# C1 Set Theory

## Robin Adams

## August 22, 2022

# 1 Primitive Notions

Let there be *sets*.

Let there be a binary relation called *membership*, $\in$. When $x \in y$ holds, we say $x$ is a *member* or *element* of $y$. We write $x \notin y$ iff $x$ is not a member of $y$.

# 2 The Axioms

**Axiom 1** (Extensionality). *If two sets have exactly the same members, then they are equal.*

As a consequence of this axiom, we may identify a set $A$ with the class $\{x : x \in A\}$. The use of the symbols $\in$ and $=$ is consistent.

**Definition 2.** We say that a class $\mathbf{A}$ *is a set* iff there exists a set $A$ such that $A = \mathbf{A}$. That is, the class $\{x : P(x)\}$ is a set iff

$$\exists A.\forall x(x \in A \leftrightarrow P(x)) \ .$$

Otherwise, $\mathbf{A}$ is a *proper class*.

**Definition 3** (Subset). If $A$ is a set and $\mathbf{B}$ is a class, we say $A$ is a *subset* of $\mathbf{B}$ iff $A \subseteq \mathbf{B}$.

**Axiom 4** (Empty Set). *The empty class is a set, called the* empty set*.*

**Axiom 5** (Pairing). *For any objects $a$ and $b$, the class $\{a, b\}$ is a set, called a* pair set*.*

**Definition 6** (Union). For any class of sets $\mathbf{A}$, the *union* $\bigcup \mathbf{A}$ is the class $\{x : \exists A \in \mathbf{A}.x \in A\}$.

We write $\bigcup_{P[x_1,\ldots,x_n]} t[x_1, \ldots, x_n]$ for $\bigcup\{t[x_1, \ldots, x_n] : P[x_1, \ldots, x_n]\}$.

**Proposition 7.** *If $\mathbf{A} \subseteq \mathbf{B}$ then $\bigcup \mathbf{A} \subseteq \bigcup \mathbf{B}$.*

PROOF: Easy. $\square$

**Axiom 8** (Union). *For any set $A$, the union $\bigcup A$ is a set.*

**Proposition 9.** *For any sets $A$ and $B$, the class $A \cup B$ is a set.*

PROOF: It is $\bigcup\{A, B\}$. □

**Proposition Schema 10.** *For any objects $a_1$, ..., $a_n$, the class $\{a_1, \ldots, a_n\}$ is a set.*

PROOF: By repeated application of the Pairing and Union axioms. □

**Definition 11** (Power Set)**.** For any set $A$, the *power set* of $A$, $\mathcal{P}A$, is the class of all subsets of $A$.

**Axiom 12** (Power Set)**.** *For any set $A$, the class $\mathcal{P}A$ is a set.*

**Axiom 13** (Subset, Aussonderung)**.** *For any class $\mathbf{A}$ and set $B$, if $\mathbf{A} \subseteq B$ then $\mathbf{A}$ is a set.*

**Proposition 14.** *For any set $A$ and class $\mathbf{B}$, the intersection $A \cap \mathbf{B}$ is a set.*

PROOF: By the Subset Axiom since it is a subclass of $A$. □

**Proposition 15.** *For any set $A$ and class $\mathbf{B}$, the relative complement $A - \mathbf{B}$ is a set.*

PROOF: By the Subset Axiom since it is a subclass of $A$. □

**Theorem 16.** *The universal class $\mathbf{V}$ is a proper class.*

PROOF:
⟨1⟩1. ASSUME: $\mathbf{V}$ is a set.
⟨1⟩2. LET: $R = \{x : x \notin x\}$
⟨1⟩3. $R$ is a set.
   PROOF: By the Subset Axiom.
⟨1⟩4. $R \in R$ if and only if $R \notin R$
⟨1⟩5. Q.E.D.
   PROOF: This is a contradiction.
□

**Definition 17** (Intersection)**.** For any class of sets $\mathbf{A}$, the *intersection* $\bigcap \mathbf{A}$ is the class $\{x : \forall A \in \mathbf{A}.x \in A\}$.
   We write $\bigcap_{P[x_1,\ldots,x_n]} t[x_1, \ldots, x_n]$ for $\bigcap\{t[x_1, \ldots, x_n] : P[x_1, \ldots, x_n]\}$.

**Proposition 18.** *For any nonempty class of sets $\mathbf{A}$, the class $\bigcap \mathbf{A}$ is a set.*

PROOF: Pick $A \in \mathbf{A}$. Then $\bigcap \mathbf{A} \subseteq A$. □

**Proposition 19.** *If $\mathbf{A} \subseteq \mathbf{B}$ then $\bigcap \mathbf{B} \subseteq \bigcap \mathbf{A}$.*

PROOF: Easy. □

**Proposition 20.** *For any set $A$ and class of sets $\mathbf{B}$, we have*

$$A \cup \bigcap \mathbf{B} = \bigcap\{A \cup X \mid X \in \mathbf{B}\}$$

PROOF: Easy. □

**Proposition 21.** *For any set $A$ and class of sets $\mathbf{B}$, we have*

$$A \cap \bigcup \mathbf{B} = \bigcup \{A \cap X \mid X \in \mathbf{B}\}$$

PROOF: Easy. □

**Proposition 22.** *For any set $C$ and class of sets $\mathbf{A}$, we have*

$$C - \bigcup \mathbf{A} = \bigcap \{C - X \mid X \in \mathbf{A}\} \ .$$

PROOF: Easy. □

**Proposition 23.** *For any set $C$ and class of sets $\mathbf{A}$, we have*

$$C - \bigcap \mathbf{A} = \bigcup \{C - X \mid X \in \mathbf{A}\} \ .$$

PROOF: Easy. □

# 3  Ordered Pairs

**Definition 24** (Ordered Pair)**.** For any objects $a$ and $b$, the *ordered pair* $(a, b)$ is $\{\{a\}, \{a, b\}\}$. We call $a$ its *first coordinate* and $b$ its *second coordinate*.

**Theorem 25.** *For any objects $(a, b)$, we have $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.*

PROOF:
$\langle 1 \rangle 1$. If $(a, b) = (c, d)$ then $a = c$ and $b = d$
$\quad \langle 2 \rangle 1$. ASSUME: $(a, b) = (c, d)$
$\quad \langle 2 \rangle 2$. $a = c$
$\quad \quad$ PROOF: Since $\{a\} = \bigcap(a, b) = \bigcap(c, d) = \{c\}$.
$\quad \langle 2 \rangle 3$. $\{a, b\} = \{c, d\}$
$\quad \quad$ PROOF: $\{a, b\} = \bigcup(a, b) = \bigcup(c, d) = \{c, d\}$.
$\quad \langle 2 \rangle 4$. $b = c$ or $b = d$
$\quad \langle 2 \rangle 5$. CASE: $b = c$
$\quad \quad \langle 3 \rangle 1$. $a = b$
$\quad \quad \langle 3 \rangle 2$. $\{c, d\} = \{a\}$
$\quad \quad \langle 3 \rangle 3$. $b = d$
$\quad \langle 2 \rangle 6$. CASE: $b = d$
$\quad \quad$ PROOF: We have $a = c$ and $b = d$ as required.
$\langle 1 \rangle 2$. If $a = c$ and $b = d$ then $(a, b) = (c, d)$
$\quad$ PROOF: Trivial.
□

**Definition 26** (Cartesian Product)**.** The *Cartesian product* of classes $\mathbf{A}$ and $\mathbf{B}$ is the class

$$\mathbf{A} \times \mathbf{B} = \{(x, y) : x \in \mathbf{A}, y \in \mathbf{B}\} \ .$$

**Lemma 27.** *For any objects $x$ and $y$ and set $C$, if $x \in C$ and $y \in C$ then $(x, y) \in \mathcal{PP}C$.*

PROOF: Easy. ☐

**Corollary 27.1.** *For any sets $A$ and $B$, the Cartesian product $A \times B$ is a set.*

PROOF: By the Subset Axiom applied to $\mathcal{PP}(A \cup B)$. ☐

**Lemma 28.** *If $(x, y) \in \mathbf{A}$ then $x, y \in \bigcup\bigcup \mathbf{A}$.*

PROOF: Easy. ☐

# 4 Relations

**Definition 29** (Relation). A *relation* is a class of ordered pairs. It is *small* iff it is a set.

When $\mathbf{R}$ is a relation, we write $x\mathbf{R}y$ for $(x, y) \in \mathbf{R}$.

**Definition 30** (Domain). The *domain* of a class $\mathbf{R}$ is $\operatorname{dom} \mathbf{R} = \{x : \exists y.(x, y) \in \mathbf{R}\}$.

**Definition 31** (Range). The *range* of a class $\mathbf{R}$ is $\operatorname{ran} \mathbf{R} = \{y : \exists x.(x, y) \in \mathbf{R}\}$.

**Definition 32** (Field). The *field* of a class $\mathbf{R}$ is $\operatorname{fld} \mathbf{R} = \operatorname{dom} \mathbf{R} \cup \operatorname{ran} \mathbf{R}$.

