

CHAPTER 1 SUMMARY: THE NATURAL NUMBERS (PART I)

MATH 422, CSUSM. SPRING 2009. AITKEN

1. INTRODUCTION

This is a summary of Chapter 1 from Number Systems (Math 378). In Chapter 1, addition, multiplication, and exponentiation are defined in terms of iteration. In this summary we will not focus on the particular method for defining these operation, since there are a variety of possible definitions. Instead we will focus on the properties of these operations.

2. NATURAL NUMBERS

The number natural numbers are the ordinary whole numbers

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

starting with 0 and continuing indefinitely.¹

An important proof technique for \mathbb{N} is the induction principle:

Induction Principle (Subsets). *Suppose S is a subset of \mathbb{N} such that (i) $0 \in S$, and (ii) $n \in S$ implies $n + 1 \in S$ for arbitrary $n \in \mathbb{N}$. Then $S = \mathbb{N}$.*

$$S \subseteq \mathbb{N} \wedge 0 \in S \wedge \left(\forall n (n \in S \Rightarrow \sigma n \in S) \right) \implies S = \mathbb{N}$$

Since every property of the natural numbers determines a subset, this is equivalent to the following:

Induction Principle (Properties). *Suppose $P(x)$ is a property of natural numbers. Suppose (i) $P(0)$, and (ii) $P(n) \implies P(n+1)$ for arbitrary $n \in \mathbb{N}$. Then $P(x)$ holds for all $x \in \mathbb{N}$.*

There is a more succinct way of stating this axiom using the ideas of successor and closure. The *successor* of a natural number n is $n + 1$. A subset $S \subseteq \mathbb{N}$ is said to be *closed under successor* if $x + 1 \in S$ whenever $x \in S$. For example, $\{7, 8, 9, \dots\}$ is closed under successor but $\{0, 1, 2, 3, 4\}$ is not closed. Using these concepts, we can express the induction principle as follows:

Induction Principle (Short Form). *If $S \subseteq \mathbb{N}$ contains 0 and is closed under successor then $S = \mathbb{N}$.*

Date: January 25, 2009.

¹Warning: some authors do not include 0 in the set of natural numbers.

3. ADDITION

Addition defines a function $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$. Functions $S \times S \rightarrow S$ are called *binary operations*, so $+$ is a binary operation on \mathbb{N} . It can be described as the n th natural number following m .

$$m + n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

Theorem 1. *For all $m \in \mathbb{N}$*

$$m + 0 = m.$$

Theorem 2 (Associative Law). *For all $x, y, z \in \mathbb{N}$*

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

Theorem 3 (Commutative Law). *If $x, y \in \mathbb{N}$ then*

$$x + y = y + x.$$

Exercise 1. Prove $(x + y) + z = (x + z) + y$.

Theorem 4. *If $n, m \in \mathbb{N}$ are such that $0 = m + n$ then $n = m = 0$.*

By definition of addition, we know that \mathbb{N} is closed under addition. In other words, if $a, b \in \mathbb{N}$ then $a + b \in \mathbb{N}$. The following states that \mathbb{N}^+ is closed as well.

Corollary 5. *The set \mathbb{N}^+ of nonzero natural numbers is closed under addition. In other words, if $m, n \in \mathbb{N}^+$ then $m + n \in \mathbb{N}^+$.*

Exercise 2. Prove the above corollary.

Theorem 6 (Cancellation Law). *Suppose $x, y, z \in \mathbb{N}$. Then*

$$x + z = y + z \quad \text{implies} \quad x = y.$$

4. MULTIPLICATION

Multiplication defines a function $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, so it is a binary operation on \mathbb{N} . It can be described as

$$m \cdot n = \underbrace{m + m + \cdots + m + m}_{n \text{ times}}.$$

In the case of $n = 0$ it is given by

$$m \cdot 0 = 0.$$

Theorem 7 (Distributive Law: part 1). *For all $x, y, z \in \mathbb{N}$*

$$(x + y)z = xz + yz.$$

Theorem 8 (Commutative Law). *For all $x, y \in \mathbb{N}$*

$$xy = yx.$$

Corollary 9 (Distributive Law: part 2). *For all $x, y, z \in \mathbb{N}$*

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

Theorem 10 (Associative Law). *For all $x, y, z \in \mathbb{N}$*

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

5. EXPONENTIATION

Exponentiation can be described as

$$m^n = \underbrace{m \cdot m \cdots m \cdot m}_{n \text{ times}}$$

and

$$m^0 = 1.$$

Exercise 3. Is $(m, n) \mapsto m^n$ a commutative binary operation $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$? Is it associative? If you said ‘no’ to either question, back up your answer with a counter-example.

