CHAPTER 2 SUMMARY: THE NATURAL NUMBERS (PART 2)

MATH 422, CSUSM. SPRING 2009. AITKEN

1. Introduction

This is a summary of Chapter 2 from Number Systems (Math 378). Here we continue the discussion of the set $\mathbb{N}$. We begin by considering subtraction $n-m$ where we assume $n \geq m$. Next we consider the well-ordering property of $\mathbb{N}$ and the related maximum principle. Next we consider *counting* and *cardinality* which are the most basic applications of the natural numbers. We end with a few theorems about infinite sets.

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

Of course, there is nothing wrong with adopting the other convention as long as it is done consistently.

2. Subtraction

Subtraction $n - m$ 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 consider negative integers, and then we will be able to define $n - m$ for all integers n and m.

In Chapter 1 we saw 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.

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*.

Directly from the definition we have the following.

Date: January 20, 2009.

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 $n - n = 0$.*

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 with Theorem 2.

Exercise 3. Give a counter-example showing that subtraction is not associative. Is subtraction commutative?

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

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

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

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

3. The well-ordering property

Throughout this section, let U be a set which is linearly ordered by a relation $<$. In other words, $<$ is transitive and satisfies the trichotomy law. In this chapter we are mainly interested in the case $U = \mathbb{N}$, but Definition 2 and Theorem 9 are more general and will apply to all linearly ordered sets U including some of the other number systems developed in later chapters (such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$). For a general U, we define $\leq$ in terms of $<$ and $=$ in the same way we defined it for $U = \mathbb{N}$. In other words $a \leq b$ is defined as $a < b \vee a = b$.

Some of the properties that we established in Chapter 1 for $\mathbb{N}$ hold for all linearly ordered sets. This is illustrated in the next two exercises which hold on account of the trichotomy assumption.

Exercise 4. Suppose $x, y \in U$. Show that $x \leq y$ is the negation of $y < x$. In other words, show that $x \leq y$ is true if and only if $y < x$ is false. (It then follows, by easy logic, that $x \leq y$ is false if and only if $y < x$ is true.)

Exercise 5. Suppose $x, y \in U$. Show that if $x \leq y$ and $y \leq x$ then $x = y$. (This generalizes a result of Chapter 1).

Definition 2. Let $S \subseteq U$. An element $m \in S$ is called a *minimum* if $m \leq x$ holds for all $x \in S$. An element $M \in S$ is called a *maximum* if $x \leq M$ holds for all $x \in S$.

Warning. The elements m and M in the above must be in S. It is not enough for them to be in U. If the requirement $m, M \in S$ is replaced by $m, M \in U$, then we call m a *lower bound* for S and M an *upper bound* for S.

Not all sets $S \subseteq U$ have a minimum or a maximum. For example, if $S = U = \mathbb{N}$ then S has no maximum. In a later chapter we will describe intervals such as $S = (0, 1]$ in $U = \mathbb{Q}$ that have no minimum (0 is not a minimum of $(0, 1]$ since it is not in the set, but it is a lower bound). If a minimum does exist in S then it is unique, likewise for a maximum:

Theorem 9. *The minimum of S, if it exists, is unique. The maximum of S, if it exists, is unique.*

Exercise 6. Prove the above theorem.

Warning. On the other hand, upper and lower bounds, if they exist, are not necessarily unique.

Exercise 7. What is the minimum of $S = \mathbb{N}$? Show that $S = \mathbb{N}$ has no maximum. (Here $U = \mathbb{N}$.)

Now we focus on $U = \mathbb{N}$. In this case, a non-empty subset of S may or may not have a maximum, but, as we will show, it is guaranteed to have a minimum.

Definition 3. An linearly ordered set U is said to be *well-ordered* if every non-empty subset $S \subseteq U$ has a minimum.

Of course, different subsets of S can have different minima.

Theorem 10. *The set of natural numbers $\mathbb{N}$ is well-ordered.*

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

Theorem 11 (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.*

4. 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 definitions.

Definition 4. 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 $\{x \in \mathbb{N} \mid m \leq x \leq n\}$. This is considered to be the empty set unless $m \leq n$.

We allow common variants. For example, $\{1, 2, \ldots, n\}$ is another way of writing $\{x \in \mathbb{N} \mid 1 \leq x \leq n\}$.

Definition 5. A *finite counting* of a 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 $m = n$. This expectation can indeed be proved mathematically:

Theorem 12 (Invariance of counting)**.** *Suppose that a set S can be counted by m and n. Then $m = n$.*

Definition 6. 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. We write the cardinality of S as $|S|$ or $\#S$.

5. Basic properties of counting

Theorem 13. *Suppose S is finite of cardinality n. If $f : S \to T$ is a bijection, then T is finite and has cardinality n.*

Theorem 14. *Suppose S and T are finite of cardinality n. Then there is a bijection $S \to T$.*

Corollary 15. *If $S = \{a\}$ then S has cardinality* 1.

Corollary 16. *If $S = \{a, b\}$ where $a \neq b$, then S has cardinality* 2.

Theorem 17. *Let $n \in \mathbb{N}$. The set $\{1, \ldots, n\}$ has cardinality n.*

Exercise 8. Give a very short proof of the above theorem.

Theorem 18. *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 $m + n$.*

Theorem 19. *Every subset of a finite set is itself finite. 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 $a < c$.*

Theorem 20. *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 $a < b$.*

Corollary 21 (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.*

Remark 2. 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.

Corollary 22. *Let $f : A \to B$ be an injection between two finite sets of the same size. Then f is a bijection.*

Theorem 23. *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 $a > b$.*

Corollary 24. *Let $g : A \to B$ be a surjection between two finite sets of the same size. Then g is a bijection.*

We know 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 25. *Let S be a non-empty subset of $\mathbb{N}$. Then S has a maximum if and only if S is finite.*

Exercise 9. 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.

Theorem 26. *Suppose that A and B are finite sets. Let m be the size of A, and let n be the size of B. Then the Cartesian product $A \times B$ is finite with size $m \cdot n$.*

Remark 3. 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 4. 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,

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

Theorem 27. *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 $n - m$.*

Above we mentioned 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 28 (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

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

Remark 5. The above idea can be extended to three or more sets. 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

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

Definition 7. Let A and B be sets. Then define B^A to be the set of functions $A \to B$.

Theorem 29. *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.*

Remark 6. We can write the conclusion of the above theorem as

$$\big|B^A\big| = |B|^{|A|}.$$

6. Infinite Sets

Definition 8. A set is *infinite* if it is not finite.

Theorem 30. *If $A \subseteq B$ and if A is infinite, then so is B.*

Theorem 31. *Suppose that B is infinite and that A is a finite subset of B. Then $B - A$ is infinite.*

Theorem 32. *If A is infinite, then there are subsets of every finite cardinality. In other words, given n there is a subset of A of cardinality n.*

Theorem 33. *If A has subsets of every finite cardinality, then A is infinite.*

Theorem 34. *If there is an injection $\mathbb{N} \to A$ then A is infinite.*