**Proposition 33.** *If $R$ is a set then $\operatorname{dom} R$, $\operatorname{ran} R$ and $\operatorname{fld} R$ are sets.*

PROOF: Apply the Subset Axiom to $\bigcup\bigcup R$. ☐

**Definition 34** (Single-Rooted). A class $\mathbf{R}$ is *single-rooted* iff, for all $y \in \operatorname{ran} \mathbf{R}$, there is only one $x$ such that $x\mathbf{R}y$.

**Definition 35** (Inverse). The *inverse* of a class $\mathbf{F}$ is the class $\mathbf{F}^{-1} = \{(y, x) \mid (x, y) \in \mathbf{F}\}$.

**Theorem 36.** *For any class $\mathbf{F}$, we have $\operatorname{dom} \mathbf{F}^{-1} = \operatorname{ran} \mathbf{F}$ and $\operatorname{ran} \mathbf{F}^{-1} = \operatorname{dom} \mathbf{F}$.*

PROOF: Easy. ☐

**Theorem 37.** *For a relation $\mathbf{F}$, $(\mathbf{F}^{-1})^{-1} = \mathbf{F}$.*

PROOF: Easy. ☐

**Definition 38** (Composition). The *composition* of classes $\mathbf{F}$ and $\mathbf{G}$ is the class $\mathbf{G} \circ \mathbf{F} = \{(x, z) \mid \exists y.(x, y) \in \mathbf{F} \wedge (y, z) \in \mathbf{G}\}$.

**Theorem 39.** *For any classes $\mathbf{F}$ and $\mathbf{G}$, $(\mathbf{F} \circ \mathbf{G})^{-1} = \mathbf{G}^{-1} \circ \mathbf{F}^{-1}$.*

PROOF: Easy. ☐

**Definition 40** (Restriction)**.** The *restriction* of the class $\mathbf{F}$ to the class $\mathbf{A}$ is the class $\mathbf{F} \upharpoonright \mathbf{A} = \{(x, y) : x \in A \land (x, y) \in \mathbf{F}\}$.

**Definition 41** (Image)**.** The *image* of the class $\mathbf{A}$ under the class $\mathbf{F}$ is the class $\mathbf{F}(\mathbf{A}) = \{y : \exists x \in \mathbf{A}.(x, y) \in \mathbf{F}\}$.

**Theorem 42.**
$$\mathbf{F}(\mathbf{A} \cup \mathbf{B}) = \mathbf{F}(\mathbf{A}) \cup \mathbf{F}(\mathbf{B})$$

PROOF: Easy. □

**Theorem 43.**
$$\mathbf{F}(\bigcup \mathbf{A}) = \bigcup \{\mathbf{F}(X) : X \in \mathbf{A}\}$$

PROOF: Easy. □

**Theorem 44.**
$$\mathbf{F}(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$$

*Equality holds if* $\mathbf{F}$ *is single-rooted.*

PROOF: Easy. □

**Theorem 45.**
$$\mathbf{F}(\bigcap \mathbf{A}) \subseteq \bigcap \{\mathbf{F}(X) : X \in \mathbf{A}\}$$

*Equality holds if* $\mathbf{F}$ *is single-rooted.*

PROOF: Easy. □

**Theorem 46.**
$$\mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B}) \subseteq \mathbf{F}(\mathbf{A} - \mathbf{B})$$

*Equality holds if* $\mathbf{F}$ *is single-rooted.*

PROOF: Easy. □

**Definition 47** (Reflexive)**.** A binary relation $\mathbf{R}$ on $\mathbf{A}$ is *reflexive* on $\mathbf{A}$ if and only if $\forall x \in \mathbf{A}.x\mathbf{R}x$.

**Definition 48** (Symmetric)**.** A binary relation $\mathbf{R}$ is *symmetric* iff, whenever $x\mathbf{R}y$, then $y\mathbf{R}x$.

**Definition 49** (Transitive)**.** A binary relation $\mathbf{R}$ is *transitive* iff, whenever $x\mathbf{R}y$ and $y\mathbf{R}z$, then $x\mathbf{R}z$.

## 5   $n$-ary Relations

**Definition 50.** Given objects $a$, $b$, $c$, define the *ordered triple* $(a, b, c)$ to be $((a, b), c)$.

Define $(a, b, c, d) = ((a, b, c), d)$, etc.

Define the *1-tuple* $(a)$ to be $a$.

**Definition 51** ($n$-ary Relation)**.** Given a class $\mathbf{A}$, an *$n$-ary relation* on $\mathbf{A}$ is a class of ordered $n$-tuples, all of whose components are in $\mathbf{A}$.

# 6   Functions

**Definition 52** (Function). A *function* is a relation $\mathbf{F}$ such that, for all $x \in \operatorname{dom} \mathbf{F}$, there is only one $y$ such that $x\mathbf{F}y$. We call this unique $y$ the *value* of $\mathbf{F}$ at $x$ and denote it by $\mathbf{F}(x)$.

We say $\mathbf{F}$ is a function *from* $\mathbf{A}$ *into* $\mathbf{B}$, or $\mathbf{F}$ *maps* $\mathbf{A}$ into $\mathbf{B}$, and write $\mathbf{F} : \mathbf{A} \to \mathbf{B}$, iff $\mathbf{F}$ is a function, $\operatorname{dom} \mathbf{F} = \mathbf{A}$, and $\operatorname{ran} \mathbf{F} \subseteq \mathbf{B}$.

If, in addition, $\operatorname{ran} \mathbf{F} = \mathbf{B}$, we say $\mathbf{F}$ is a function from $\mathbf{A}$ *onto* $\mathbf{B}$.

**Theorem 53.** *For a class* $\mathbf{F}$*,* $\mathbf{F}^{-1}$ *is a function if and only if* $\mathbf{F}$ *is single-rooted.*

PROOF: Easy. □

**Theorem 54.** *A relation* $\mathbf{F}$ *is a function if and only if* $\mathbf{F}^{-1}$ *is single-rooted.*

PROOF: Easy. □

**Theorem 55.** *For any function* $\mathbf{G}$ *and classes* $\mathbf{A}$ *and* $\mathbf{B}$*,*

$$\mathbf{G}^{-1}(\bigcup \mathbf{A}) = \bigcup \{\mathbf{G}^{-1}(X) : X \in \mathbf{A}\}$$
$$\mathbf{G}^{-1}(\bigcap \mathbf{A}) = \bigcap \{\mathbf{G}^{-1}(X) : X \in \mathbf{A}\} \qquad (\textit{if } \mathbf{A} \neq \emptyset)$$
$$\mathbf{G}^{-1}(\mathbf{A} - \mathbf{B}) = \mathbf{G}^{-1}(\mathbf{A}) - \mathbf{G}^{-1}(\mathbf{B})$$

PROOF: Easy. □

**Theorem 56.** *Assume that* $\mathbf{F}$ *and* $\mathbf{G}$ *are functions. Then* $\mathbf{F} \circ \mathbf{G}$ *is a function, its domain is* $\{x \in \operatorname{dom} \mathbf{G} : \mathbf{G}(x) \in \operatorname{dom} \mathbf{F}\}$*, and for* $x$ *in its domain,*

$$(\mathbf{F} \circ \mathbf{G})(x) = \mathbf{F}(\mathbf{G}(x)) \ .$$

PROOF: Easy. □

**Definition 57** (One-to-one). A function $\mathbf{F}$ is *one-to-one* or an *injection* iff it is single-rooted.

**Theorem 58.** *Let* $\mathbf{F}$ *be a one-to-one function. For* $x \in \operatorname{dom} \mathbf{F}$*,* $\mathbf{F}^{-1}(\mathbf{F}(x)) = x$*.*

PROOF: Easy. □

**Theorem 59.** *Let* $\mathbf{F}$ *be a one-to-one function. For* $y \in \operatorname{ran} \mathbf{F}$*,* $\mathbf{F}(\mathbf{F}^{-1}(y)) = y$*.*

PROOF: Easy. □

**Definition 60** (Identity Function). For any class $\mathbf{A}$, the *identity* function on $\mathbf{A}$ is $\operatorname{id}_{\mathbf{A}} = \{(x, x) \mid x \in \mathbf{A}\}$.

**Theorem 61.** *Let* $F : A \to B$*. Assume* $A \neq \emptyset$*. Then* $F$ *has a left inverse (i.e. there exists* $G : B \to A$ *such that* $G \circ F = \operatorname{id}_A$*) if and only if* $F$ *is one-to-one.*

PROOF:
$\langle 1 \rangle 1$. If $F$ is one-to-one then $F$ has a left inverse.

