Abstract Algebra 1 (MATH 3140)

Background on the Natural Numbers and Induction

Recall the

Infinity Axiom: There exists an *inductive set*; that is, a set S (of sets) such that $\emptyset \in S$ and for every member X of S, we have that $X' := X \cup \{X\}$ (a set!) is also a member of S.

The set X' is called the *successor of* X.

This axiom allows us to define the natural numbers, define the usual order $<$ and the arithmetic operations (addition, multiplication, exponentiation) on the set of natural numbers, and prove their basic properties.

Notice, however, that the axiom itself does not say anything about infinity; in fact, it can't, since we have not defined yet what 'infinite' means for sets. The name of the axiom is motivated by the following facts:

- The axiom asserts the existence of an inductive set S, and if we follow the definition, we see that S must have the following elements:

$$(\dagger) \qquad \emptyset,\ \emptyset' = \{\emptyset\},\ (\emptyset')' = \{\emptyset, \{\emptyset\}\},\ ((\emptyset')')' = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \ldots\ .$$

  Our intuitive notion of 'infinite' suggests that S has infinitely many elements.
- After we define the natural numbers and define rigorously what it means that a set is infinite, we will be able to prove that inductive sets are indeed infinite.

1. NATURAL NUMBERS

By the Infinity Axiom and the Subset Axioms, the intersection of all inductive sets is a set, which is easily shown to be inductive. This intersection is therefore the least inductive set (i.e., it is an inductive set, which is a subset of every inductive set). The elements are the sets listed in ($\dagger$).

Definition 1.1. The least inductive set is called *the set of natural numbers*, which we will denote[1] by $\mathbb{N}$. The members of $\mathbb{N}$ are called *natural numbers*. The sets listed in ($\dagger$) are the natural numbers that we call *zero*, *one*, *two*, *three*, and denote by $0, 1, 2, 3$.

This definition of $\mathbb{N}$ immediately implies that if S is an inductive subset of $\mathbb{N}$, then it must be the case that $S = \mathbb{N}$. We restate this fact in the Induction Theorem below. This theorem justifies proof by induction (on $n \in \mathbb{N}$) and the definition of functions on $\mathbb{N}$ by recursion.

Induction Theorem 1.2. *If S is a set of natural numbers such that*

(i) $0 \in S$, *and*

(ii) *for every $n \in S$ we have $n' \in S$,*

then $S = \mathbb{N}$.

[1] In set theory the usual notation is ω.

Notice also that using our notation $0, 1, 2, 3, \ldots$, we can rewrite the definitions

$$0 := \emptyset,\ 1 := \emptyset' = \{\emptyset\},\ 2 := (\emptyset')' = \{\emptyset, \{\emptyset\}\},\ 3 := ((\emptyset')')' = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \ldots$$

of $0, 1, 2, 3, \ldots$ (see Def. 1.1) as follows:

$$0 = \{\} = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \quad \ldots \quad .$$

This suggests that the way we defined the natural numbers may imply that every natural number is the set of all 'smaller' natural numbers, or more precisely: every natural number has only natural numbers as its elements, and $\in$ (membership) captures the idea of 'smaller' for natural numbers. The next theorem and corollary show that this is indeed the case.

Theorem 1.3.

(1) *If $n \in \mathbb{N}$ and $a \in n$ then $a \in \mathbb{N}$.*
(2) *If $k, m, n \in \mathbb{N}$ satisfy $k \in m \in n$ then $k \in n$.*
(3) *Exactly one of the following conditions holds for any $m, n \in \mathbb{N}$:*

$$m \in n, \quad m = n, \quad n \in m.$$

All statements in Theorem 1.3 can be proved by induction on n.[2] For (3), prove and use:

$(*)$ $\quad \mathbb{N} = \{0\} \cup \{n' : n \in \mathbb{N}\}$, $\qquad$ and $\qquad$ $(**)$ $\quad m \in n$ implies $m' \in n'$ for all $m, n \in \mathbb{N}$.

Now we define the (usual) ordering of the natural numbers.

Definition 1.4. Define the relations $<$ and $\leq$ on $\mathbb{N}$ as follows:

$$< := \{(m,n) \in \mathbb{N} \times \mathbb{N} : m \in n\} \quad \text{and} \quad \leq := \{(m,n) \in \mathbb{N} \times \mathbb{N} : m \in n \text{ or } m = n\};$$

i.e., $m < n$ iff $m \in n$, and $m \leq n$ iff $m \in n$ or $m = n$ (iff $m < n$ or $m = n$) for any $m, n \in \mathbb{N}$.

