Foundations Of Mathematics

John A. Hildebrant

Department of Mathematics
Louisiana State University
Baton Rouge, Louisiana 70803
Contents

1 Sets and Relations ............................................. 1
2 The Peano Axioms .............................................. 3
3 Order Relations .................................................. 5
4 The Axiom Of Choice .......................................... 6
5 Finite and Infinite Sets ....................................... 7
6 Well-Ordered Sets .............................................. 8
7 Quotient Sets and the Integers ............................ 9
8 The Real Numbers .............................................. 11
9 Ordinal Numbers .............................................. 15
10 Cardinal Numbers ............................................ 16
Typesetter’s Note: Theorems and problems that are denoted by a number preceded by the letter A refer to material from the author’s analysis sequence.

1 Sets and Relations

The word set is assumed to be a primitive dictionary word. One synonym for this word is collection. We hypothesize the existence of a set \( \emptyset \) which contains no members, called the empty set.

The statement that \( x \) is an element of a set \( A \) (or \( x \) is a member of \( A \); or \( x \) belongs to \( A \)) is written \( x \in A \).

To designate that \( B \) is the set of all elements satisfying property \( p \), we write:
\[
B = \{ x : x \text{ has property } p \}.
\]

To state that a set \( A \) is a subset of a set \( B \) (meaning that each member of \( A \) is also a member of \( B \)), we write \( A \subseteq B \).

The statement \( A = B \) means \( A \subseteq B \) and \( B \subseteq A \).

If \( A \subseteq B \) and \( A \neq B \), then we write \( A \subset B \) and say that \( A \) is a proper subset of \( B \).

If \( A \) and \( B \) are sets, we define the union of \( A \) and \( B \):
\[
A \cup B = \{ x : x \in A \text{ or } x \in B \}
\]

and define the intersection of \( A \) and \( B \):
\[
A \cap B = \{ x : x \in A \text{ and } x \in B \}
\]

If \( A \) and \( B \) have no elements in common, then we say that \( A \) and \( B \) are disjoint, and write \( A \cap B = \emptyset \).

If \( A \subseteq B \), then the complement of \( A \) in \( B \) is:
\[
B \setminus A = \{ x : x \in B \text{ and } x \notin A \}
\]

1. DeMorgan’s Laws: If \( A \) and \( B \) are subsets of a set \( X \), then
   \[
   (1) \quad X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B); \quad \text{and}
   \]
   \[
   (2) \quad X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).
   \]

2. Theorem: Let \( A \) and \( B \) be subsets of a set \( X \). These are equivalent:
   \[
   (1) \quad A \subseteq B;
   (2) \quad A \cap B = A;
   (3) \quad A \cup B = B;
   (4) \quad X \setminus B \subseteq X \setminus A;
   (5) \quad A \cap (X \setminus B) = \emptyset; \quad \text{and}
   (6) \quad B \cup (X \setminus A) = X.
   \]
If $A$ and $B$ are sets, then the **product set** $A \times B$ consists of all ordered pairs $(a, b)$ such that $a \in A$ and $b \in B$, i.e.

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

A **relation** on a set $A$ is a subset of $A \times A$.

The **diagonal relation** on a set $A$ is defined:

$$\Delta_A = \{(a, a) : a \in A\}$$

If $R$ is a relation on a set $A$, then the **converse** of $R$ is defined:

$$R^{-1} = \{(y, x) : (x, y) \in R\}$$

If $R$ and $Q$ are relations on a set $A$, then the **composition** of $R$ and $Q$ is defined:

$$R \circ Q = \{(x, y) \in A \times A : \text{exists } z \in A \text{ such that } (x, z) \in R \text{ and } (z, y) \in Q\}$$

Let $A$ be a set, and let $R$ be a relation on $A$. We say that:

- $R$ is **reflexive** if $(a, a) \in R$ for each $a \in A$;
- $R$ is **symmetric** if whenever $(a, b) \in R$, then $(b, a) \in R$, for $a, b \in A$;
- $R$ is **antisymmetric** if whenever both $(a, b) \in R$ and $(b, a) \in R$, then $a = b$, for $a, b \in A$; and
- $R$ is **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for $a, b, c \in A$.

3. **Theorem:** Let $A$ be a set, and $R$ a relation on $A$. Then

   (1) $R$ is reflexive if and only if $\Delta_A \subseteq R$;
   (2) $R$ is symmetric if and only if $R = R^{-1}$;
   (3) $R$ is antisymmetric if and only if $R \cap R^{-1} \subseteq \Delta_A$; and
   (4) $R$ is transitive if and only if $R \circ R \subseteq R$.

If $\mathcal{A}$ is a collection of sets, then the **union** of $\mathcal{A}$ is defined $\bigcup\{A : A \in \mathcal{A}\} = \{x : x \in A \text{ for some } A \in \mathcal{A}\}$, and the **intersection** of $\mathcal{A}$ is defined $\bigcap\{A : A \in \mathcal{A}\} = \{x : x \in A \text{ for all } A \in \mathcal{A}\}$.

A collection of sets $\mathcal{A}$ is said to be **indexed** by $A$ provided that for each $\alpha \in A$, there is exactly one $X_\alpha \in \mathcal{A}$ such that $\mathcal{A} = \{X_\alpha : \alpha \in A\}$. The union is denoted $\bigcup_{\alpha \in A} X_\alpha$, and the intersection is denoted $\bigcap_{\alpha \in A} X_\alpha$.

As we will see (using the Axiom of Choice), each collection of sets is an indexed collection.

4. **DeMorgan’s Laws:** Let $\{X_\alpha : \alpha \in A\}$ be a collection of subsets of a set $X$. Then

(1) \( X \setminus \bigcup_{\alpha \in A} X_{\alpha} = \bigcap_{\alpha \in A} (X \setminus X_{\alpha}) \); and
(2) \( X \setminus \bigcap_{\alpha \in A} X_{\alpha} = \bigcup_{\alpha \in A} (X \setminus X_{\alpha}) \).

A partition of a set \( X \) is a collection \( A \) of subsets of \( X \) such that \( X = \bigcup \{ A : A \in \mathcal{A} \} \), and if \( A \) and \( B \) are distinct members of \( \mathcal{A} \), then \( A \cap B = \emptyset \).

A relation \( R \) on a set \( X \) is called an equivalence relation provided \( R \) is reflexive, symmetric, and transitive. The \( R \)-classes of \( X \) are called equivalence classes.