$\langle 2 \rangle$1. ASSUME: $F$ is one-to-one.
$\langle 2 \rangle$2. $F^{-1} : \operatorname{ran} F \to A$
$\langle 2 \rangle$3. PICK $a \in A$
$\langle 2 \rangle$4. Define $G : B \to A$ by:
$$G(x) = \begin{cases} F^{-1}(x) & \text{if } x \in \operatorname{ran} F \\ a & \text{if } x \in B - \operatorname{ran} F \end{cases}$$
$\langle 2 \rangle$5. $\forall x \in A.G(F(x)) = x$
$\langle 1 \rangle$2. If $F$ has a left inverse then $F$ is one-to-one.
$\quad$ $\langle 2 \rangle$1. ASSUME: $F$ has a left inverse $G$.
$\quad$ $\langle 2 \rangle$2. LET: $x, y \in A$ with $F(x) = F(y)$
$\quad$ $\langle 2 \rangle$3. $x = y$
$\quad\quad$ PROOF: $x = G(F(x)) = G(F(y)) = y$.
□

**Definition 62** (Binary Operation)**.** A *binary operation* on a set $A$ is a function from $A \times A$ into $A$.

# 7  The Axiom of Choice

**Axiom 63** (Choice)**.** *For any relation $R$ there exists a function $H \subseteq R$ with* $\operatorname{dom} H = \operatorname{dom} R$.

**Theorem 64.** *Let $F : A \to B$. Then $F$ has a right inverse if and only if $F$ maps $A$ onto $B$.*

PROOF:
$\langle 1 \rangle$1. If $F$ has a right inverse then $F$ maps $A$ onto $B$.
$\quad$ PROOF: If $H : B \to A$ is a right inverse, then for any $y$ in $B$, we have $y = F(H(y))$.
$\langle 1 \rangle$2. If $F$ maps $A$ onto $B$ then $F$ has a right inverse.
$\quad$ $\langle 2 \rangle$1. ASSUME: $F$ maps $A$ onto $B$.
$\quad$ $\langle 2 \rangle$2. PICK a function $H$ with $H \subseteq F^{-1}$ and $\operatorname{dom} H = \operatorname{dom} F^{-1}$
$\quad\quad$ PROOF: By the Axiom of Choice.
$\quad$ $\langle 2 \rangle$3. $\operatorname{dom} H = B$
$\quad\quad$ PROOF: $\operatorname{dom} H = \operatorname{dom} F^{-1} = \operatorname{ran} F = B$ by $\langle 2 \rangle$1.
$\quad$ $\langle 2 \rangle$4. For all $y \in B$ we have $F(H(y)) = y$
$\quad\quad$ $\langle 3 \rangle$1. LET: $y \in B$
$\quad\quad$ $\langle 3 \rangle$2. $(y, H(y)) \in F^{-1}$
$\quad\quad$ $\langle 3 \rangle$3. $F(H(y)) = y$
□

# 8  Sets of Functions

**Definition 65.** Let $A$ be a set and $\mathbf{B}$ be a class. Then $\mathbf{B}^A$ is the class of all functions $A \to \mathbf{B}$.

# 9 Dependent Products

**Definition 66.** Let $I$ be a set and $H_i$ a set for all $i \in I$. Define

$$\prod_{i \in I} H_i = \{f : f \text{ is a function}, \operatorname{dom} f = I, \forall i \in I. f(i) \in H_i\} \ .$$

**Theorem 67.** *The Axiom of Choice is equivalent to the statement: For any set $I$ and any function $H$ with domain $I$, if $H(i) \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \emptyset$*

PROOF:
$\langle 1 \rangle 1$. If the Axiom of Choice is true then, for any set $I$ and any function $H$ with domain $I$, if $H(i) \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \emptyset$.
  $\langle 2 \rangle 1$. ASSUME: The Axiom of Choice.
  $\langle 2 \rangle 2$. LET: $I$ be a set.
  $\langle 2 \rangle 3$. LET: $H$ be a function with domain $I$.
  $\langle 2 \rangle 4$. ASSUME: $H(i) \neq \emptyset$ for all $i \in I$.
  $\langle 2 \rangle 5$. LET: $R = \{(i, x) : i \in I, x \in H(i)\}$
  $\langle 2 \rangle 6$. PICK a function $F \subseteq R$ with $\operatorname{dom} F = \operatorname{dom} R$
        PROVE:   $F \in \prod_{i \in I} H(i)$
    PROOF: By the Axiom of Choice.
  $\langle 2 \rangle 7$. $\operatorname{dom} H = I$
    PROOF: We have $\operatorname{dom} R = I$ since for all $i \in I$ there exists $x$ such that $x \in H(i)$.
  $\langle 2 \rangle 8$. $\forall i \in I. F(i) \in H(i)$
    PROOF: Since $iRF(i)$.
$\langle 1 \rangle 2$. If, for any set $I$ and any function $H$ with domain $I$, if $H(i) \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \emptyset$, then the Axiom of Choice is true.
  $\langle 2 \rangle 1$. ASSUME: For any set $I$ and any function $H$ with domain $I$, if $H(i) \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \emptyset$
  $\langle 2 \rangle 2$. LET: $R$ be a relation
  $\langle 2 \rangle 3$. LET: $I = \operatorname{dom} R$
  $\langle 2 \rangle 4$. Define the function $H$ with domain $I$ by: for $i \in I$, $H(i) = \{y : iRy\}$
  $\langle 2 \rangle 5$. $H(i) \neq \emptyset$ for all $i \in I$
  $\langle 2 \rangle 6$. PICK $F \in \prod_{i \in I} H(i)$
    PROOF: By $\langle 2 \rangle 1$
  $\langle 2 \rangle 7$. $F$ is a function
  $\langle 2 \rangle 8$. $F \subseteq R$
    PROOF: For all $i \in I$ we have $F(i) \in H(i)$ and so $iRF(i)$.
  $\langle 2 \rangle 9$. $\operatorname{dom} F = \operatorname{dom} R$
$\square$

# 10 Equivalence Relations

**Definition 68** (Equivalence Relation)**.** An *equivalence relation* on $\mathbf{A}$ is a binary relation on $\mathbf{A}$ that is reflexive on $\mathbf{A}$, symmetric and transitive.

**Theorem 69.** *If* **R** *is a symmetric and transitive relation then* **R** *is an equivalence relation on* fld **R**.

PROOF:
⟨1⟩1. LET: $x \in$ fld **R**
⟨1⟩2. PICK $y$ such that either $x\mathbf{R}y$ or $y\mathbf{R}x$
⟨1⟩3. $x\mathbf{R}y$ and $y\mathbf{R}x$
  PROOF: Since **R** is symmetric.
⟨1⟩4. $x\mathbf{R}x$
  PROOF: Since **R** is transitive.
□

**Definition 70** (Equivalence Class)**.** If **R** is an equivalence relation and $x \in$ fld **R**, the *equivalence class* of $x$ modulo **R** is

$$[x]_\mathbf{R} = \{t : x\mathbf{R}t\} \ .$$

**Lemma 71.** *Assume that* **R** *is an equivalence relation on* **A** *and that* $x$ *and* $y$ *belong to* **A**. *Then*
$$[x]_\mathbf{R} = [y]_\mathbf{R} \ \textit{iff} \ x\mathbf{R}y \ .$$

PROOF:
⟨1⟩1. If $[x]_\mathbf{R} = [y]_\mathbf{R}$ then $x\mathbf{R}y$
  ⟨2⟩1. ASSUME: $[x]_\mathbf{R} = [y]_\mathbf{R}$
  ⟨2⟩2. $y \in [y]_\mathbf{R}$
    PROOF: Since **R** is reflexive on **A**.
  ⟨2⟩3. $y \in [x]_\mathbf{R}$
  ⟨2⟩4. $x\mathbf{R}y$
⟨1⟩2. If $x\mathbf{R}y$ then $[x]_\mathbf{R} = [y]_\mathbf{R}$
  ⟨2⟩1. ASSUME: $x\mathbf{R}y$
  ⟨2⟩2. $[y]_\mathbf{R} \subseteq [x]_\mathbf{R}$
    ⟨3⟩1. LET: $z \in [y]_\mathbf{R}$
    ⟨3⟩2. $y\mathbf{R}z$
    ⟨3⟩3. $x\mathbf{R}z$
      PROOF: Since **R** is transitive.
    ⟨3⟩4. $z \in [x]_\mathbf{R}$
  ⟨2⟩3. $y\mathbf{R}x$
    PROOF: Since **R** is symmetric.
  ⟨2⟩4. $[x]_\mathbf{R} \subseteq [y]_\mathbf{R}$
    PROOF: Similar.
□

**Definition 72** (Partition)**.** A *partition* of a set $A$ is a set $P \subseteq \mathcal{P}A$ such that:

- Every member of $P$ is nonempty.

- Any two distinct members of $P$ are disjoint.

