining the value $b \in B$ for $f(x)$. In other words, specifying a function $f : X \to B$ is the same as choosing an ordered pair (g, b) where $g \in B^{X-\{x\}}$ and where $b \in B$. Thus there is a bijection

$$B^{X-\{x\}} \times B \to B^X.$$

[2] I do not recommend proving this now. Life is much easier when we have the identity $x - y = x + (-y)$, which is not developed until Chapter 3.

But $B^{X-\{x\}} \times B$ has size $n^k \cdot n$ by Theorem 41 and the inductive hypothesis. By Theorem 20, B^X must also have size $n^k \cdot n$. From Chapter 1 we know $n^k \cdot n = n^{k+1}$. We have established that $k+1 \in S$.

By the induction axiom, $S = \mathbb{N}$. Since $m \in \mathbb{N}$ it must be in S. By the definition of S, the set B^A has size n^m. □

Remark 11. We can write the conclusion of the above theorem as

$$\left|B^A\right| = |B|^{|A|}.$$

Remark 12. The only exponentiation identities from Chapter 1 used in the above proof are that $n^0 = 1$ and $n^k n = n^{k+1}$. The following give new, independent, proofs of other identities from Chapter 1.

Theorem 48. *If $x, y, n \in \mathbb{N}$ then*

$$(xy)^n = x^n y^n.$$

Proof. (sketch). Let A be a finite set of size x, let B be a finite set of size y, and let C be a finite set of size n. Choosing a function $f : C \to A \times B$ is the same as choosing two functions (f_1, f_2) with $f_1 : C \to A$ and $f_2 : C \to B$. In other words, there is bijection

$$(A \times B)^C \to A^C \times B^C.$$

The result follows from Theorem 41 and Theorem 47. □

Theorem 49. *If $x, m, n \in \mathbb{N}$ then*

$$x^{m+n} = x^m x^n.$$

Proof. (sketch). Let A be a finite set of size x, let B be a finite set of size m, and let C be a finite set of size n. Choose B and C to be disjoint. Choosing a function $f : B \cup C \to A$ is the same as choosing two functions (f_1, f_2) with $f_1 : B \to A$ and $f_2 : C \to A$. In other words, there is bijection

$$A^{B \cup C} \to A^B \times A^C.$$

The result follows from Theorem 29, Theorem 41, and Theorem 47. □

Theorem 50. *If $n \in \mathbb{N}$ is not 0 then*

$$0^n = 0.$$

Proof. (sketch). Let B be the empty set, and let A be a finite set of size n. There are no functions from A into the empty set. So B^A is empty. The result follows from Theorem 47. □

Theorem 51. *If $n \in \mathbb{N}$ then*

$$1^n = 1.$$

Proof. (sketch). Let $B = \{1\}$, and let A be a finite set of size n. Every function $f : A \to B$ is given by the formula $f(x) = 1$. Thus there is one function in B^A. The result follows from Theorem 47. □

Theorem 52. *If $x, n, m \in \mathbb{N}$ then*

$$\big(x^m\big)^n = x^{mn}.$$

Proof. (sketch). Let A be a finite set of size x, let B be a finite set of size m, and let C be a finite set of size n. Claim: there is a bijection

$$\varphi : (A^B)^C \to A^{B\times C}.$$

To see this, suppose $f : C \to A^B$ is given. Then define $\varphi(f) : B \times C \to A$ by the rule $(b, c) \mapsto \big(f(c)\big)(b)$. This rule makes sense since $f(c)$ is itself a function $B \to A$. It is an exercise to show that φ has an inverse. Thus φ is a bijection.

The result follows from Theorem 41 and Theorem 47. □

12. Laws of iteration

We have two fundamentally different ways of viewing addition: (i) iterated successor (from Chapter 1), and (ii) the size of disjoint unions. In this section we give a third way of looking at addition: (iii) the order of iteration obtained by composing two iterations. We give a similar result for multiplication.

Theorem 53. *Let $f : S \to S$ be a function whose domain equals its codomain. If $m, n \in \mathbb{N}$ then*

$$f^m \circ f^n = f^{m+n}.$$

Proof. (Induction on n). Fix $m \in \mathbb{N}$. Let $A_m = \{x \in \mathbb{N} \mid f^{m+x} = f^m \circ f^x\}$. Observe that $0 \in A_m$ since f^0 is the identity (Chapter 1).

Now assume $n \in A_m$. We will show that $n + 1 \in A_m$.

$$\begin{aligned} f^m \circ f^{n+1} &= f^m \circ (f^n \circ f) && \text{(Lem. 54 below)} \\ &= (f^m \circ f^n) \circ f && \text{(Assoc. of } \circ) \\ &= f^{m+n} \circ f && (n \in A_m) \\ &= f^{m+n+1} && \text{(Lem. 54)} \end{aligned}$$

So $n + 1 \in A_m$.