5. Theorem: The classes of an equivalence relation on a set \( X \) form a partition of \( X \). Moreover, the elements of a partition of a set \( X \) form the equivalence classes of a unique equivalence relation on \( X \).

Let \( \mathbb{N} = \{1, 2, 3, \ldots \} \) denote the set of all natural numbers.

2 The Peano Axioms

For each \( x \in \mathbb{N} \), there is a unique element \( x' \in \mathbb{N} \) (called the successor of \( x \)), such that:

(a) If \( x' = y' \), then \( x = y \);
(b) There is an element of \( \mathbb{N} \), which is denoted by 1, such that for each \( x \in \mathbb{N} \), \( x' \neq 1 \); and
(c) If \( M \) is a set which contains 1 and which contains \( x' \) whenever it contains \( x \), then \( M \) contains every element of \( \mathbb{N} \).

Axiom (c) is called The Axiom of Finite Induction.

6. Theorem: If \( x \in \mathbb{N} \) and \( x \neq 1 \), then there exists a unique \( y \in \mathbb{N} \) such that \( x = y' \).

A function is a triple \((A, B, f)\), where \( A \) and \( B \) are sets, and \( f \) is a rule which assigns to each element \( x \) of \( A \) a unique element \( f(x) \) of \( B \). The notation \( f : A \to B \) is frequently used to denote a function \((A, B, f)\), and if the sets \( A \) and \( B \) are understood, then \( f \) is used to denote the function.

The set \( A \) is called the domain of the function, and \( B \) is called the codomain of the function. For \( x \in A \), we call \( f(x) \) the image or value of \( x \) under the function \( f \). The set of all images of elements of \( A \) is a subset of \( B \) called the range of \( f \).

If \( x \neq y \) in \( A \) implies that \( f(x) \neq f(y) \), then \( f \) is called a one-to-one function. If the codomain \( B \) is also the range of \( f \), then \( f \) is said to be an onto function.

A function which is both one-to-one and onto is called a bijection of \( A \) onto \( B \).
The function $1_A : A \to A$ defined by $1_A(x) = x$ for each $x \in A$, is called the identity function on $A$.
If $f : A \to B$ and $g : B \to C$ are functions, then the composition $g \circ f : A \to C$ is defined by $g \circ f(x) = g(f(x))$ for each $x \in A$.

7. **Theorem:** Let $f : A \to B$ be a bijection. Then there is a unique function $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

The function $g$ in A1.8 is called the inverse of $f$, and is denoted $f^{-1}$. Notice that it is a bijection from $B$ to $A$.
If $f : A \to B$ is a function and $P \subseteq A$, then $f[P] = \{f(x) : x \in P\}$, and for $Q \subseteq B$, then $f^{-1}[Q] = \{x \in A : f(x) \in Q\}$.

8. **Theorem:** Let $f : X \to Y$ be a function, and let $A$ and $B$ be subsets of $X$. Then:

(1) $f[A \cup B] = f[A] \cup f[B]$;
(2) $f[A \cap B] \subseteq f[A] \cap f[B]$;
(3) $f[A \setminus f[B]] \subseteq f[A \setminus B]$; and
(4) if $A \subseteq B$, then $f[A] \subseteq f[B]$.

9. **Theorem:** Let $f : X \to Y$ be a function, and let $A$ and $B$ be subsets of $Y$. Then:

(1) $f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$;
(2) $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$;
(3) $f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B]$; and
(4) if $A \subseteq B$, then $f^{-1}[A] \subseteq f^{-1}[B]$.

10. **Theorem:** Let $f : X \to Y$ be a function, and let $\{X_\alpha : \alpha \in A\}$ be a collection of subsets of $X$. Then

(1) $f[\bigcup_{\alpha \in A} X_\alpha] = \bigcup_{\alpha \in A} f[X_\alpha]$; and
(2) $f[\bigcap_{\alpha \in A} X_\alpha] \subseteq \bigcap_{\alpha \in A} f[X_\alpha]$.

11. **Theorem:** Let $f : X \to Y$ be a function, and let $\{Y_\beta : \beta \in B\}$ be a collection of subsets of $Y$. Then:

(1) $f^{-1}[\bigcup_{\beta \in B} Y_\beta] = \bigcup_{\beta \in B} f^{-1}[Y_\beta]$; and
(2) $f^{-1}[\bigcap_{\beta \in B} Y_\beta] = \bigcap_{\beta \in B} f^{-1}[Y_\beta]$.

12. **Theorem:** Let $f : X \to Y$ be a function, and let $B \subseteq Y$. Then $f^{-1}[Y \setminus B] = X \setminus f^{-1}[B]$.
13. **Theorem:** There is a unique function \( \theta : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) such that:

(i) \( \theta(x, 1) = x' \) for each \( x \in \mathbb{N} \); and

(ii) \( \theta(x, y') = \theta(x, y)' \) for each \( x, y \in \mathbb{N} \).

The function \( \theta \) in A1.15 is called *addition* on \( \mathbb{N} \). For \( a, b \in \mathbb{N} \), we write \( a + b = \theta(a, b) \).

14. **Theorem:** If \( a, b, c \in \mathbb{N} \), then:

(1) \( (a + b) + c = a + (b + c) \) (associative); and

(2) \( a + b = b + a \) (commutative).

15. **Theorem:** If \( a, b, c \in \mathbb{N} \) such that \( a + c = b + c \), then \( a = b \) (cancellation).

3 **Order Relations**

A relation \( \leq \) on a set \( X \) is called a *quasi-order* (we write \( x \leq y \) in place of \( (x, y) \in \leq \)), provided it is reflexive and transitive. If \( \leq \) is a quasi-order on a set \( X \), then \((X, \leq)\) is called a *quasi-ordered set*.

A quasi-order on a set \( X \) is called a *partial order*, provided it is antisymmetric. In this case, \((X, \leq)\) is called a *partially ordered set*.

A partial order \( \leq \) on a set \( X \) is called a *total order*, provided that for \( x, y \in X \), either \( x \leq y \) or \( y \leq x \). In this case, \((X, \leq)\) is called a *totally ordered set*.

If \((X, \leq)\) is a quasi-ordered set, an element \( m \in X \) is called a *maximal element* of \( X \), provided \( m \leq x \) for \( x \in X \) implies \( m = x \).

If \((X, \leq)\) is a quasi-ordered set and \( A \subseteq X \), then \( u \in X \) is called an *upper bound* for \( A \), provided \( a \leq u \) for all \( a \in A \).