- $A = \bigcup P$

**Theorem 73.** *Let $R$ be an equivalence relation on the set $A$. Then the set of all equivalence classes is a partition of $A$.*

Proof:

⟨1⟩1. Every equivalence class is nonempty.
   Proof: For any $x \in A$ we have $x \in [x]_R$.
⟨1⟩2. Any two distinct equivalence classes are disjoint.
   ⟨2⟩1. Let: $x, y \in A$
   ⟨2⟩2. Assume: $z \in [x]_R \cap [y]_R$
        Prove: $[x]_R = [y]_R$
   ⟨2⟩3. $xRy$
      ⟨3⟩1. $xRz$
      ⟨3⟩2. $yRz$
      ⟨3⟩3. $zRy$
        Proof: By ⟨3⟩2 and symmetry.
      ⟨3⟩4. $xRy$
        Proof: By ⟨3⟩1, ⟨3⟩3 and transitivity.
   ⟨2⟩4. $[x]_R = [y]_R$
      Proof: By Lemma 3N.
⟨1⟩3. $A$ is the union of all the equivalence classes.
   Proof: For any $x \in A$ we have $x \in [x]_R$.
□

**Definition 74** (Quotient Set)**.** If $R$ is an equivalence relation on the set $A$, then the *quotient set $A/R$* is the set of all equivalence classes, and the *natural map* or *canonical map* $\phi : A \to A/R$ is defined by $\phi(x) = [x]_R$.

**Theorem 75.** *Assume that $R$ is an equivalence relation on $A$ and that $F : A \to B$. Assume that $F$ is* compatible *with $R$; that is, whenever $xRy$, then $F(x) = F(y)$. Then there exists a unique $\overline{F} : A/R \to B$ such that $F = \overline{F} \circ \phi$.*

Proof: The unique such $\overline{F}$ is $\{([x], F(x)) : x \in A\}$. □

# 11   Linear Orders

**Definition 76** (Linear Ordering)**.** Let $\mathbf{A}$ be a class. A *linear ordering* or *total ordering* on $\mathbf{A}$ is a relation $\mathbf{R}$ on $\mathbf{A}$ such that:

- $\mathbf{R}$ is transitive.

- $\mathbf{R}$ satisfies *trichotomy* on $\mathbf{A}$; i.e. for any $x, y \in \mathbf{A}$, exactly one of

$$x\mathbf{R}y, x = y, y\mathbf{R}x$$

  holds.

**Theorem 77.** *Let $\mathbf{R}$ be a linear ordering on $\mathbf{A}$.*

  *1. There is no $x$ such that $x\mathbf{R}x$.*

*2. For distinct $x$ and $y$ in $\mathbf{A}$, either $x\mathbf{R}y$ or $y\mathbf{R}x$.*

PROOF: Immediate from trichotomy. □

**Definition 78** (Strictly Monotone Functions)**.** Let $A$ and $B$ be linearly ordered sets. A function $f : A \to B$ is *strictly monotone* iff, for all $x, y \in A$, if $x < y$ then $f(x) < f(y)$.

**Theorem 79.** *Let $A$ and $B$ be linearly ordered sets and $f : A \to B$ be strictly monotone. For all $x, y \in A$, if $f(x) < f(y)$ then $x < y$.*

PROOF: We have $f(x) \neq f(y)$ and $f(y) \not< f(x)$ by trichotomy, hence $x \neq y$ and $y \not< x$ since $f$ is strictly monotone, hence $x < y$ by trichotomy. □

**Theorem 80.** *Every strictly monotone function is injective.*

PROOF: If $f(x) = f(y)$, then we have $f(x) \not< f(y)$ and $f(y) \not< f(x)$ by trichotomy, hence $x \not< y$ and $y \not< x$ since $f$ is strictly monotone, hence $x = y$ by trichotomy. □

# 12 Natural Numbers

**Definition 81** (Successor)**.** The *successor* of a set $a$ is the set $a^+ = a \cup \{a\}$.

**Definition 82** (Inductive)**.** A class $\mathbf{A}$ is *inductive* iff $\emptyset \in \mathbf{A}$ and $\forall a \in \mathbf{A}.a^+ \in \mathbf{A}$.

**Axiom 83** (Infinity)**.** *There exists an inductive set.*

**Definition 84** (Natural Number)**.** A *natural number* is a set that belongs to every inductive set.

We write $\omega$ for the class of all natural numbers.

**Theorem 85.** *The class $\omega$ is a set.*

PROOF: Pick an inductive set $I$ (by the Axiom of Infinity), then apply a Subset Axiom to $I$. □

**Theorem 86.** *The set $\omega$ is inductive, and is a subset of every inductive set.*

PROOF: Easy. □

**Corollary 86.1** (Proof by Induction)**.** *Any inductive subclass of $\omega$ is equal to $\omega$.*

**Theorem 87.** *Every natural number except 0 is the successor of some natural number.*

PROOF: Easy proof by induction. □

**Definition 88** (Peano System)**.** A *Peano system* is a triple $\langle N, S, e \rangle$ consisting of a set $N$, a function $S : N \to N$ and an element $e \in N$ such that:

1. $e \notin \operatorname{ran} S$

2. $S$ is one-to-one

3. Any subset $A \subseteq N$ that contains $e$ and is closed under $S$ equals $N$.

**Definition 89** (Transitive Set). A set $A$ is a *transitive set* iff every member of a member of $A$ is a member of $A$.

**Theorem 90.** *For any transitive set $a$, $\bigcup(a^+) = a$.*

PROOF:

$$\bigcup(a^+) = \bigcup(a \cup \{a\})$$
$$= \bigcup a \cup \bigcup\{a\}$$
$$= \bigcup a \cup a$$
$$= a$$

since $\bigcup a \subseteq a$. $\square$

**Theorem 91.** *Every natural number is a transitive set.*

PROOF:
$\langle 1 \rangle 1.$ 0 is a transitive set.
   PROOF: Vacuous.
$\langle 1 \rangle 2.$ For any natural number $n$, if $n$ is a transitive set then $n^+$ is a transitive set.
   $\langle 2 \rangle 1.$ LET: $n$ be a natural number that is a transitive set.
   $\langle 2 \rangle 2.$ $\bigcup(n^+) \subseteq n^+$
     PROOF: Theorem 90.
$\square$

**Theorem 92.** $\langle \omega, \sigma, 0 \rangle$ *is a Peano system, where $0 = \emptyset$ and $\sigma = \{\langle n, n^+ \rangle : n \in \omega\}$.*

PROOF:
$\langle 1 \rangle 1.$ $0 \notin \operatorname{ran} \sigma$
   PROOF: For any $n \in \omega$ we have $0 \neq n^+$ since $n \in n^+$ and $n \notin 0$.
$\langle 1 \rangle 2.$ $\sigma$ is one-to-one.
   PROOF: If $m^+ = n^+$ then $m = \bigcup(m^+) = \bigcup(n^+) = n$ using Theorems 90 and 91.
$\langle 1 \rangle 3.$ Any subset $A \subseteq \omega$ that contains 0 and is closed under $\sigma$ equals $\omega$.
$\square$

**Theorem 93.** *The set $\omega$ is a transitive set.*

PROOF:
$\langle 1 \rangle 1.$ For every natural number $n$ we have $\forall m \in n.$ $m$ is a natural number.
   $\langle 2 \rangle 1.$ $\forall m \in 0.$ $m$ is a natural number.
     PROOF: Vacuous.

$\langle 2 \rangle 2$. If $n$ is a natural number and $\forall m \in n.\ m$ is a natural number, then $\forall m \in n^+.\ m$ is a natural number.

PROOF: Since if $m \in n^+$ we have either $m \in n$ or $m = n$, and $m$ is a natural number in either case.

☐

**Theorem 94** (Recursion Theorem on $\omega$). *Let $A$ be a set, $a \in A$ and $F : A \to A$. Then there exists a unique function $h : \omega \to A$ such that*

$$h(0) = a \ ,$$

*and for every $n$ in $\omega$,*

$$h(n^+) = F(h(n)) \ .$$

PROOF:

$\langle 1 \rangle 1$. Let us call a function $v$ *acceptable* iff $\operatorname{dom} v \subseteq \omega$, $\operatorname{ran} v \subseteq A$ and:

    1. If $0 \in \operatorname{dom} v$ then $v(0) = a$

    2. For all $n \in \omega$, if $n^+ \in \operatorname{dom} v$ then $n \in \operatorname{dom} v$ and $v(n^+) = F(v(n))$.

$\langle 1 \rangle 2$. LET: $\mathcal{K}$ be the set of acceptable functions.

$\langle 1 \rangle 3$. LET: $h = \bigcup \mathcal{K}$

$\langle 1 \rangle 4$. $h$ is a function.

  $\langle 2 \rangle 1$. LET: $S = \{n \in \omega : \text{for at most one } y, (n, y) \in h\}$

  $\langle 2 \rangle 2$. $S$ is inductive.

