PRINCIPLES OF ANALYSIS
LECTURE 3

PAUL L. BAILEY

1. Set Proof Example

The following properties are sometimes useful in proofs:

- $A = A \cup A = A \cap A$
- $\varnothing \cap A = \varnothing$
- $\varnothing \cup A = A$
- $A \subset B \Leftrightarrow A \cap B = A$
- $A \subset B \Leftrightarrow A \cup B = B$

As an example, we prove one of these properties.

Proposition 1. *Let A and B be a sets. Then $A \subset B \Leftrightarrow A \cap B = A$.*

Proof. To prove an if and only if statement, we prove implication in both directions.

($\Rightarrow$) Assume that $A \subset B$. We wish to show that $A \cap B = A$. To show that two sets are equal, we show that each is contained in the other.

($\subset$) To show that $A \cap B \subset A$, it suffices to show that every element of $A \cap B$ is in A. Thus we select an arbitrary element $c \in A \cap B$ and show that it is in A. Now by definition of intersection, $c \in A \cap B$ means that $c \in A$ and $c \in B$. Thus $c \in A$. Since c was arbitrary, every element of $A \cap B$ is contained in A. Thus $A \cap B \subset A$.

($\supset$) Let $a \in A$. We wish to show that $a \in A \cap B$. Since $A \subset B$, then every element of A is an element of B. Thus $a \in B$. So $a \in A$ and $a \in B$. By definition of intersection, $a \in A \cap B$. Thus $A \subset A \cap B$.

Since $A \cap B \subset A$ and $A \subset A \cap B$, we have $A \cap B = A$.

($\Leftarrow$) Assume that $A \cap B = A$. We wish to show that $A \subset B$. Let $a \in A$. It suffices to show that $a \in B$. Since $A \cap B = A$, then $a \in A \cap B$. Thus $a \in A$ and $a \in B$. In particular, $a \in B$. □

Now let us prove the analogous statement in compressed form.

Proposition 2. *Let A and B be a sets. Then $A \subset B \Leftrightarrow A \cup B = B$.*

Proof.

($\Rightarrow$) Assume that $A \subset B$. Clearly $B \subset A \cup B$, so we show that $A \cup B \subset B$. Let $c \in A \cup B$. Then $c \in A$ or $c \in B$. If $c \in B$ we are done, so assume that $c \in A$. Since $A \subset B$, then $c \in B$ by definition of subset. Thus $A \cup B \subset B$.

($\Leftarrow$) Assume that $A \cup B = B$ and let $a \in A$. Thus $a \in A \cup B$, so $a \in B$. Thus $A \subset B$. □

Date: August 27, 2003.

2. Natural Numbers

Define the natural numbers.

- $0 = \varnothing$;
- $1 = \{\varnothing\}$;
- $2 = \{\varnothing, \{\varnothing\}\}$;
- $3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$;

and so forth. We could have written this as

- $0 = \varnothing$;
- $1 = \{0\}$;
- $2 = \{0, 1\}$;
- $3 = \{0, 1, 2\}$;

and so forth. A given natural number is the set containing all of the previous natural numbers. Restate as follows.

We define 0 to be the empty set. If x is a set, the *successor* of x is denoted x^+ and is defined as

$$x^+ = x \cup \{x\}.$$

The *natural numbers* are the set $\mathbb{N}$ defined by following properties:

(1) $0 \in \mathbb{N}$;
(2) if $n \in \mathbb{N}$, then $n^+ \in \mathbb{N}$;
(3) if $S \subset \mathbb{N}$, $0 \in S$, and $n \in S \Rightarrow n^+ \in S$, then $S = \mathbb{N}$.

For $m, n \in \mathbb{N}$, we say the m is less than or equal to n if $m \subset n$:

$$m \leq n \Leftrightarrow m \subset n.$$

3. Induction

Note that the third property of natural numbers asserts that only successors of 0 are in $\mathbb{N}$; that is, this property asserts that $\mathbb{N}$ is a minimal set of successors of 0, and that $\mathbb{N}$ is the unique set satisfying (1) through (3). This property is known as the *Principal of Mathematical Induction.*

Suppose that for every natural number n, we have a proposition $p(n)$ which is either true or false. Let

$$S = \{n \in \mathbb{N} \mid p(n) \text{ is true}\}.$$

Now if $p(0)$ is true, and if the truth of $p(n)$ implies the truth of $p(n^+)$, then the set S contains 0 and it contains the successor of every element in it. Thus, in this case, $S = \mathbb{N}$, which means that $p(n)$ is true for all $n \in \mathbb{N}$. We state this as

Theorem 1. Induction Theorem
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$. If

(1) $p(0)$ *is true;*
(2) *If $p(n)$ is true, then $p(n^+)$ is true;*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Example 1. Show that $\sum_{i=1}^{n} = \frac{(n-1)n}{2}$ for all $n \in \mathbb{N}$.