If \((X, \leq)\) is a quasi-ordered set and \( C \subseteq X \), then \( C \) is called a *chain* in \( X \), provided \((C \times C) \cap \leq \) is a total order on \( C \).

A chain \( C \) in a quasi-ordered set \((X, \leq)\) is called a *maximal chain*, provided \( C \) is not properly contained in another chain in \( X \); i.e., \( C \) is maximal with respect to \( \subseteq \) in the family of chains in \( X \).

If \((X, \leq)\) is a quasi-ordered set and \( A \subseteq X \), an element \( a \in A \) is called a *first element* of \( A \), provided \( a \leq x \) for all \( x \in A \).

A quasi-order on a set \( X \) is called a *well-order*, provided that each non-empty subset of \( X \) has a unique first element. In this case, \((X, \leq)\) is called a *well-ordered set*.

16. **Theorem:** Each well-ordered set is totally ordered.

Define \( \leq \) on \( \mathbb{N} \) by \( a \leq b \) provided there exists \( c \in \mathbb{N} \) such that \( b = a + c \) or \( b = a \).

17. **Theorem:** The set \((\mathbb{N}, \leq)\) is a well-ordered set.
18. **Recursion Theorem**: Let $A$ be a collection, $e \in A$, and suppose that for each $n \in \mathbb{N}$, there exists $R_n : A \rightarrow A$. Then there exists $F : \mathbb{N} \rightarrow A$ such that $F(1) = e$ and $F(n + 1) = R_{n+1}[F(n)]$ for each $n \in \mathbb{N}$.

19. **Example**: Let $X$ be a set, and let $f : X \rightarrow X$ be a function. We will use the Recursion Theorem to establish the existence of the $n$-fold composition of $f$ with itself.

Let $A$ be the collection of all functions from $X$ into $X$, and define $R_n : A \rightarrow A$ by $R_n(g) = f \circ g$ for each $n \in \mathbb{N}$. Then, by the Recursion Theorem, there exists $F : \mathbb{N} \rightarrow A$ such that $F(1) = f$ and $F(n + 1) = R_{n+1}[F(n)] = f \circ F(n)$ for each $n \in \mathbb{N}$. Define $f^{(n)} = F(n)$ for each $n \in \mathbb{N}$.

4 **The Axiom Of Choice**

The **Axiom of Choice** states: If $A$ is a collection of non-empty sets, then there exists a function

$$\phi : A \rightarrow \bigcup\{A : A \in \mathbb{A}\}$$

such that $\phi(A) \in A$ for each $A \in \mathbb{A}$. The function $\phi$ is called a choice function for the collection $\mathbb{A}$.

The **Cartesian product** of a collection $\mathbb{A}$ of sets is the collection of all choice functions for $\mathbb{A}$. It is denoted $\prod\{A : A \in \mathbb{A}\}$. For each $\phi$ in this product and each $A \in \mathbb{A}$, the value $\phi(A)$ is called the $A$ coordinate of $\phi$. For each $B \in \mathbb{A}$, the function $\pi_B : \prod\{A : A \in \mathbb{A}\} \rightarrow B$ defined by $\pi_B(\phi) = \phi(B)$ is called the $B$ projection.

If $(X, \leq)$ is a partially ordered set and $A \subseteq X$, then an element $b \in X$ is called a least upper bound for $A$, provided $b$ is an upper bound for $A$ and $b \leq u$ for each upper bound $u$ of $A$. Note that if a least upper bound exists for a subset of a partially ordered set, then it is unique.

If $(X, \leq)$ is a non-empty partially ordered set such that each totally ordered subset of $X$ has a least upper bound $b \in X$, and if $f : X \rightarrow X$ is a function such that $x \leq f(x)$ for all $x \in X$, then a subset $A$ of $X$ is said to be admissible (with respect to $b$), provided:

(a) $b \in A$;
(b) $f[A] \subseteq A$; and
(c) every least upper bound of a totally ordered subset of $A$ belongs to $A$.

20. **Lemma**: Let $(X, \leq)$ be a non-empty partially ordered set such that each totally ordered subset of $X$ has a least upper bound, let $f : X \rightarrow X$ be a function such that $x \leq f(x)$ for each $x \in X$, and let $A$ be the family of all admissible subsets of $X$ (with respect to $b$). Then:

(a) $A \neq \emptyset$;
(b) \((A, \subseteq)\) is a partially ordered set with \(M = \bigcap\{A : A \in A\}\) as a unique minimal element;

(c) if \(x \in M\), then \(b \leq x\);

(d) Let \(P = \{x \in M : \text{if } y \in M \text{ and } y < x, \text{ then } f(y) \leq x\}\). Now if
\(x \in P\) and \(z \in M\), then either \(z \leq x\) or \(f(x) \leq z\);

(e) \(P\) is an admissible subset of \(M\), and hence \(P = M\); and

(f) \(M\) is totally ordered.

21. **Lemma:** Let \((X, \leq)\) be a non-empty partially ordered set such that each totally ordered subset of \(X\) has a least upper bound. If \(f : X \to X\) is such that \(x \leq f(x)\) for all \(x \in X\), then there exists \(p \in X\) such that \(f(p) = p\).

22. **Theorem:** Each of the following is equivalent to the Axiom of Choice:

(a) **Kuratowski's Lemma:** Each chain in a partially ordered set is contained in a maximal chain.

(b) **Hausdorff Maximal Principle:** Each partially ordered set contains a maximal chain.

(c) **Zorn's Lemma:** If each chain in a partially ordered set \((X, \leq)\) has an upper bound, then \(X\) has a maximal member.

(d) **The Well-Ordering Principle:** Each set can be well-ordered.

5  **Finite and Infinite Sets**

A set \(X\) is said to be *infinite* provided there exists a proper subset \(B \subset X\) and a one-to-one function \(f : X \to B\) from \(X\) onto \(B\). Otherwise, we say that \(X\) is *finite*.

For \(n \in \mathbb{N}\), we use \(\{n\}\) to denote the set \(\{m \in \mathbb{N} : m \leq n\}\).

23. **Lemma:** Let \(X\) be a set. Then exactly one of the following holds:

(i) There exists a one-to-one function \(\phi : \{n\} \to X\) of \(\{n\}\) onto \(X\); or

(ii) There exists a one-to-one function \(\psi : \mathbb{N} \to X\) of \(\mathbb{N}\) into \(X\).

24. **Theorem:** Let \(X\) be a non-empty set. Then \(X\) is finite if and only if there exists \(n \in \mathbb{N}\) and a one-to-one onto function \(f : X \to \{n\}\).