Theorem 1.3, combined with Definiton 1.4 immediately implies

Corollary 1.5.

(1) *$\leq$ is a linear order on $\mathbb{N}$ with least element 0.*
(2) *For every natural number n we have that $n = \{k \in \mathbb{N} : k < n\}$.*

These considerations show that induction and the (usual) ordering of the natural numbers are more primitive notions than arithmetic.

2. STRONG INDUCTION AND WELL-ORDERING

Before discussing arithmetic, we now state the Strong Induction Theorem and the Well-Ordering Theorem. These theorems are equivalent to the Induction Theorem above, but the way they are usually stated relies on the ordering of the natural numbers.

Strong Induction Theorem 2.1. *If T is a set of natural numbers such that*

- *for every natural number n, if $k \in T$ holds for all $k < n$, then $n \in T$,*

then $T = \mathbb{N}$.

Definition 2.2. Let $\leq$ be a linear order on a set A. We say that $\leq$ is a *well-order on A* if every nonempty subset B of A has a least element; that is, for every nonempty $B \subseteq A$ there exists $b_0 \in B$ such that $b_0 \leq b$ for all $b \in B$.

Well-Ordering Theorem 2.3. *The linear order $\leq$ on $\mathbb{N}$ (see Cor. 1.5) is a well-order.*

3. ARITHMETIC

To introduce the usual arithmetic on the natural numbers, notice that the (binary) operations $+, \cdot, \downarrow$ (addition, multiplication, exponentiation) on $\mathbb{N}$, which we want to define, are functions $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, namely: $(m,n) \overset{+}{\mapsto} m+n$, $(m,n) \overset{\cdot}{\mapsto} mn$, and $(m,n) \overset{\downarrow}{\mapsto} m^n$.

Definition 3.1. For each fixed $m \in \mathbb{N}$, we define $m+n$, $m \cdot n$ (or simply mn), and m^n for all $n \in \mathbb{N}$ by recursion on n as follows:

$$\begin{array}{ccc} m+0 := m, & m \cdot 0 := 0, & m^0 := 1, \\ m+n' := (m+n)'; & m \cdot n' := m \cdot n + m; & m^{n'} := m^n \cdot m. \end{array}$$

By $(*)$, Definition 3.1 indeed defines $m+n$, $m \cdot n$, and m^n for all $m, n \in \mathbb{N}$. Now the basic rules of arithmetic, listed in Theorem 1.10 below, can be proved (in the given order) by induction[2], using the definitions and previously proved properties.

Theorem 3.2. *For arbitrary natural numbers k, m, and n,*

(1) $m' = m+1$, $m \cdot 1 = 0 + m = m$, *and* $m^1 = 1 \cdot m = m$, *where* $1 := 0'$*;*
(2) $k + (m+n) = (k+m)+n$ *(associative law for addition);*
(3) $m+n = n+m$ *(commutative law for addition);*
(4) $k(m+n) = km + kn$ *(distributive law);*
(5) $k(mn) = (km)n$ *(associative law for multiplication);*
(6) $mn = nm$ *(commutative law for multiplication);*
(7) $m < n$ *if and only if* $m+k < n+k$ *(monotonicity of addition);*
(8) *if* $k \neq 0$*, then* $m < n$ *if and only if* $mk < nk$ *(monotonicity of multiplication);*
(9) $m+k = n+k$ *implies* $m = n$ *(cancellation law for addition);*
(10) *if* $k \neq 0$*, then* $mk = nk$ *implies* $m = n$ *(cancellation law for multiplication);*
(11) $m < n$ *if and only if* $n = m + k'$ *for some* $k \in \mathbb{N}$*;*
(12) *if* $m \neq 0$*, then there exist (uniquely determined)* $q, r \in \mathbb{N}$ *such that* $n = mq + r$ *and* $r < m$ *(division algorithm).*

Applying (12) repeatedly with $q = 9'$ we get that every natural number can be written uniquely in base ten, therefore we need notation only for the first ten natural numbers:

$$0, \;\; 1 = 0', \;\; 2 = 1', \;\; \ldots, \;\; 9 = 8'.$$

[2]Occasionally, there is an induction inside the induction.