Example 2. Show that $7 \mid (11^n - 4^n)$ for all $n \in \mathbb{N}$.

Proof. For $n = 1$, we have $7 = 11 - 4$, so clearly $7 \mid 11^1 - 4^1$. Thus assume that $7 \mid 11^{n-1} - 4^{n-1}$, so there exists $x \in \mathbb{Z}$ such that $7x = (11^{n-1} - 4^{n-1})$. Now

$$\begin{aligned} 11^n - 4^n &= 11^n - 11 \cdot 4^{n-1} + 11 \cdot 4^{n-1} - 4 \cdot 4^{n-1} \\ &= (11^{n-1} - 4^{n-1})11 + (11 - 4)4^{n-1} \\ &= 7x \cdot 11 + 7 \cdot 4^{n-1} \\ &= 7(11x + 4^{n-1}. \end{aligned}$$

Thus $7 \mid (11^n - 4^n)$. □

Now the induction theorem can be made stronger by weakening the hypothesis. The resulting theorem gives a proof technique which is known as strong induction.

Theorem 2. Strong Induction Theorem
Let $p(n)$ be a proposition for each $n \in \mathbb{N}$. If

(1) $p(0)$ *is true;*
(2) *If $p(m)$ is true for all $m \leq n$, then $p(n+1)$ is true;*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $t(n)$ be the statement that "p(m) is true for all $m \leq n$".

Our first assumption is that $p(0)$ is true, and since the only natural number less than or equal to 0 is zero (because the only subset of the empty set is itself), this means that $t(0)$ is true.

Our second assumption is that if $t(n)$ is true, then $p(n+1)$ is true. Thus assume that $t(n)$ is true so that $p(n+1)$ is also true. Then $p(i)$ is true for all $i \leq n+1$. Thus $t(n+1)$ is true.

By our original Induction Theorem, we conclude that $t(n)$ is true for all $n \in \mathbb{N}$. This implies that $p(n)$ is true for all $n \in \mathbb{N}$. □

4. Recursion

We now state the Recursion Theorem, which will allows us to define addition and multiplication of natural numbers.

Theorem 3. Recursion Theorem
Let X be a set, $f : X \to X$, and $a \in X$. Then there exists a unique function $\phi : \mathbb{N} \to X$ such that $\phi(0) = a$ and $\phi(n^+) = f(\phi(n))$ for all $n \in \mathbb{N}$.

Reason. May be proved by induction. □

Let $f : \mathbb{N} \to \mathbb{N}$ be given by $f(n) = n^+$. Let $\sigma_m : \mathbb{N} \to \mathbb{N}$ be the unique function, whose existence is guaranteed by the Recursion Theorem, defined by $\sigma_m(0) = m$ and $\sigma_m(n^+) = f(\sigma_m(n)) = (\sigma_m(n))^+$. Then $\sigma_m(n)$ is defined to be the *sum* of m and n:

$$m + n = \sigma_m(n).$$

Let $f : \mathbb{N} \to \mathbb{N}$ be given by $f = \sigma_m$. Let $\mu_m : \mathbb{N} \to \mathbb{N}$ be the unique function, whose existence is guaranteed by the Recursion Theorem, defined by $\mu_m(0) = 0$ and $\mu_m(n^+) = f(\mu_m(n)) = \sigma_m(\mu_m(n)) = m + \mu_m(n)$. Then $\mu_m(n)$ is defined to be the *product* of m and n:

$$mn = \mu_m(n).$$

The following properties of natural numbers can be proved using the above definitions:

- $m + n = n + m$ (commutativity of addition);
- $(m + n) + o = m + (n + o)$ (associativity of addition);
- $mn = nm$ (commutativity of multiplication);
- $(mn)o = m(no)$ (associativity of multiplication);
- $m(n + o) = mn + mo$ (distributivity of multiplication over addition);
- $m + 0 = m$ (0 is an additive identity);
- $1m = m$ (1 is a multiplicative identity);
- $0m = 0$.