A set \(X\) is said to be *denumerable* if there exists a one-to-one function \(\phi : X \to \mathbb{N}\) from \(X\) onto \(\mathbb{N}\).

A set \(X\) is said to be *countable* if it is either finite or denumerable. It is *uncountable* otherwise.

25. **Theorem:** A set \(X\) is infinite if and only if \(X\) contains a denumerable subset.
26. **Theorem:** If the domain of a function is countable, then the range is also countable.

27. **Theorem:** If \( A \) is a countable family of countable sets, then \( \bigcup \{ A : A \in A \} \) is countable.

The following Lemma will be useful in the proof of A4.7:

28. **Lemma:** Let \( \{ x_n \} \) be a sequence in \( \mathbb{N} \). Then there exists an increasing sequence \( \{ p_n \} \) such that \( x_n < p_n \) for each \( n \in \mathbb{N} \).

**Proof:** We will apply the Recursion Theorem. Let \( p_1 = x_1 + 1 = e \), and define \( R_n : \mathbb{N} \to \mathbb{N} \) by \( R_n(x) = x + x_n + 1 \). Then there exists a function \( F : \mathbb{N} \to \mathbb{N} \) such that \( F(1) = p_1 \) and \( F(n+1) = R_{n+1}[F(n)] \) for each \( n \in \mathbb{N} \). Let \( p_n = F(n) \) for each \( n \in \mathbb{N} \). Then \( p_{n+1} = F(n + 1) = p_n + x_{n+1} + 1 \).

29. **Theorem:** Let \( D \) be a denumerable set, \( \mathcal{F} \) the family of all finite subsets of \( D \), and let \( \mathcal{S} \) be the family of all subsets of \( D \). Then \( \mathcal{F} \) is denumerable and \( \mathcal{S} \) is uncountable.

## 6 Well-Ordered Sets

If \( (X, \leq) \) is a well-ordered set and \( a \in X \), then \( x < a \) means that \( x \leq a \) and \( x \neq a \). The set \( L(a) = \{ x \in X : x < a \} \) is called the initial interval determined by \( a \).

If \( (X, \leq) \) is a well-ordered set and \( I \subseteq X \), then \( I \) is said to be an ideal of \( X \), provided \( L(a) \subseteq I \) for each \( a \in I \).

If \( (X, \leq) \) is a well-ordered set, then \( X \) and \( \emptyset \) are ideals of \( X \). Observe that \( \emptyset \) is an initial interval determined by the first element of \( X \), and \( X \) is not an initial interval. Also, \( L(a) \) is an ideal for each \( a \in X \).

If \( (X, \leq) \) is a well-ordered set, then \( \mathcal{I}(X) \) denotes the family of all ideals of \( X \), and \( \mathcal{J}(X) \) denotes the family of all initial intervals of \( X \).

30. **Theorem:** Let \( (X, \leq) \) be a well-ordered set. Then:

   (a) The intersection of ideals of \( X \) is an ideal of \( X \);

   (b) The union of ideals of \( X \) is an ideal of \( X \); and

   (c) \( \mathcal{J}(X) = \mathcal{I}(X) \setminus \{ X \} \).

31. **Theorem:** If \( (X, \leq) \) is a well-ordered set, then \( (\mathcal{I}(X), \subseteq) \) is a well-ordered set.

   If \( (X, \leq) \) and \( (X', \leq') \) are well-ordered sets, a function \( f : X \to X' \) is called a monomorphism, provided \( f \) is one-to-one and order-preserving; i.e., \( x \leq y \) in \( X \) implies that \( f(x) \leq' f(y) \) in \( X' \). If \( f \) also maps \( X \) onto \( X' \), then \( f \) is called an isomorphism.
32. **Theorem:** If \((X, \leq)\) is a well-ordered set, then the function \(a \mapsto L(a)\) of \((X, \leq)\) onto \((\mathcal{J}(X), \subseteq)\) is an isomorphism.

33. **Theorem:** Let \((X, \leq)\) be a well-ordered set, and let \(\Sigma\) be a family of ideals of \(X\) satisfying:

   (a) Any union of members of \(\Sigma\) is a member of \(\Sigma\); and
   (b) If \(L(a) \in \Sigma\), then \(L(a) \cup \{a\} \in \Sigma\).
   (c) Then \(\Sigma = \mathcal{I}(X)\) and, in particular, \(X \in \Sigma\).

34. **Lemma:** Let \((X, \leq)\) and \((X', \leq')\) be well-ordered sets, and let \(\phi : X \to X'\) be an isomorphism of \(X\) onto an ideal of \(X'\). Then any monomorphism \(f : X \to X'\) satisfies the condition that \(\phi(x) \leq' f(x)\) for each \(x \in X\). In particular, there can be at most one isomorphism between an ideal of \(X\) and an ideal of \(X'\).

35. **Theorem:** Let \((X, \leq)\) and \((X', \leq')\) be well-ordered sets. Then exactly one of the following holds:

   (a) There is a unique isomorphism of \(X\) onto \(X'\);
   (b) There is a unique isomorphism of \(X\) onto an initial interval of \(X'\);
   (c) There is a unique isomorphism of \(X'\) onto an initial interval of \(X\).

36. **Corollary:** Let \((X, \leq)\) be a well-ordered set, and let \(A \subseteq X\). Then \(A\) is isomorphic to \(X\) or to an initial interval of \(X\).

37. **Corollary:** Let \((X, \leq)\) be a well-ordered set. Then no initial interval of \(X\) is isomorphic to \(X\).

38. **Corollary:** The class of all well-ordered sets is well-ordered, if we define \(X \leq X'\) to mean that \(X\) is isomorphic to an ideal of \(X'\) (and \(X = X'\) means that \(X\) is isomorphic to \(X'\)).

39. **Transfinite Induction:** Let \((X, \leq)\) be a well-ordered set, and let \(A \subseteq X\). If \(L(x) \subseteq A\) implies that \(x \in A\) for each \(x \in X\), then \(A = X\).

   Note that if \((\mathbb{N}, \leq)\) is the positive integers with its usual order, then A39 is equivalent to what is usually referred to as strong finite induction.

7 Quotient Sets and the Integers

40. **Theorem:** There is a unique function \(\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}\) such that:

   (1) \(\phi(x, 1) = x\) for each \(x \in \mathbb{N}\); and
   (2) \(\phi(x, y + 1) = \phi(x, y) + x\) for each \(x, y \in \mathbb{N}\).
The function $\phi$ in A6.1 is called multiplication on $\mathbb{N}$, and we write $xy$ for $\phi(x,y)$ for each $x, y \in \mathbb{N}$.