    $\langle 3 \rangle 1$. $0 \in S$

      $\langle 4 \rangle 1$. LET: $\langle 0, y_1 \rangle, \langle 0, y_2 \rangle \in h$

      $\langle 4 \rangle 2$. PICK acceptable $v_1$ and $v_2$ such that $v_1(0) = y_1$ and $v_2(0) = y_2$

      $\langle 4 \rangle 3$. $y_1 = a$

      $\langle 4 \rangle 4$. $y_2 = a$

      $\langle 4 \rangle 5$. $y_1 = y_2$

    $\langle 3 \rangle 2$. $\forall k \in S.k^+ \in S$

      $\langle 4 \rangle 1$. LET: $k \in S$

      $\langle 4 \rangle 2$. LET: $(k^+, y_1), (k^+, y_2) \in h$

      $\langle 4 \rangle 3$. PICK acceptable $v_1, v_2$ such that $v_1(k^+) = y_1$ and $v_2(k^+) = y_2$

      $\langle 4 \rangle 4$. $y_1 = F(v_1(k))$

      $\langle 4 \rangle 5$. $f_2 = F(v_2(k))$

      $\langle 4 \rangle 6$. $v_1(k) = v_2(k)$

        $\langle 5 \rangle 1$. $(k, v_1(k)), (k, v_2(k)) \in h$

        $\langle 5 \rangle 2$. Q.E.D.

          PROOF: By $\langle 4 \rangle 1$

      $\langle 4 \rangle 7$. $y_1 = y_2$

  $\langle 2 \rangle 3$. $S = \omega$

$\langle 1 \rangle 5$. $h$ is acceptable.

  $\langle 2 \rangle 1$. If $0 \in \operatorname{dom} h$ then $h(0) = a$

    $\langle 3 \rangle 1$. ASSUME: $0 \in \operatorname{dom} h$

    $\langle 3 \rangle 2$. PICK $v$ acceptable with $v(0) = h(0)$

    $\langle 3 \rangle 3$. $v(0) = a$

13

$\langle 3 \rangle 4$. $h(0) = a$

$\langle 2 \rangle 2$. For all $n \in \omega$, if $n^+ \in \operatorname{dom} h$ then $n \in \operatorname{dom} h$ and $h(n^+) = F(h(n))$

$\quad \langle 3 \rangle 1$. LET: $n \in \omega$ with $n^+ \in \operatorname{dom} h$

$\quad \langle 3 \rangle 2$. PICK $v$ acceptable with $v(n^+) = h(n^+)$

$\quad \langle 3 \rangle 3$. $n \in \operatorname{dom} v$

$\quad \langle 3 \rangle 4$. $v(n) = h(n)$

$\quad \langle 3 \rangle 5$. $h(n^+) = F(h(n))$

$\quad \quad$ PROOF:

$$h(n^+) = v(n^+)$$
$$= F(v(n))$$
$$= F(h(n))$$

$\langle 1 \rangle 6$. $\operatorname{dom} h = \omega$

$\quad \langle 2 \rangle 1$. $0 \in \operatorname{dom} h$

$\quad \quad$ PROOF: Since $\{(0, a)\}$ is an acceptable function.

$\quad \langle 2 \rangle 2$. $\forall n \in \operatorname{dom} h. n^+ \in \operatorname{dom} h$

$\quad \quad \langle 3 \rangle 1$. LET: $n \in \operatorname{dom} h$

$\quad \quad \langle 3 \rangle 2$. PICK an acceptable $v$ such that $n \in \operatorname{dom} v$

$\quad \quad \langle 3 \rangle 3$. ASSUME: w.l.o.g. $n^+ \notin \operatorname{dom} v$

$\quad \quad \langle 3 \rangle 4$. $v \cup \{(n^+, F(v(n)))\}$ is acceptable.

$\langle 1 \rangle 7$. For any acceptable function $h' : \omega \to A$ we have $h' = h$

$\quad \langle 2 \rangle 1$. LET: $h' : \omega \to A$ be acceptable.

$\quad \langle 2 \rangle 2$. $h'(0) = h(0)$

$\quad \quad$ PROOF: $h'(0) = h(0) = a$

$\quad \langle 2 \rangle 3$. $\forall n \in \omega. h'(n) = h(n) \Rightarrow h'(n^+) = h(n^+)$

$\quad \quad$ PROOF: We have $h'(n^+) = F(h'(n)) = F(h(n)) = h(n^+)$.

□

**Theorem 95.** *Let $(N, S, e)$ be a Peano system. Then $(\omega, \sigma, 0)$ is isomorphic to $(N, S, e)$, i.e. there is a function $h$ mapping $\omega$ one-to-one onto $N$ in a way that preserves the successor operation*

$$h(\sigma(n)) = S(h(n))$$

*and the zero element*

$$h(0) = e \ .$$

PROOF:

$\langle 1 \rangle 1$. There exists a function $h$ that satisfies those two conditions.

$\quad$ PROOF: By the Recursion Theorem.

$\langle 1 \rangle 2$. For all $m, n \in \omega$, if $m \neq n$ then $h(m) \neq h(n)$

$\quad \langle 2 \rangle 1$. For all $n \in \omega$, if $n \neq 0$ then $h(n) \neq h(0)$

$\quad \quad \langle 3 \rangle 1$. LET: $n \in \omega$

$\quad \quad \langle 3 \rangle 2$. ASSUME: $n \neq 0$

$\quad \quad \langle 3 \rangle 3$. PICK $p$ such that $n = p^+$

$\quad \quad \langle 3 \rangle 4$. $h(n) \neq h(0)$

$\quad \quad \quad$ PROOF: $h(n) = S(h(p)) \neq e = h(0)$.

$\langle 2 \rangle 2$. For all $m \in \omega$, if $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$ then $\forall n(m^+ \neq n \Rightarrow h(m^+) \neq h(n))$

  $\langle 3 \rangle 1$. LET: $m \in \omega$

  $\langle 3 \rangle 2$. ASSUME: $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$

  $\langle 3 \rangle 3$. LET: $n \in \omega$

  $\langle 3 \rangle 4$. ASSUME: $m^+ \neq n$

    PROVE: $h(m^+) \neq h(n)$

  $\langle 3 \rangle 5$. CASE: $n = 0$

   PROOF: $h(m^+) = S(h(m)) \neq e = h(n)$

  $\langle 3 \rangle 6$. CASE: $n = p^+$

    $\langle 4 \rangle 1$. $m \neq p$

    $\langle 4 \rangle 2$. $h(m) \neq h(p)$

    $\langle 4 \rangle 3$. $S(h(m)) \neq S(h(p))$

    $\langle 4 \rangle 4$. $h(m^+) \neq h(p^+)$

$\langle 1 \rangle 3$. For all $x \in N$, there exists $n \in \omega$ such that $h(n) = x$

 PROOF: An easy induction on $x$.

∎

# 13   Finite Sets

**Definition 96** (Finite). A set is *finite* iff it is equinumerous with a natural number. Otherwise it is infinite.

**Theorem 97.** *No natural number is equinumerous with a proper subset of itself.*

PROOF:

$\langle 1 \rangle 1$. Any injective function $f : 0 \to 0$ has range 0.

 PROOF: Since the only such function is $\emptyset$.

$\langle 1 \rangle 2$. For any natural number $n$, if every injective function $f : n \to n$ has range $n$, then every injective function $f : n^+ \to n^+$ has range $n^+$.

  $\langle 2 \rangle 1$. LET: $n \in \omega$

  $\langle 2 \rangle 2$. ASSUME: Every injective function $f : n \to n$ has range $n$.

  $\langle 2 \rangle 3$. LET: $f : n^+ \to n^+$ be injective.

  $\langle 2 \rangle 4$. Define $g : n \to n$ by

$$g(k) = \begin{cases} f(k) & \text{if } f(k) \in n \\ f(n) & \text{if } f(k) = n \end{cases}$$

  PROOF: If $k \in n$ and $f(k) = n$ then $f(n) \in n$ since $f$ is injective.

  $\langle 2 \rangle 5$. $g$ is injective.

    $\langle 3 \rangle 1$. LET: $i, j \in n$

    $\langle 3 \rangle 2$. ASSUME: $g(i) = g(j)$

    $\langle 3 \rangle 3$. CASE: $f(i) \in n$, $f(j) \in n$

     PROOF: Then $f(i) = f(j)$ so $i = j$

    $\langle 3 \rangle 4$. CASE: $f(i) \in n$, $f(j) \notin n$

     PROOF: Then $f(i) = f(n)$ which is impossible as $f$ is injective.

    $\langle 3 \rangle 5$. CASE: $f(i) \notin n$, $f(j) \in n$

PROOF: Then $f(n) = f(j)$ which is impossible as $f$ is injective.

$\langle 3 \rangle 6$. CASE: $f(i) \notin n$, $f(j) \notin n$

    PROOF: Then $f(i) = f(j) = n$ so $i = j$.

$\langle 2 \rangle 6$. $\operatorname{ran} g = n$

  PROOF: By $\langle 2 \rangle 2$.

$\langle 2 \rangle 7$. $\operatorname{ran} f = n^+$

$\langle 3 \rangle 1$. $\forall k \in n.k \in \operatorname{ran} f$

  PROOF: Since $\operatorname{ran} g \subseteq \operatorname{ran} f$.

$\langle 3 \rangle 2$. $n \in \operatorname{ran} f$

$\langle 4 \rangle 1$. CASE: $f(n) \in n$

$\langle 5 \rangle 1$. PICK $k$ such that $g(k) = f(n)$

$\langle 5 \rangle 2$. $f(k) = n$

$\langle 4 \rangle 2$. CASE: $f(n) = n$

    PROOF: Then $n \in \operatorname{ran} f$.