We state two additional properties, which we will use to show that multiplication of integers is well-defined.

Proposition 3. Cancellation Law of Addition
Let $a, b, c \in \mathbb{N}$ and suppose that $a + c = b + c$. Then $a = b$.

Proposition 4. Cancellation Law of Multiplication
Let $a, b, c \in \mathbb{N}$ and suppose that $ac = bc$. Then $a = b$.

5. Integers

Develop the integers from the natural numbers as follows.

Let $A = \mathbb{N} \times \mathbb{N}$. We wish to think of the elements (a, b) of A as differences $a - b$.

Define a relation $\sim$ on A by

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Prove that this is an equivalence relation. Let $[a, b]$ denote the equivalence class of (a, b).

Set $\mathbb{Z} = \{[a, b] \mid a, b \in \mathbb{N}\}$.

Define addition and multiplication on $\mathbb{Z}$ as follows:

- $[a, b] + [c, d] = [a + c, b + d]$;
- $[a, b] \cdot [c, d] = [ac + bd, ad + bc]$.

Prove that these binary operations are well-defined and satisfy the desired properties of the integers. The additive identity is $[0, 0]$ and the additive inverse of $[a, b]$ is $[b, a]$. The multiplicative identity is $[1, 0]$.

Define a relation $\leq$ on $\mathbb{Z}$ by

$$[a, b] \leq [c, d] \Leftrightarrow a + d \leq b + c.$$

Prove that this is a linear order relation on $\mathbb{Z}$, and that it relates to addition and multiplication in the desired way.

6. Rationals

Develop the rationals from the integers as follows.

Let $A = \mathbb{Z} \times \mathbb{Z} \smallsetminus \{0\}$. We wish to think of the elements (a, b) of A as fractions $\frac{a}{b}$.

Define a relation $\sim$ on A by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Prove that this is an equivalence relation. Let $[a, b]$ denote the equivalence class of (a, b).

Set $\mathbb{Q} = \{[a, b] \mid a, b \in \mathbb{Z} \text{ with } b \neq 0\}$.

Define addition and multiplication on $\mathbb{Q}$ as follows:

- $[a, b] + [c, d] = [ad + bc, bd]$;
- $[a, b] \cdot [c, d] = [ac, bd]$.

Prove that these binary operations are well-defined and satisfy the desired properties of the integers. The additive identity is $[0, 1]$ and the additive inverse of $[a, b]$ is $[-a, b]$. The multiplicative identity/is $[1, 1]$ and the multiplicative inverse of $[a, b]$ is $[b, a]$. Denote $[0, 1]$ by 0 and $[1, 1]$ by 1. For $x = [a, b]$, denote $[-a, b]$ by $-x$ and $[b, a]$ by x^{-1}.

Define a relation $\leq$ on $\mathbb{Q}$ by

$$[a, b] \leq [c, d] \Leftrightarrow (ad - bc)bd \leq 0.$$

Prove that this is a linear order relation on $\mathbb{Q}$, and that it relates to addition and multiplication in the desired way.

The set $\mathbb{Q}$ satisfies the following properties:

(F1) $(x + y) + z = x + (y + z)$;
(F2) $x + 0 = x$;
(F3) $x + (-x) = 0$;
(F4) $xy = yx$;
(F5) $(xy)z = x(yz)$;
(F6) $x \cdot 1 = x$;
(F7) $x \cdot x^{-1} = 1$;
(F8) $xy = yx$;
(F9) $x(y + z) = xy + xz$;
(O1) $x \leq x$;
(O2) $x \leq y$ and $y \leq x$ implies $x = y$;
(O3) $x \leq y$ and $y \leq z$ implies $x \leq z$;
(O4) $x \leq y$ or $y \leq x$.

Properties **(F1)** through **(F2)** say that $\mathbb{Q}$ is a *field*, and properties **(O1)** through **(O4)** say that $\mathbb{Q}$ is a *linearly ordered set.*

Department of Mathematics and CSCI, Southern Arkansas University
E-mail address: `plbailey@saumag.edu`