41. Theorem: If $a, b, c \in \mathbb{N}$, then:
   
   (1) $(ab)c = a(bc)$ (associative);
   
   (2) $ab = ba$ (commutative);

   (3) $a(b + c) = ab + ac$ (distributive); and

   (4) If $ac = bc$, then $a = b$ (cancellation).

If $X$ is a set and $\sigma$ is an equivalence relation on $X$, then $X/\sigma$ denotes the set of $\sigma$-classes of $X$. We call $X/\sigma$ the quotient set of $X$ mod $\sigma$. Then function $\eta : X \to X/\sigma$, defined by letting $\eta(x)$ be the $\sigma$-class containing $x$ for each $x \in X$, is called the natural map. Observe that for $x, y \in X$, $\eta(x) = \eta(y)$ if and only if $(x, y) \in \sigma$. Moreover, for each $x \in X$, $\eta^{-1}\eta(x) = \{y \in X : (x, y) \in \sigma\}$ (the $\sigma$-class of $x$).

Define a relation $\tau$ on $\mathbb{N} \times \mathbb{N}$ as follows:

$$\tau = \{(a, b), (x, y)\} \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) : a + y = x + b\}$$

42. Theorem: The relation $\tau$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Let $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\tau$, and let $\mu : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ be the natural map.

43. Theorem: The map $\beta : \mathbb{N} \to \mathbb{Z}$ defined by $\beta(x) = \mu((x + 1, 1))$ is a one-to-one function.

The set $\mathbb{Z}$ is called the integers. In view of A6.4, we will identify $\mathbb{N}$ with its image under $\beta$ in $\mathbb{Z}$.

Let $\Delta = \{(a, a) : a \in \mathbb{N}\}$.

44. Theorem: The set $\Delta$ is a $\tau$-class in $\mathbb{N} \times \mathbb{N}$.

The image $\mu[\Delta]$ in $\mathbb{Z}$ is called zero and is denoted by 0.

45. Lemma: If $a, b, x \in \mathbb{N}$, then $\mu(a + x, b + x) = \mu(a, b)$.

We define addition on $\mathbb{Z}$ by $\mu(a, b) + \mu(c, d) = \mu(a + c, b + d)$ for $a, b, c, d \in \mathbb{N}$.

46. Theorem: Addition on $\mathbb{Z}$ is well-defined. Moreover, if $x, y, z \in \mathbb{Z}$, then:

   (1) $(x + y) + z = x + (y + z)$ (associative);

   (2) $x + y = y + x$ (commutative);

   (3) $x + z = y + z$ implies $x = y$ (cancelative); and

   (4) if $x, y \in \mathbb{N}$, then $x + y \in \mathbb{N}$. 

If $z = \mu(a, b)$ in $\mathbb{Z}$, then we write $-z = \mu(b, a)$. For $x, y \in \mathbb{Z}$, we write $x - y = x + (-y)$.

**47. Theorem:** The set $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$, and these sets are disjoint.

**48. Theorem:** If $x \in \mathbb{Z}$, then

1. $x + 0 = x$; and
2. $x + (-x) = 0$.

Note: $(\mathbb{Z}, +)$ is an abelian group whose identity is 0.

We define $\leq$ on $\mathbb{Z}$ by $x \leq y$, provided that either $x = y$ or $y - x \in \mathbb{N}$. We say that $z \in \mathbb{Z}$ is positive provided $z \in \mathbb{N}$.

**49. Theorem:** The relation $\leq$ is a total order on $\mathbb{Z}$. Moreover,

1. $x \in \mathbb{Z}$ is positive if and only if $0 < x$ ($0 \leq x$ and $x \neq 0$); and
2. If $x \leq y$ and $z \in \mathbb{Z}$, then $x + z \leq y + z$.

We define multiplication on $\mathbb{Z}$ by

$$\mu(a, b) \cdot \mu(c, d) = \mu(ac + bd, bc + ad)$$

**50. Theorem:** Multiplication on $\mathbb{Z}$ is well-defined. Moreover, if $x, y, z \in \mathbb{Z}$, then:

1. $(xy)z = x(yz)$ (associative);
2. $xy = yx$ (commutative);
3. If $z \neq 0$ and $xz = yz$, then $x = y$ (cancellative);
4. $x \cdot 0 = 0$;
5. $x \cdot 1 = x$; and
6. $x(y + z) = xy + xz$ (distributive).

**51. Theorem:** Let $x, y, z \in \mathbb{Z}$.

1. If $x \leq y$ and $0 \leq z$, then $xz \leq yz$; and
2. If $x \leq y$ and $z \leq 0$, then $yz \leq xz$.

## 8 The Real Numbers

Let $\mathbb{Z} = \mathbb{Z} \setminus \{0\}$, and let $\sigma = \{((a, b), (x, y)) \in (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) : ay = bx\}$.

**52. Theorem:** The relation $\sigma$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$.

Note:
(1) $\sigma(0, 1) = \sigma(0, x)$ for all $x \in \mathbb{Z}_*$;
(2) If $\sigma(0, 1) = \sigma(a, b)$, then $a = 0$; and
(3) If $x \neq 0$, then $\sigma(a, b) = \sigma(xa, xb)$.

The quotient $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}_*)/\sigma$ is called the set of rational numbers. Let $\sigma[a, b]$ denote the $\sigma$-class of $(a, b) \in \mathbb{Z} \times \mathbb{Z}_*$.

Define addition on $\mathbb{Q}$ by $\sigma[a, b] + \sigma[c, d] = \sigma[ad + bc, bd]$; and multiplication by $\sigma[a, b] \cdot \sigma[c, d] = \sigma[ac, bd]$.

53. Theorem: Addition and multiplication are well-defined functions from $\mathbb{Q} \times \mathbb{Q}$ into $\mathbb{Q}$.

54. Theorem: Addition and multiplication on $\mathbb{Q}$ are associative and commutative. Moreover, $1 = \sigma[1, 1]$ is a multiplicative identity and $0 = \sigma[0, 1]$ is an additive identity.

If $x \in \mathbb{Q}$, let $x = \sigma[a, b]$, then $-x = \sigma[-a, b]$ ($= \sigma[a, -b]$), and if $x \neq 0$, let $x^{-1} = \sigma[b, a]$.