$\square$

**Corollary 97.1.** *No finite set is equinumerous with a proper subset of itself.*

**Corollary 97.2.** *The set $\omega$ is infinite.*

PROOF: Since the function that maps $n$ to $n + 1$ is a bijection between $\omega$ and the proper subset $\omega - \{0\}$. $\square$

**Corollary 97.3.** *Every finite set is equinumerous with a unique natural number.*

**Lemma 98.** *Let $n$ be a natural number and $C \subseteq n$. Then there exists $m \in n$ such that $C \approx m$.*

PROOF:

$\langle 1 \rangle 1$. For all $C \subseteq 0$, there exists $m \in 0$ such that $C \approx m$.

  PROOF: In this case $C = \emptyset$ and so $C \approx 0$.

$\langle 1 \rangle 2$. Let $n \in \omega$. Assume that, for all $C \subseteq n$, there exists $m \in n$ such that $C \approx m$.

    Let $C \subseteq n^+$. Then there exists $m \in n^+$ such that $C \approx m$.

$\langle 2 \rangle 1$. LET: $n \in \omega$

$\langle 2 \rangle 2$. ASSUME: For all $C \subseteq n$, there exists $m \in n$ such that $C \approx m$.

$\langle 2 \rangle 3$. LET: $C \subseteq n^+$

$\langle 2 \rangle 4$. CASE: $n \in C$

$\langle 3 \rangle 1$. PICK $m \in n$ such that $C - \{n\} \approx m$

$\langle 3 \rangle 2$. $C \approx m^+$

$\langle 2 \rangle 5$. CASE: $n \notin C$

  PROOF: Then $C \subseteq n$ so $C \approx m$ for some $m \in n$.

$\square$

**Corollary 98.1.** *Any subset of a finite set is finite.*

# 14   Cardinal Numbers

**Definition 99** (Cardinality)**.** TODO

**Theorem 100.** *For any sets $A$ and $B$, $|A| = |B|$ if and only if $A \approx B$.*

PROOF: TODO □

**Theorem 101.** *For any finite set $A$, $|A|$ is the natural number such that $A \approx |A|$.*

PROOF: TODO □

**Definition 102.** We write $\aleph_0$ for $|\omega|$.

# 15    Cardinal Arithmetic

**Definition 103** (Addition). Let $\kappa$ and $\lambda$ be any cardinal numbers. Then $\kappa + \lambda = |K \cup L|$, where $K$ and $L$ are any disjoint sets of cardinality $\kappa$ and $\lambda$ respectively.

To show this is well-defined, we must prove that, if $K_1 \approx K_2$, $L_1 \approx L_2$, and $K_1 \cap L_1 = K_2 \cap L_2 = \emptyset$, then $K_1 \cup L_1 \approx K_2 \cup L_2$.

PROOF: Easy.

**Lemma 104.** *For any cardinal number $\kappa$ we have $\kappa + 0 = \kappa$.*

PROOF: Since for any set $K$ we have $K \cup \emptyset = K$.

**Lemma 105.** *For any natural number $n$ we have $n + \aleph_0 = \aleph_0$.*

PROOF: Easy. □

**Lemma 106.**
$$\aleph_0 + \aleph_0 = \aleph_0$$

PROOF: Define $f : (\omega \times \{0\}) \cup (\omega \times \{1\}) \to \omega$ by $f(n, 0) = 2n$ and $f(n, 1) = 2n+1$. Then $f$ is a bijection. □

**Theorem 107.**
$$\kappa + \lambda = \lambda + \kappa$$

PROOF: Easy. □

**Theorem 108.**
$$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$$

PROOF: Easy. □

**Definition 109** (Multiplication). Let $\kappa$ and $\lambda$ be any cardinal numbers. Then $\kappa\lambda = |K \times L|$, where $K$ and $L$ are any sets of cardinality $\kappa$ and $\lambda$ respectively.

It is easy to prove this well-defined.

**Lemma 110.** *For any cardinal number $\kappa$ we have $\kappa 0 = 0$.*

PROOF: For any set $K$ we have $K \times \emptyset = \emptyset$. □

**Lemma 111.** *For any natural number $n$ we have $n\aleph_0 = \aleph_0$.*

Proof: Induction on $n$ using Lemma 106. □

**Lemma 112.**
$$\aleph_0 \aleph_0 = \aleph_0$$

Proof: Define $f : \omega \times \omega \to \omega$ by $f(m, n) = 2^m(2n + 1) - 1$. Then $f$ is a bijection. □

**Lemma 113.**
$$\kappa 1 = \kappa$$

Proof: Easy. □

**Theorem 114.**
$$\kappa \lambda = \lambda \kappa$$

Proof: Easy. □

**Theorem 115.**
$$\kappa(\lambda \mu) = (\kappa \lambda)\mu$$

Proof: Easy. □

**Theorem 116.**
$$\kappa(\lambda + \mu) = \kappa \lambda + \kappa \mu$$

Proof: Easy. □

**Definition 117** (Exponentiation)**.** Let $\kappa$ and $\lambda$ be any cardinal numbers. Then $\kappa^\lambda = |K^L|$, where $K$ and $L$ are any sets of cardinality $\kappa$ and $\lambda$ respectively.

It is easy to prove this well-defined.

**Theorem 118.** *For any cardinal $\kappa$, $\kappa^0 = 1$.*

Proof: For any set $K$, there is only one function $\emptyset \to K$, namely $\emptyset$. □

**Theorem 119.** *For any non-zero cardinal $\kappa$, we have $0^\kappa = 0$.*

Proof: For any nonempty set $K$, there is no function $K \to \emptyset$. □

**Theorem 120.** *For any set $A$, $|\mathcal{P}A| = 2^{|A|}$.*

Proof: Define the bijection $f : \mathcal{P}A \to 2^A$ by $f(S)(a) = 1$ if $a \in S$, 0 if $a \notin S$. □

**Corollary 120.1.** *For any cardinal $\kappa$, we have $\kappa \neq 2^\kappa$.*

**Theorem 121.**
$$\kappa^{\lambda + \mu} = \kappa^\lambda \kappa^\mu$$

Proof: Easy. □

18

**Theorem 122.**
$$(\kappa\lambda)^{\mu} = \kappa^{\mu}\lambda^{\mu}$$

PROOF: Easy. □

**Theorem 123.**
$$(\kappa^{\lambda})^{\mu} = \kappa^{\lambda\mu}$$

PROOF: Easy. □

# 16   Arithmetic

**Lemma 124.** *For any natural numbers $m$ and $n$, we have $m + n^{+} = (m+n)^{+}$.*

PROOF: Easy. □

**Corollary 124.1.** *The union of two finite sets is finite.*

**Lemma 125.** *For any natural numbers $m$ and $n$ we have $mn^{+} = mn + m$.*

PROOF: Easy. □

**Corollary 125.1.** *The Cartesian product of two finite sets is finite.*

**Lemma 126.** *For any natural numbers $m$ and $n$ we have $m^{n^{+}} = m^{n}m$.*

PROOF: Easy. □

**Corollary 126.1.** *If $A$ and $B$ are finite sets then $A^{B}$ is finite.*

# 17   Ordering on the Natural Numbers

**Lemma 127.** *For any natural numbers $m$ and $n$, $m \in n$ if and only if $m^{+} \in n^{+}$.*

PROOF:
$\langle 1 \rangle 1.$ $\forall m, n \in \omega(m \in n \Rightarrow m^{+} \in n^{+})$
$\quad \langle 2 \rangle 1.$ $\forall m \in \omega(m \in 0 \Rightarrow m^{+} \in 0^{+})$
$\quad\quad$ PROOF: Vacuous.
$\quad \langle 2 \rangle 2.$ For all $n \in \omega$, if $\forall m \in n.m^{+} \in n^{+}$ then $\forall m \in n^{+}.m^{+} \in n^{++}$
$\quad\quad \langle 3 \rangle 1.$ LET: $n \in \omega$
$\quad\quad \langle 3 \rangle 2.$ ASSUME: $\forall m \in n.m^{+} \in n^{+}$
$\quad\quad \langle 3 \rangle 3.$ LET: $m \in n^{+}$
$\quad\quad \langle 3 \rangle 4.$ CASE: $m \in n$
$\quad\quad\quad \langle 4 \rangle 1.$ $m^{+} \in n^{+}$
$\quad\quad\quad\quad$ PROOF: By $\langle 3 \rangle 2$
$\quad\quad\quad \langle 4 \rangle 2.$ $m^{+} \in n^{++}$
$\quad\quad \langle 3 \rangle 5.$ CASE: $m = n$
$\quad\quad\quad$ PROOF: $m^{+} = n^{+} \in n^{++}$
$\langle 1 \rangle 2.$ $\forall m, n \in \omega(m^{+} \in n^{+} \Rightarrow m \in n)$