Warning. Although the equation $0^0 = 1$ is valid in our current context, there are some parts of mathematics where 0^0 is regarded as undefined. This is related to the use of limits in calculus where we have to be careful with limits that converge to indeterminate expressions of the form $0/0$, ∞/∞ , $\infty - \infty$, or even 0^0 . Limits of expressions in indeterminate form do not consistently converge to any fixed value. In fact, some limits in indeterminate form diverge, and some converge, and those that converge do not all converge to the same value. The problem with limits with indeterminate form 0^0 is related to the fact that the function $f(x, y) = x^y$ is not continuous at $(0, 0)$. So in calculus and other contexts, 0^0 is often left undefined.

Theorem 11. *If $x, y, n \in \mathbb{N}$ then*

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

Theorem 12. *If $x, m, n \in \mathbb{N}$ then*

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

Theorem 13. *If $n \in \mathbb{N}$ is not 0 then*

$$0^n = 0.$$

Theorem 14. *If $n \in \mathbb{N}$ then*

$$1^n = 1.$$

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

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

6. THE ORDER RELATIONS

We use addition to develop the order relations on \mathbb{N} .

Definition 1. Let $m, n \in \mathbb{N}$. If there is a nonzero $b \in \mathbb{N}$ such that $n = m + b$ then we say that m is *strictly less than* n , and write $m < n$. In symbols:

$$m < n \Leftrightarrow \exists b \in \mathbb{N} ((b \neq 0) \wedge (n = m + b)).$$

When $m < n$ we also say n is *strictly greater than* m and write $n > m$. So by definition $m < n \Leftrightarrow n > m$.

Theorem 16. If $x, y \in \mathbb{N}$ and if $y \neq 0$ then $x + y > x$.

Definition 2. If $m, n \in \mathbb{N}$, then $m \leq n$ means that either $m < n$ or $m = n$. In this case we say that m is *less than or equal to* n . We also say that n is *greater than or equal to* m and write $n \geq m$. So, in symbols,

$$m \leq n \Leftrightarrow n \geq m \Leftrightarrow (m < n) \vee (m = n) \Leftrightarrow (n > m) \vee (m = n).$$

Theorem 17. Suppose $m, n \in \mathbb{N}$. Then

$$m \leq n \Leftrightarrow \exists b \in \mathbb{N} (n = m + b).$$

Corollary 18. The least element of \mathbb{N} is 0. In other words, if $n \in \mathbb{N}$ then $n \geq 0$.

Corollary 19 (transitivity of \leq). Suppose $x, y, z \in \mathbb{N}$. If $x \leq y$ and $y \leq z$ then $x \leq z$.

The relation $<$ is also transitive:

Theorem 20 (transitivity of $<$). Suppose $x, y, z \in \mathbb{N}$. If $x < y$ and $y < z$ then $x < z$.

Corollary 21 (mixed transitivity). Suppose $x, y, z \in \mathbb{N}$.

(i) If $x < y$ and $y \leq z$ then $x < z$.

(ii) If $x \leq y$ and $y < z$ then $x < z$.

Remark 1. Since $<$ and \leq are transitive, it follows easily that $>$ and \geq are transitive as well.

Theorem 22. Suppose $n \in \mathbb{N}$. Then $n \neq 0$ if and only if $n > 0$. Thus

$$\mathbb{N}^+ = \{n \in \mathbb{N} \mid n \neq 0\} = \{n \in \mathbb{N} \mid n > 0\}.$$

Definition 3. The notation $a < b < c$ is short for $(a < b) \wedge (b < c)$. By transitivity, $a < b < c$ also implies $a < c$. A similar notation is adopted for $>$, \leq , and \geq .

Theorem 23. Let $n \in \mathbb{N}$. There are no natural numbers between n and $n + 1$. In other words, there is no $x \in \mathbb{N}$ such that $n < x < n + 1$.

Theorem 24 (Trichotomy). Suppose $m, n \in \mathbb{N}$. Then exactly one of the following can occur: (i) $m < n$, (ii) $m = n$, (iii) $n < m$.

Exercise 4. Suppose $m, n \in \mathbb{N}$. Show that if $m \leq n$ and $n \leq m$ then $m = n$.