7.4. Theorem:

(i) If $x \in \mathbb{Q}$, then $x + (-x) = 0$;
(ii) If $x \in \mathbb{Q}$, $x \neq 0$, then $xx^{-1} = 1$;
(iii) If $x, y, z \in \mathbb{Q}$, then $x(y + z) = xy + xz$ (distributive); and
(iv) If $x \in \mathbb{Q}$, then $x \cdot 0 = 0$.

For $p \in \mathbb{Q}$, define $0 \leq p$ provided either $p = 0$ or $p = \sigma[a, b]$, where $0 < a$ and $0 < b$ in $\mathbb{Z}$. For $x, y \in \mathbb{Q}$, define $x \leq y$ if $0 \leq y - x$ ($= y + (-x)$).

55. Theorem: If $x, y, z \in \mathbb{Q}$ with $x \leq y$, then

(i) $x + z \leq y + z$;
(ii) if $0 < z$, then $xz \leq yz$; and
(iii) if $z < 0$, then $yz \leq xz$.

We say that $x \in \mathbb{Q}$ is positive if $0 < x$, and negative if $x < 0$.

56. Theorem: The relation $\leq$ is a total order on $\mathbb{Q}$.

57. Theorem: The map $\psi : \mathbb{Z} \rightarrow \mathbb{Q}$ defined by $\psi(x) = \sigma[x, 1]$ is a one-to-one map of $\mathbb{Z}$ into $\mathbb{Q}$ such that $\psi(x+y) = \psi(x) + \psi(y)$ and $\psi(xy) = \psi(x)\psi(y)$ for each $x, y \in \mathbb{Z}$.

We identify $\mathbb{Z}$ with its image under $\psi$ in $\mathbb{Q}$.

For $x \in \mathbb{Q}$, define absolute value of $x$:

$$|x| = \begin{cases} x & \text{if } 0 \leq x; \\ -x & \text{if } x < 0 \end{cases}$$
58. **Theorem:** If \( x, y, z \in \mathbb{Q} \), then \(|x + y| \leq |x| + |y|\).

**Note:** \((\mathbb{Q}, +, \cdot, \leq)\) is an ordered field.

Let \( \mathbb{Q}^N = \{ f : \mathbb{N} \to \mathbb{Q} \} \); i.e., the set of all sequences in \( \mathbb{Q} \). We will adopt the usual convention of writing \( x_n = f(n) \), and say that \( \{x_n\} \) is a sequence.

A sequence \( \{x_n\} \) is called a **Cauchy sequence**, provided for each \( \epsilon \in \mathbb{Q} \) such that \( 0 < \epsilon \), there exists \( p \in \mathbb{N} \) such that \( |x_n - x_m| < \epsilon \) when \( p < n, m \). We denote by \( \mathbb{Q}^*_N \) the set of all Cauchy sequences in \( \mathbb{Q} \).

Define \( \rho = \{(x_n), (y_n)\} \in \mathbb{Q}_N^* \times \mathbb{Q}_N^* : \) for each \( 0 < \epsilon \in \mathbb{Q} \), there exists \( p \in \mathbb{N} \) such that \( |x_n - y_n| < \epsilon \), when \( p < n \).

**Note:** Each Cauchy sequence \( \{x_n\} \in \mathbb{Q} \) is bounded; i.e., there exists \( r \in \mathbb{Q} \) such that \( |x_n| \leq r \) for all \( n \in \mathbb{N} \).

59. **Theorem:** The relation \( \rho \) is an equivalence relation on \( \mathbb{Q}^*_N \).

The quotient \( \mathbb{R} = \mathbb{Q}^*_N/\rho \) is called the **set of real numbers**. For a Cauchy sequence \( \{x_n\} \in \mathbb{Q} \), we let \( \rho[x_n] \) denote the \( \rho \)-class of \( \{x_n\} \).

Note that for \( r \in \mathbb{Q} \), the sequence \( \{x_n\} \) such that \( x_n = r \) for all \( n \in \mathbb{N} \) is a Cauchy sequence (which we denote by \( \{r\} \)).

Define **addition** on \( \mathbb{R} \) by \( \rho[x_n] + \rho[y_n] = \rho[x_n + y_n] \); and define **multiplication** on \( \mathbb{R} \) by \( \rho[x_n] \cdot \rho[y_n] = \rho[x_n y_n] \).

60. **Theorem:** Multiplication and addition are well-defined functions \( \mathbb{R} \times \mathbb{R} \to \mathbb{R} \).

61. **Theorem:** Multiplication and addition on \( \mathbb{R} \) are associative and commutative. Moreover, \( 1 = \rho[1] \) is a multiplicative identity and \( 0 = \rho[0] \) is an additive identity.

62. **Lemma:** If \( x \neq 0 \) in \( \mathbb{R} \), then there exists a Cauchy sequence \( \{x_n\} \in \mathbb{Q} \) such that \( x = \rho[x_n] \) and \( x_n \neq 0 \) for all \( n \in \mathbb{N} \).

If \( x \in \mathbb{R} \), \( x = \rho[x_n] \), define \( -x = \rho[-x_n] \).

If \( x \in \mathbb{R} \) and \( x \neq 0 \), let \( \{x_n\} \) be a Cauchy sequence in \( \mathbb{Q} \) such that \( x_n \neq 0 \) for all \( n \in \mathbb{N} \), and define \( x^{-1} = \rho[x_n^{-1}] \).

63. **Theorem:** If \( x \in \mathbb{R} \), then \( -x \) is well-defined. Moreover, if \( x \neq 0 \), then \( x^{-1} \) is well-defined.

64. **Theorem:** Let \( x, y, z \in \mathbb{R} \).

(i) \( x + (-x) = 0 \);

(ii) if \( x \neq 0 \), then \( xx^{-1} = 1 \);

(iii) \( x(y + z) = xy + xz \) (distributive); and

(iv) \( x \cdot 0 = 0 \).
For \( p \in \mathbb{R} \), define \( 0 \leq p \) provided there exists a Cauchy sequence \( \{x_n\} \) in \( \mathbb{Q} \) such that \( 0 \leq x_n \) for all \( n \in \mathbb{N} \) and \( p = \rho[x_n] \). Define \( 0 < p \) if \( 0 \leq p \) and \( p \neq 0 \). For \( x, y \in \mathbb{R} \), define \( x \leq y \) provided \( 0 \leq y - x \) (= \( y + (-x) \)).

65. **Theorem:** If \( x, y, z \in \mathbb{R} \) with \( x \leq y \), then

   (i) \( x + z \leq y + z \);

   (ii) if \( 0 < z \), then \( xz \leq yz \); and

   (iii) if \( z < 0 \), then \( yz \leq xz \).