$\langle 2 \rangle$1.  LET: $m, n \in \omega$
$\langle 2 \rangle$2.  ASSUME: $m^+ \in n^+$
$\langle 2 \rangle$3.  $m \in m^+$
$\langle 2 \rangle$4.  $m^+ \in n$ or $m^+ = n$
$\langle 2 \rangle$5.  $m \in n$
   PROOF: If $m^+ \in n$ this follows because $n$ is transitive (Theorem 91).
☐

**Lemma 128.** *For any natural number $n$ we have $n \notin n$.*

PROOF:
$\langle 1 \rangle$1.  $0 \notin 0$
$\langle 1 \rangle$2.  For all $n \in \omega$, if $n \notin n$ then $n^+ \notin n^+$
   $\langle 2 \rangle$1.  LET: $n \in \omega$
   $\langle 2 \rangle$2.  ASSUME: $n^+ \in n^+$
       PROVE:  $n \in n$
   $\langle 2 \rangle$3.  $n^+ \in n$ or $n^+ = n$
   $\langle 2 \rangle$4.  $n \in n^+$
   $\langle 2 \rangle$5.  $n \in n$
      PROOF: If $n^+ \in n$ this follows because $n$ is transitive (Theorem 91).
☐

**Theorem 129** (Trichotomy Law for $\omega$). *For any natural numbers $m$ and $n$, exactly one of*

$$m \in n, m = n, n \in m$$

*holds.*

PROOF:
$\langle 1 \rangle$1.  For any $m, n \in \omega$, at most one of $m \in n$, $m = n$, $n \in m$ holds.
   PROOF: If $m \in n$ and $m = n$ then $m \in m$ contradicting Lemma 128.
   If $m \in n$ and $n \in m$ then $m \in m$ by Theorem 91, contradicting Lemma 128.
$\langle 1 \rangle$2.  For any $m, n \in \omega$, at least one of $m \in n$, $m = n$, $n \in m$ holds.
   $\langle 2 \rangle$1.  For all $n \in \omega$, either $0 \in n$ or $0 = n$
      $\langle 3 \rangle$1.  $0 = 0$
      $\langle 3 \rangle$2.  For all $n \in \omega$, if $0 \in n$ or $0 = n$ then $0 \in n^+$
   $\langle 2 \rangle$2.  For all $m \in \omega$, if $\forall n \in \omega(m \in n \vee m = n \vee n \in m)$ then $\forall n \in \omega(m^+ \in n \vee m^+ = n \vee n \in m^+)$
      $\langle 3 \rangle$1.  LET: $m \in \omega$
      $\langle 3 \rangle$2.  ASSUME: $\forall n \in \omega(m \in n \vee m = n \vee n \in m)$
      $\langle 3 \rangle$3.  LET: $n \in \omega$
      $\langle 3 \rangle$4.  CASE: $m \in n$
        PROOF: Then $m \in n^+$
      $\langle 3 \rangle$5.  CASE: $m = n$
        PROOF: Then $m \in n^+$
      $\langle 3 \rangle$6.  CASE: $n \in m$
        PROOF: Then $n^+ \in m^+$ by Lemma 127 so $n^+ \in m$ or $n^+ = m$.
☐

**Corollary 129.1.** *The relation $\in$ is a linear ordering on $\omega$.*

**Corollary 129.2.** *For any natural numbers $m$ and $n$,*

$$m \in n \Leftrightarrow m \subset n \ .$$

Proof:
⟨1⟩1. Let: $m, n \in \omega$
⟨1⟩2. If $m \in n$ then $m \subset n$.
  ⟨2⟩1. Assume: $m \in n$
  ⟨2⟩2. $m \subseteq n$
    Proof: Theorem 91.
  ⟨2⟩3. $m \neq n$
    Proof: Lemma 128.
⟨1⟩3. If $m \subset n$ then $m \in n$.
  Proof: We have $m \neq n$ and $n \notin m$ by ⟨1⟩2, hence $m \in n$ by trichotomy.
□

**Theorem 130.** *For any natural number $p$, the function that maps $n$ to $n + p$ is strictly monotone. For any natural numbers $m$, $n$ and $p$, we have $m \in n$ if and only if $m + p \in n + p$.*

Proof: We prove that $m \in n \Rightarrow m + p \in n + p$. This is an easy induction on $p$ using Lemma 127. □

**Theorem 131.** *For any non-zero natural number $p$, the function that maps $n$ to $np$ is strictly monotone.*

Proof: Easy induction on $p$ using Theorem 130. □

**Theorem 132** (Strong Induction). *Let $A$ be a subset of $\omega$ and suppose that, for all $n \in \omega$, we have*

$$(\forall m < n.m \in A) \Rightarrow n \in A \ .$$

*Then $A = \omega$.*

Proof: Prove $\forall n \in \omega.\forall m < n.m \in A$ by induction on $n$. □

**Theorem 133** (Well-Ordering of $\omega$). *Every nonempty subset of $\omega$ has a least element.*

Proof: If $A$ is a subset of $\omega$ with no least element, we prove $\forall n \in \omega.n \notin A$ by strong induction on $n$. □

**Corollary 133.1.** *There is no function $f : \omega \to \omega$ such that $f(n + 1) < f(n)$ for every $n$.*

**Lemma 134.** *For any natural numbers $m$ and $n$, we have $m \in n$ if and only if there exists a natural number $p$ such that $n = m + p^+$.*

PROOF:

⟨1⟩1. For all $m$, $p$, we have $m \in m + p^+$

   PROOF: $m = m + 0 \in m + p^+$

⟨1⟩2. For all $m$, $n$, if $m \in n$ then there exists $p$ such that $n = m + p^+$

   ⟨2⟩1. For all $m$, if $m \in 0$ then there exists $p$ such that $0 = m + p^+$

      PROOF: Vacuous.

   ⟨2⟩2. For all $n \in \omega$, if $\forall m \in n.\exists p \in \omega.n = m+p^+$ then $\forall m \in n^+.\exists p \in \omega.n^+ = m + p^+$

      ⟨3⟩1. LET: $n \in \omega$

      ⟨3⟩2. ASSUME: $\forall m \in n.\exists p \in \omega.n = m + p^+$

      ⟨3⟩3. LET: $m \in n^+$

      ⟨3⟩4. CASE: $m \in n$

         ⟨4⟩1. PICK $p$ such that $n = m + p^+$

         ⟨4⟩2. $n^+ = m + p^{++}$

      ⟨3⟩5. CASE: $m = n$

         PROOF: $n^+ = m + 0^+$

□

**Lemma 135.** *For natural numbers $m$, $n$, $p$ and $q$, if $m \in n$ and $p \in q$ then $mp + nq \in mq + np$.*

⟨1⟩1. PICK natural numbers $a$ and $b$ such that $n = m + a^+$ and $q = p + b^+$

   PROOF: Lemma 134.

⟨1⟩2. $mp + nq = mq + np + (a^+ + b)^+$

⟨1⟩3. $mp + nq \in mq + np$

   PROOF: Lemma 134.

# 18   The Integers

**Theorem 136.** *The relation $\sim$ is an equivalence relation on $\omega \times \omega$, where $(m,n) \sim (p,q)$ iff $m + q = n + p$.*

PROOF:

⟨1⟩1. The relation $\sim$ is reflexive on $\omega^2$

   PROOF: For any $m$, $n$, we have $m + n = m + n$ and so $(m,n) \sim (m,n)$.

⟨1⟩2. The relation $\sim$ is symmetric.

   PROOF: If $m + q = n + p$ then $p + n = q + m$.

⟨1⟩3. The relation $\sim$ is transitive.

   ⟨2⟩1. ASSUME: $(m,n) \sim (p,q) \sim (r,s)$

   ⟨2⟩2. $m + q = n + p$

   ⟨2⟩3. $p + s = q + r$

   ⟨2⟩4. $m + p + q + s = n + p + q + r$

   ⟨2⟩5. $m + s = n + r$

      PROOF: By cancellation of addition in $\omega$.