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

The above used the following lemma. Recall that $f^{n+1} = f \circ f^n$ by the iteration axiom of Chapter 1 (actually a theorem: see the optional sections).

Lemma 54. *Let $f : S \to S$ be a function whose domain equals its codomain. If $n \in \mathbb{N}$ then*

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

Proof. Let $A = \{x \in \mathbb{N} \mid f^{x+1} = f^x \circ f\}$. Observe that $0 \in A$ since f^0 is the identity and $f^1 = f$ (see Chapter 1).

Now assume $n \in A$. We must show that $n+1 \in A$.

$$\begin{aligned} f^{(n+1)+1} &= f \circ f^{n+1} && \text{(Iteration Axiom/Theorem)} \\ &= f \circ (f^n \circ f) && (n \in A) \\ &= (f \circ f^n) \circ f && \text{(Assoc. of } \circ) \\ &= f^{n+1} \circ f. && \text{(Iteration Axiom/Theorem)} \end{aligned}$$

So $n+1 \in A$.

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

Theorem 55. *Let $f : S \to S$ be a function whose domain equals its codomain. If $m, n \in \mathbb{N}$ then*

$$(f^m)^n = f^{mn}.$$

Exercise 26. Prove the above theorem.

Observe that we now have three fundamental ways to think of multiplication. (i) iterated addition, (ii) size of finite Cartesian products, (iii) the index of iteration of an iteration of an iteration.

13. Infinite Sets

Definition 10. A set is *infinite* if it is not finite.

Theorem 56. *Suppose that B is infinite and that A is a finite subset of B. Then $B - A$ is infinite.*

Exercise 27. Use Theorem 26 to prove the above theorem.

Theorem 57. *If A is infinite, then A has subsets of every finite cardinality. In other words, given n there is a subset of A of cardinality n.*

Proof. (sketch) Induction on n. □

Theorem 58. *If A has subsets of every finite cardinality, then A is infinite.*

Proof. (sketch) Suppose not. Then $|A| = a$ for some $a \in \mathbb{N}$. By assumption, A has a subset of size $a+1$. This contradicts Theorem 33. □

Theorem 59. *If there is an injection $\mathbb{N} \to A$ then A is infinite.*

Proof. (sketch) Such an injection can be used to produce subsets of every finite cardinality. □

There is another axiom of mathematics that we have not needed called the *axiom of choice*. If we assumed such an axiom, we could prove the following converse to the above theorem.

Theorem 60. *If A is infinite, then there is an injection $\mathbb{N} \to A$.*

The basic idea of the proof is to use the axiom of choice to give a function h that chooses an element $h(B)$ in $A - B$ for each finite subset B of A. Next recursively define $B_0 = \varnothing$ and $B_{n+1} = B_n \cup \{h(B_n)\}$. Now consider the function $n \mapsto h(B_n)$ and show it is injective.

14. Developing counting without addition (optional)

Earlier in this chapter we used $\{1, \ldots, n\}$ in our development of counting. The sets $\{1, \ldots, n\}$ depend on properties of $\leq$, which in turn depend on properties of addition. In this section we explore a way of developing counting that does not depend in any way on addition.

Instead of using $\{1, \ldots, n\}$, it will be more convenient to use $\{0, \ldots, n-1\}$. In other words, we will count n objects by starting with 0 and ending with $n-1$. This is a bit unusual, but it will work. We write $\{0, \ldots, n-1\}$ compactly as $[n]$.

We will show how to define $[n]$ without mentioning $\leq$. The formal definition of $[n]$ is a recursive definition. The technique of recursion was developed in the optional sections of Chapter 1, and does not depend on addition or inequalities.

Definition 11. Define $[n]$, for $n \in \mathbb{N}$, by the following recursive conditions:

$$[0] \stackrel{\text{def}}{=} \varnothing,$$

$$[\sigma n] \stackrel{\text{def}}{=} [n] \cup \{n\}.$$

Informally it is clear that the above definition will give $[1] = \{0\}$, $[2] = \{0, 1\}$, $[3] = \{0, 1, 2\}$, et cetera.

The following is an easy consequence of the recursive definition:

Theorem 61. *If $n \neq 0$, then $[n]$ contains the predecessor of n. In particular, $[n]$ is non-empty.*

The following can be proved by induction.

Theorem 62. *If x is a non-zero element of $[n]$, then the predecessor of x is in $[n]$.*

A consequence of the above theorem is the following:

Theorem 63. *Given $n \in \mathbb{N}$,*

$$n \notin [n].$$

In particular, the union $[\sigma n] = [n] \cup \{n\}$ is a disjoint union.