7. ORDER LAWS INVOLVING ADDITION AND MULTIPLICATION

Theorem 25. *Suppose that $x, y, z \in \mathbb{N}$. If $x \leq y$ then $xz \leq yz$.*

Theorem 26. *Suppose that $x, y, z \in \mathbb{N}$.*

Then $x < y$ if and only if $x + z < y + z$.

Similarly, $x \leq y$ if and only if $x + z \leq y + z$.

Theorem 27. *Suppose that $x, y, z \in \mathbb{N}$ where $z > 0$. If $x < y$ then $xz < yz$*

Theorem 28. *Suppose that $x, y, z \in \mathbb{N}$ where $z > 0$. If $xz < yz$ then $x < y$*

Exercise 5. Suppose $m_1 < m_2$ and $n_1 < n_2$. Show $m_1 + n_1 < m_2 + n_2$ and $m_1 n_1 < m_2 n_2$. Hint: for the last inequality, it helps to first show that $m_2 > 0$.

Theorem 29 (Cancellation Law for Multiplication). *Suppose $x, y, z \in \mathbb{N}$. If $xz = yz$ and $z \neq 0$ then $x = y$.*

Theorem 30. *Suppose $m, n \in \mathbb{N}$. If $mn = 0$ then $m = 0$ or $n = 0$.*

Exercise 6. Prove that \mathbb{N}^+ is closed under multiplication. Show this as a corollary to the above theorem.

Exercise 7. Show that if $B^n = 0$ then $B = 0$.

8. RECURSION

It is common to define a function $g : \mathbb{N} \rightarrow S$ by recursive equations. These are equations which define $g(n)$ in terms of other values $g(m)$ of the same function g . This seems circular, but it is not since we require that $m < n$.

For example, suppose we want to define a function $g : \mathbb{N} \rightarrow \mathbb{N}$ by the equations

$$g(0) = 1, \quad \text{and} \quad g(n+1) = 2g(n) + 1.$$

These equations force $g(0) = 1$, $g(1) = 2g(0) + 1 = 3$, $g(2) = 2g(1) + 1 = 2 \cdot 3 + 1 = 7$, and so on.

Theorem 31 (Simple Recursion). *Let S be a set. Suppose that $f : S \rightarrow S$ and $a \in S$ are given. Then there is a unique function $g : \mathbb{N} \rightarrow S$ satisfying the equations*

$$g(0) = a, \quad \text{and} \quad g(n+1) = f(g(n)).$$

A famous function defined by recursion is the *Fibonacci function*. This is defined by the recursive equations:

$$F(0) = 0, \quad F(1) = 1, \quad F(n+2) = F(n) + F(n+1).$$

The difference between this and simple recursion is that, in general, a value of F depends not only on the previous value of F , but the previous *two* values of F . Note that the equations force

$$\begin{aligned} F(0) = 0, \quad F(1) = 1, \quad F(2) = 1 + 0 = 1, \quad F(3) = 1 + 1 = 2, \\ F(4) = 1 + 2 = 3, \quad F(5) = 2 + 3 = 5, \quad F(6) = 3 + 5 = 8, \end{aligned}$$

and so on.

We end with a different sort of recursion. The following equations defines the so-called *triangular numbers*:

$$T(0) = 0, \quad T(n + 1) = (n + 1) + T(n).$$

The difference between this and simple recursion is that $T(n + 1)$ is not a function of $T(n)$ alone, but also depends on n . In other words, you need to know both $T(n)$ and n (or $n + 1$) in order to find $T(n + 1)$. Note that the equations force

$$T(0) = 0, \quad T(1) = 1 + 0 = 1, \quad T(2) = 2 + 1 = 3, \quad T(3) = 3 + 6 = 6,$$

and so on.²

Here is a generalization of the triangular number example:

Theorem 32. *Let S be a set, c an element of S , and $g : \mathbb{N} \times S \rightarrow S$ a function. Then there is a unique function $f : \mathbb{N} \rightarrow S$ satisfying the equations*

$$f(0) = c, \quad f(n + 1) = g(n, f(n)).$$

for all $n \in \mathbb{N}$.

Example. To define the factorial function $f(n) = n!$, take $S = \mathbb{N}$, $c = 1$, and $g(n, m) = (n + 1) \cdot m$.

²It turns out that $T(n) = n(n + 1)/2$, so we do not need to define T recursively. However, the recursive definition captures the idea of a triangle better than the formula $T(n) = n(n + 1)/2$.