   We say that \( x \in \mathbb{R} \) is **positive** if \( 0 < x \), and **negative** if \( x < 0 \).

66. **Theorem:** The relation \( \leq \) is a total order on \( \mathbb{R} \).

67. **Theorem:** The map \( \phi : \mathbb{Q} \to \mathbb{R} \) defined by \( \phi(a) = \rho[a] \) is a one-to-one map of \( \mathbb{Q} \) into \( \mathbb{R} \) such that \( \phi(a + b) = \phi(a) + \phi(b) \) and \( \phi(ab) = \phi(a) \cdot \phi(b) \) for each \( a, b \in \mathbb{Q} \).

   We identify \( \mathbb{Q} \) with its image under \( \phi \) in \( \mathbb{R} \).

**Note:** \( (\mathbb{R}, +, \cdot, \leq) \) is an ordered field.

For \( x \in \mathbb{R} \), define the **absolute value** of \( x \):

\[
|x| = \begin{cases} x & \text{if } 0 \leq x; \\ -x & \text{if } x < 0 \end{cases}
\]

A68. **Theorem:** If \( x, y \in \mathbb{R} \), then \( |x + y| \leq |x| + |y| \).

A69. **Theorem:** If \( x < y \) in \( \mathbb{R} \), then there exists \( q \in \mathbb{Q} \) such that \( x < q < y \).

A sequence \( \{x_n\} \) in \( \mathbb{R} \) is called a **Cauchy sequence** provided that for each \( 0 < \epsilon \) in \( \mathbb{R} \), there exists \( p \in \mathbb{N} \) such that \( |x_n - x_m| < \epsilon \) when \( p < n, m \).

A sequence \( \{x_n\} \) in \( \mathbb{R} \) is said to **converge** to \( x \in \mathbb{R} \) if for each \( 0 < \epsilon \) in \( \mathbb{R} \), there exists \( p \in \mathbb{N} \) such that \( |x_n - x| < \epsilon \) when \( p < n \).

A70. **Archimedean Property:** If \( r \in \mathbb{R} \), then there exists \( n \in \mathbb{N} \) such that \( r < n \).

A71. **Completeness:** Each Cauchy sequence in \( \mathbb{R} \) converges.

A72. **Theorem:** Each subset of \( \mathbb{R} \) which has an upper bound has a least upper bound.

A73. **Theorem:** The set \( \mathbb{Q} \) is denumerable.

A74. **Theorem:** The set \( \mathbb{R} \) is non-denumerable.
9 Ordinal Numbers

An ordinal number is a set \( P \) satisfying:

(a) If \( x \in P \) and \( y \in P \), then either \( x \in y \) or \( y \in x \), or \( x = y \); and

(b) If \( x \in y \) and \( y \in P \), then \( x \in P \).

75. Example: \( P = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \) is an ordinal number.

Some results from set theory are:

(a) Axiom: If \( A \) is a set, then there exists \( u \in A \) such that \( u \cap A = \emptyset \).

(b) Theorem: If \( A \) is a set, then \( A \notin A \).

(c) Theorem: If \( A \) and \( B \) are sets, then either \( A \notin B \) or \( B \notin A \).

Note that if \( P \) is an ordinal number, then \( \in \) is not a quasi-order on \( P \), since \( x \notin x \) for any \( x \in P \).

76. Theorem: Let \( P \) be an ordinal number, and let \( A \) be a non-empty subset of \( P \). Then there is a unique \( a \in A \) such that either \( a \in x \) or \( a = x \) for each \( x \in A \).

The element \( a \) in A8.1 is called the first element of \( A \).

77. Theorem: If \( P \) is an ordinal number, then \( \emptyset \) is the first element of \( P \).

78. Theorem: If \( P \) is an ordinal number and \( x \in P \), then \( x \) is an ordinal number.

79. Theorem: If \( P \) and \( Q \) are distinct ordinal numbers, then \( P \subset Q \) if and only if \( P \in Q \).

80. Theorem: Let \( P \) and \( Q \) be distinct ordinal numbers. Then either \( P \subset Q \) or \( Q \subset P \).

81. Theorem: The class of all ordinal numbers is well-ordered by \( \subseteq \).

82. Theorem: If \( \mathcal{E} \) is a class of ordinal numbers, then \( \mathcal{E} \) is well-ordered by \( \subseteq \), and in particular \( \mathcal{E} \) has a first element.

83. Theorem: The class of all ordinal numbers is not a set.

Let \( \mathcal{O} \) denote the class of all ordinal numbers.

84. Theorem: If \( P \) is an ordinal number, then the set \( L(P) \) of initial intervals determined by \( P \) in \( (\mathcal{O}, \subseteq) \) is \( P \). In particular, \( L(P) \) is a set.

85. Theorem: If \( E \) is a set of ordinal numbers, then \( E \) has a least upper bound in \( (\mathcal{O}, \subseteq) \).
86. **Theorem:** If \((X, \leq)\) is a well-ordered set, then \((X, \leq)\) is isomorphic to 
\((P, \subseteq)\) for some unique ordinal number \(P\).

In A86, we call \(P\) the *ordinal* of \((X, \leq)\), and denote \(P = \text{ord}(X, \leq)\).

87. **Theorem:** Let \((X, \leq)\) be a well-ordered set, and suppose \(m \notin X\). Then 
\((X \cup \{m\}, \leq)\) is well-ordered if \(\leq\) is extended to \(X \cup \{m\}\) so that \(x \leq m\) 
for all \(x \in X \cup \{m\}\). Moreover, \(\text{ord} \ (X \cup \{m\}, \leq) = \text{ord} \ (X, \leq) \cup \{\text{ord} \ (X, \leq)\}\).

88. **Theorem:** If \(P \in \mathcal{O}\), then \(P \cup \{P\}\) is the successor of \(P\) in \((\mathcal{O}, \subseteq)\).

An ordinal \(P \neq \emptyset\) is called a *limit ordinal* provided \(P\) has no predecessor in 
\((\mathcal{O}, \subseteq)\).

Let \((\mathbb{N}^*, \leq)\) denote the non-negative integers with the usual order. Let \(\omega = \text{ord} (\mathbb{N}^*, \leq)\). Let \(\pi\) denote \((\mathbb{L}(n), \leq)\) for each \(n \in \mathbb{N}^*\).

For \(n \in \mathbb{N}^*\), we will use \(\eta\) to denote \(\text{ord} \pi\).