Proof. By induction. The base case is easy since [0] is empty. To show that $\sigma n \notin [\sigma n]$ follows from $n \notin [n]$, use the equation $[\sigma n] = [n] \cup \{n\}$. Suppose σn is in $[\sigma n]$. In the first case, $\sigma n \in [n]$. Thus $n \in [n]$ by the previous theorem, a contradiction. In the second case, $\sigma n = n$, contradicting a result of Chapter 1 (proved before the definition of addition). $\square$

We now describe how counting can be developed from the sets $[n]$, avoiding addition and inequalities.

14.1. **Modifications to Section 5.** Change Definition 6 by requiring a bijection

$$[n] \to S.$$

(This actually works when $n = 0$, so we do not really need special provisions for the empty set.) Next replace Lemma 18 and Lemma 19 by the following:

Lemma 64. *Suppose that S is a finite set with element $a \in S$, and suppose that S can be counted by σn. Then there is a bijection $f : [\sigma n] \to S$ with the property that $f(n) = a$.*

Lemma 65. *Suppose S is a set, and suppose that $S' = S \cup \{a\}$ where $a \notin S$. If S' can be counted by σn, then S can be counted by n.*

The proofs of these are obtained by adapting the proofs of Lemma 18 and Lemma 19 in a straightforward manner (often by shifting numbers down by one). The invariance of counting (Theorem 16) can now be proved by appealing to Lemma 65 instead of Lemma 19.

14.2. **Modifications to Section 6.** Replace all references to $\{1, \ldots, n\}$ with $[n]$, and all references to $n + 1$ with σn. Everything remains valid. In fact, some proofs are easier because the empty set is not a separate case. In the proof of Lemma 27 use $A = \{(1, x) \mid x \in [m]\}$ and $B = \{(1, x) \mid x \in [n]\}$.

14.3. **Modifications to Section 7.** Replace Theorem 29 by the following lemma and definition.

Lemma 66. *Suppose there are bijections $A \to A'$ and $B \to B'$. If A and B are disjoint, and if A' and B' are disjoint, then there is a bijection $A \cup B \to A' \cup B'$.*

Proof. (Sketch) Define $A \cup B \to A' \cup B'$ in terms of $A \to A'$ and $B \to B'$. □

Definition 12 (addition)**.** Let $m, n \in \mathbb{N}$. Then $m + n$ is defined to be the size of $A \cup B$ where A is any set of size m, and B is any set of size n disjoint from A.

Lemma 27 tells us that such A and B exist, Theorem 26 tells us that $A \cup B$ is finite, Lemma 66 and Theorem 20 tell us that the size of $A \cup B$ is independent of the choice of A and B. This shows that $m+n$ is a well-defined natural number; in other words, it is independent of any choices.

Observe that addition is now defined in terms of sizes of sets instead of in terms of iteration.

Theorem 30 and Theorem 31 are kept unchanged.

This gives a new, independent, approach to addition and the commutative and associative laws. However, one might want to keep both approaches to addition since they both have advantanges, but at some point they should be shown to give equivalent results. This can be done with the following theorem (proved by induction on n):

Theorem 67. *All binary operators on $\mathbb{N}$ satisfying the following laws are equivalent:*

$$m + 0 = m \qquad \textit{and} \qquad m + \sigma n = \sigma(m + n)$$

Using this theorem, we would just need to show that both definitions satisfy the above laws. In Chapter 1 we showed that addition, as defined there, satisfies these laws. The definition of addition, outlined in this section, using counting can also be easily shown to satisfy these laws. Thus both approaches are ultimately seen to give the same addition operation.

15. Fourth characterization of multiplication (optional)

We now have three characterizations of multiplication: (i) iterated addition, (ii) counting finite Cartesian products, and (iii) the iteration needed to iterate a given iteration. We now discuss a common fourth characterization that is closely related to the second.

Theorem 68. *Let A be a set of pairwise disjoint finite sets. Suppose each member of A is a set of n elements, and that A has m members. Then the union $\bigcup A$ has $m \cdot n$ elements.*

Proof. This follows from Theorem 20, the existence (Lemma 69) of a bijection $\bigcup A \to A \times \{1, \ldots, n\}$, and Theorem 41. □

Lemma 69. *Let A be as above. Then there is a bijection*

$$\bigcup A \to A \times \{1, \ldots, n\}.$$

Proof. (sketch) Use induction on the size of A. □

16. The Axiom of Choice (optional)

Not needed in this course, but needed in more advanced math. (MORE IN FUTURE EDITIONS).

17. Other

Show that $n - 0 = n$.