□

**Definition 137.** The set $\mathbb{Z}$ of *integers* is the quotient set $(\omega \times \omega)/\sim$.

**Lemma 138.** *If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$ then $(m + p, n + q) \sim (m' + p', n' + q')$.*

PROOF: Assume $m + n' = m' + n$ and $p + q' = p' + q$. Then $m + p + n' + q' = m' + p' + n + q$. □

**Definition 139** (Addition). Addition $+$ on $\mathbb{Z}$ is the binary operation such that

$$[(m, n)] + [(p, q)] = [(m + p, n + q)]$$

**Theorem 140.** *Addition on $\mathbb{Z}$ is commutative.*

PROOF: From the definition. □

**Theorem 141.** *Addition on $\mathbb{Z}$ is associtative.*

PROOF: Easy. □

**Definition 142** (Zero). The zero in the integers is $0 = [(0, 0)]$.

**Theorem 143.** *For any integer $a$ we have $a + 0 = 0$.*

PROOF: Easy. □

**Theorem 144.** *For any integer $a$, there exists an integer $b$ such that $a + b = 0$.*

PROOF: If $a = [(m, n)]$ take $b = [(n, m)]$. □

**Lemma 145.** *If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$ then $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: $m + n' = m' + n$ and $p + q' = p' + q$
$\langle 1 \rangle 2$. $mp + n'p = m'p + np$
$\langle 1 \rangle 3$. $m'q + nq = mq + n'q$
$\langle 1 \rangle 4$. $mp + mq' = mp' + mq$
$\langle 1 \rangle 5$. $n'p' + n'q = n'p + n'q'$
$\langle 1 \rangle 6$. $mp + n'p + m'q + nq + mp + mq' + n'p' + n'q = m'p + np + mq + n'q + mp' + mq + n'p + n'q'$
$\langle 1 \rangle 7$. $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$
□

**Definition 146** (Multiplication). *Multiplication $\cdot$ is the binary operation on $\mathbb{Z}$* such that
$$[(m, n)][(p, q)] = [(mp + nq, mq + np)]$$

**Theorem 147.** *Multiplication is commutative.*

PROOF: Easy. □

**Theorem 148.** *Multiplication is associative.*

PROOF: Easy. □

**Theorem 149.** *Multiplication is distributive over addition.*

PROOF: Easy. □

**Definition 150.** The integer one is $1 = [(1, 0)]$.

**Theorem 151.** *For any integer $a$ we have $a1 = a$.*

PROOF: Easy. □

**Theorem 152.** $0 \neq 1$

PROOF: Easy. □

**Lemma 153.** *If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$ then $m + q \in p + n$ iff $m' + q' \in p' + n'$.*

PROOF:
$$
\begin{aligned}
m + q \in p + n &\Leftrightarrow m + q + n' + q' \in p + n + n' + q' \\
&\Leftrightarrow m' + n + q + q' \in p' + n + n' + q \\
&\Leftrightarrow m' + q' \in p' + n' \qquad\qquad\qquad \square
\end{aligned}
$$

**Definition 154** (Ordering)**.** The ordering $<$ on $\mathbb{Z}$ is defined by: $[(m, n)] < [(p, q)]$ iff $m + q \in n + p$.

**Theorem 155.** *The relation $<$ is a linear ordering on $\mathbb{Z}$.*

PROOF:
⟨1⟩1. $<$ is transitive.
　　⟨2⟩1. ASSUME: $[(m, n)] < [(p, q)]$ and $[(p, q)] < [(r, s)]$
　　⟨2⟩2. $m + q \in n + p$ and $p + s \in q + r$
　　⟨2⟩3. $m + q + s \in n + p + s$
　　⟨2⟩4. $n + p + s \in n + q + r$
　　⟨2⟩5. $m + q + s \in n + q + r$
　　⟨2⟩6. $m + s \in n + r$
⟨1⟩2. $<$ satisfies trichotomy.
　　PROOF: From trichotomy on $\omega$.
□

**Theorem 156.** *For any integers $a$, $b$ and $c$, we have $a < b$ iff $a + c < b + c$.*

PROOF: An easy consequence of the corresponding property in $\omega$.

**Corollary 156.1.** *If $a + c = b + c$ then $a = b$.*

**Theorem 157.** *If $0 < c$, then the function that maps an integer $a$ to $ac$ is strictly monotone.*

PROOF:
⟨1⟩1. LET: $a$, $b$ and $c$ be integers.
⟨1⟩2. ASSUME: $0 < c$ and $a < b$

⟨1⟩3. LET: $a = [(m, n)]$
⟨1⟩4. LET: $b = [(p, q)]$
⟨1⟩5. LET: $c = [(r, s)]$
⟨1⟩6. $s \in r$
⟨1⟩7. $m + q \in p + n$
⟨1⟩8. $(m + q)r + (p + n)s \in (m + q)s + (p + n)r$
   PROOF: Lemma 135.
⟨1⟩9. $ac < bc$
□

**Lemma 158.** *For integers $a$ and $b$, $a(-b) = -(ab)$*

PROOF: This follows from the fact that $ab + a(-b) = a(b + (-b)) = a0 = 0$. □

**Theorem 159.** *For integers $a$, $b$ and $c$, if $a < b$ and $c < 0$ then $ac > bc$.*

PROOF: We have $0 < -c$ so $a(-c) < b(-c)$ hence $-(ac) < -(bc)$ so $bc < ac$. □

**Theorem 160.** *For any integers $a$ and $b$, if $ab = 0$ then $a = 0$ or $b = 0$.*

PROOF: We prove if $a \neq 0$ and $b \neq 0$ then $ab \neq 0$.
If $a > 0$ and $b > 0$ then $ab > 0$. Similarly for the other four cases. □

**Theorem 161.** *If $ac = bc$ and $c \neq 0$ then $a = b$.*

PROOF: We have $(a - b)c = 0$ so $a - b = 0$ hence $a = b$. □

**Definition 162** (Positive)**.** An integer $a$ is *positive* iff $0 < a$.

**Theorem 163.** *Define $E : \omega \to \mathbb{Z}$ by $E(n) = [(n, 0)]$. Then $E$ maps $\omega$ one-to-one into $\mathbb{Z}$, and:*

1. *$E(m + n) = E(m) + E(n)$*

2. *$E(mn) = E(m)E(n)$*

3. *$m \in n$ if and only if $E(m) < E(n)$.*

PROOF: Routine calculations. □

# 19   Equinumerosity

**Definition 164** (Equinumerous)**.** Two sets $A$ and $B$ are *equinumerous*, $A \approx B$, iff there exists a bijection between them.

**Theorem 165.** *Equinumerosity is an equivalence relation on the class of sets.*

PROOF: Easy. □

**Theorem 166** (Cantor 1873)**.** *No set is equinumerous with its power set.*

PROOF:

$\langle 1 \rangle 1$. LET: $g : A \to \mathcal{P}A$
  PROVE:  $g$ is not surjective.
$\langle 1 \rangle 2$. LET: $B = \{x \in A : x \notin g(x)\}$
$\langle 1 \rangle 3$. $\forall x \in A . g(x) \neq B$
  PROOF: Because $x \in B$ iff $x \notin g(x)$.
$\square$

# 20  Ordering Cardinal Numbers

**Definition 167** (Dominated). A set $A$ is *dominated* by a set $B$, $A \preccurlyeq B$, iff there exists an injection $f : A \to B$.

**Lemma 168.** *Domination is a preorder on the class of sets.*

PROOF: Easy. $\square$

**Lemma 169.** *If $A \subseteq B$ then $A \preccurlyeq B$.*

PROOF: The inclusion from $A$ to $B$ is an injection. $\square$

**Lemma 170.** *If $A \preccurlyeq B$, $A \approx A'$ and $B \approx B'$ then $A' \preccurlyeq B'$.*

PROOF: Easy. $\square$

**Definition 171.** Given cardinal numbers $\kappa$ and $\lambda$, we write $\kappa \leq \lambda$ iff $K \preccurlyeq L$, where $K$ is any set of cardinality $\kappa$ and $L$ is any set of cardinality $\lambda$.
  We write $\kappa < \lambda$ iff $\kappa \leq \lambda$ and $\kappa \neq \lambda$.

**Theorem 172** (Schröder-Bernstein). *If $A \preccurlyeq B$ and $B \preccurlyeq A$ then $A \approx B$.*

PROOF:
$\langle 1 \rangle 1$. LET: $f : A \to B$ and $g : B \to A$ be one-to-one.
$\langle 1 \rangle 2$. Define the sequence of sets $C_n \subseteq A$ by:
$$C_0 = A - \operatorname{ran} g$$
$$C_{n+1} = g(f(C_n))$$
$\langle 1 \rangle 3$. Define $h : A \to B$ by
$$h(x) = \begin{cases} f(x) & \text{if } \exists n \in \mathbb{N}. x \in C_n \\ g^{-1}(x) & \text{otherwise} \end{cases}$$
$\langle 1 \rangle 4$. $h$ is injective.
  $\langle 2 \rangle 1$. LET: $x, y \in A$
  $\langle 2 \rangle 2$. ASSUME: $h(x) = h(y)$
  $\langle 2 \rangle 3$. CASE: $x \in C_m$, $y \in C_n$
    PROOF: We have $f(x) = f(y)$ so $x = y$
  $\langle 2 \rangle 4$. CASE: $x \in C_m$, $y \notin \bigcup_n C_n$
    PROOF: This case is impossible because we would have $y = g(f(x))$ and so $y \in C_{m+1}$.
  $\langle 2 \rangle 5$. CASE: $x, y \notin \bigcup_n C_n$
    PROOF: We have $g^{-1}(x) = g^{-1}(y)$ so $x = y$.

$\langle 1\rangle 5.$ $h$ is surjective.

    $\langle 2\rangle 1.$ LET: $y \in B$

    $\langle 2\rangle 2.$ ASSUME: $y \notin f(C_n)$ for all $n$

    $\langle 2\rangle 3.$ $g(y) \notin C_n$ for all $n$

    $\langle 2\rangle 4.$ $y = h(g(y))$

$\square$