For sets \(A\) and \(B\), we use \(A \cup B\) to denote the disjoint union of \(A\) and \(B\).

89. **Theorem:** Let \(A\) and \(B\) be ordinal numbers. Define \(\leq\) on \(A \cup B\) as follows:

- \(x \leq y\) if either \(x\) and \(y\) are both in \(A\) or both in \(B\) and \(x \leq y\); and
- \(x < y\) if \(x \in A\) and \(y \in B\).

Then \((A \cup B, \leq)\) is a well-ordered set.

If \(A\) and \(B\) are ordinal numbers, then the *sum* of \(A\) and \(B\) is defined as 
\(A + B = \text{ord}(A \cup B, \leq)\), where \((A \cup B, \leq)\) is the well-ordered set of A8.1A7.

90. **Theorem:** Let \(A\) and \(B\) be ordinal numbers. Define \(\leq\) on \(A \times B\): 
\(\leq\) for \((a, b), (a', b') \in A \times B\), let \((a, b) \leq (a', b')\), provided that either \(a \leq a'\) or 
\(a = a'\) and \(b \leq b'\). Then \((A \times B, \leq)\) is a well-ordered set.

The order on \(A \times B\) in A8.18 is called the *lexicographic order*.

If \(A\) and \(B\) are ordinal numbers, then the *product* \(BA\) is defined as 
\(BA = \text{ord} (A \times B, \leq)\) where \(\leq\) is the lexicographic order on \(A \times B\).

10 **Cardinal Numbers**

Two sets \(X\) and \(Y\) are said to be *equipotent* if there is a one-to-one function from \(X\) onto \(Y\). Note that equipotence is an equivalence relation on the class of all sets. An equivalence class of this relation is called an *equipotence class*.

If \(X\) is a set, then the family of all subsets of \(X\) is denoted \(\mathcal{P}(X)\) and the family of all functions from \(X\) into \(\{0, 1\}\) is denoted by \(2^X\).

91. **Theorem:** If \(X\) is a set, then \(\mathcal{P}(X)\) and \(2^X\) are equipotent.
92. **Theorem:** If \( f : X \to Y \) is a function from \( X \) onto \( Y \), then \( Y \) is equipotent to a subset of \( X \).

If \( X \) is a set, let \( \mathcal{E}_X \) denote the equipotence class of \( X \). Note that since \( X \) can be well-ordered, \( \mathcal{E}_X \) contains at least one ordinal number. The **cardinal number** of \( X \) is defined to be the first ordinal number in \( \mathcal{E}_X \) (see A5.7) and is denoted \( \sharp X \).

93. **Theorem:** Let \( X \) and \( Y \) be sets. Then \( X \) is equipotent to a subset of \( Y \) if and only if \( \sharp X \subseteq \sharp Y \). In particular, \( X \) and \( Y \) are equipotent if and only if \( \sharp X = \sharp Y \).

94. **The Schröder-Bernstein Theorem:** If \( X \) and \( Y \) are sets, and there exist one-to-one functions \( f : X \to Y \) and \( g : Y \to X \), then there exists a one-to-one function \( h : X \to Y \) from \( X \) onto \( Y \).

95. **Theorem:** If \( X \) is a set, then \( \sharp X \subseteq \sharp \mathcal{P}(X) \).

If \( X \) is an infinite set, then \( \sharp X \) is called a **transfinite cardinal number**.

96. **Theorem:** In the order \( \subseteq \) on the class of all cardinal numbers, ord \( \emptyset \) is the smallest cardinal number, and \( \aleph_0 \) is the smallest transfinite cardinal number.

97. **Theorem:** The class of all cardinal numbers is not a set.

We use \( c \) to denote \( \sharp \mathcal{R} \).

Observe that \( \mathcal{P}(\mathbb{N}) \) and \( 2^\mathbb{N} \) are equipotent (A91), and hence \( \sharp \mathcal{P}(\mathbb{N}) = \sharp 2^\mathbb{N} \) (A94). Now \( \sharp \mathcal{P}(\mathbb{N}) = \sharp \mathcal{R} = c \) (A98). In view of A9.9, we see that \( \sharp \mathbb{N} \) is a proper subset of \( \sharp \mathcal{P}(\mathbb{N}) \), and we conclude that \( \aleph_0 \) is a proper subset of \( c \).

**The Continuum Hypothesis:** If \( k \) is a cardinal number and \( \aleph_0 \subseteq k \subseteq c \), then either \( k = \aleph_0 \) or \( k = c \); i.e., there is no cardinal number between \( \aleph_0 \) and \( c \).

**The Generalized Continuum Hypothesis:** If \( X \) is an infinite set and \( k \) is a cardinal number such that \( \sharp X \subseteq k \subseteq \sharp \mathcal{P}(X) \) (see A99), then either \( k = \sharp X \) or \( k = \sharp \mathcal{P}(X) \).

98. **Theorem:** If \( A = \sharp X \), then \( 2^A = \sharp \mathcal{P}(X) \). Moreover, \( A \subset 2^A \).

99. **Theorem:** If \( A \) is a transfinite cardinal number, then \( A^2 = A \).

100. **Corollary:** Let \( A \) and \( B \) be non-empty cardinal numbers, at least one of which is transfinite. Then \( AB = A + B = \max\{A, B\} \).

If \( A \) is a transfinite cardinal number and \( C_A = \{C : C \) is a cardinal number and \( C \subseteq A\} \), then the **aleph index** of \( A \) is \( i(A) = \text{ord}(C_A, \subseteq) \).
101. **Theorem:** Let $A$ and $B$ be transfinite cardinal numbers. Then:

(a) $A = B$ if and only if $i(A) = i(B)$;

(b) $A \subseteq B$ if and only if $i(A) \subseteq i(B)$; and

(c) $A \subset B$ if and only if $i(A) \subset i(B)$.

102. **Theorem:** If $B$ is an ordinal number, then there exists a unique transfinite cardinal number $A$ such that $B = i(A)$.

The cardinal number corresponding to an ordinal number $B$ in A9.12 is denoted $\aleph_B$.

103. **Theorem:** If $B$ is an ordinal number and $A$ is a cardinal number such that $\aleph_B \subseteq A \subseteq \aleph_{B+1}$, then $A = \aleph_A$ or $A = \aleph_{A+1}$.

104. **Theorem:** If $B$ is an ordinal number and $A$ is a non-empty cardinal number, then $\aleph_A^{\aleph_B} = \aleph_A^{\aleph_B \aleph_{B+1}}$. 