C1 Set Theory

Robin Adams

October 30, 2022

Chapter 1

The Foundations

1.1 Classes

We speak informally of *classes*. A class is determined by a unary predicate. We write $\{x : P(x)\}$ or $\{x \mid P(x)\}$ for the class determined by the predicate $P(x)$.

We define what it means for an object a to be an *element* or *member* of the class $\mathbf{A}$, $a \in \mathbf{A}$, by: $a \in \{x : P(x)\}$ means $P(a)$. In this case we also write $\mathbf{A} \ni a$, and say $\mathbf{A}$ *contains* a.

We write $\{x \in \mathbf{A} : P(x)\}$ for $\{x : x \in \mathbf{A} \wedge P(x)\}$, and $\{t[x_1, \ldots, x_n] : P[x_1, \ldots, x_n]\}$ for $\{y : \exists x_1 \cdots \exists x_n(y = t[x_1, \ldots, x_n] \wedge P[x_1, \ldots, x_n])\}$.

Definition 1.1.1 (Equality of Classes)**.** Two classes $\mathbf{A}$ and $\mathbf{B}$ are *equal*, $\mathbf{A} = \mathbf{B}$, iff they have exactly the same members.

Definition 1.1.2 (Subclass)**.** A class $\mathbf{A}$ is a *subclass* of a class $\mathbf{B}$, $\mathbf{A} \subseteq \mathbf{B}$, iff every member of $\mathbf{A}$ is a member of $\mathbf{B}$. In this case we also write $\mathbf{B} \supseteq \mathbf{A}$, and say $\mathbf{B}$ *includes* $\mathbf{A}$ or $\mathbf{B}$ is a *superclass* of $\mathbf{A}$.

We say $\mathbf{A}$ is a *proper* subclass of the class $\mathbf{B}$, $\mathbf{A} \subset \mathbf{B}$, iff $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{A} \neq \mathbf{B}$. In this case we also write $\mathbf{B} \supset \mathbf{A}$, and say $\mathbf{B}$ *properly* includes $\mathbf{A}$ or $\mathbf{B}$ is a *proper* superclass of $\mathbf{A}$.

Definition 1.1.3 (Disjoint)**.** Two classes $\mathbf{A}$ and $\mathbf{B}$ are *disjoint* iff they have no common members.

Definition 1.1.4 (Empty Class)**.** The *empty class*, $\emptyset$, is $\{x : \bot\}$.

Definition 1.1.5 (Universal Class)**.** The *universal class* $\mathbf{V}$ is the class $\{x : \top\}$.

Definition 1.1.6. For any objects $a_1, \ldots, a_n$, we write $\{a_1, \ldots, a_n\}$ for the class $\{x : x = a_1 \vee \cdots \vee x = a_n\}$.

A class of the form $\{a\}$ is called a *singleton*.

A class of the form $\{a, b\}$ is called a *pair class*.

Definition 1.1.7 (Union)**.** The *union* of classes $\mathbf{A}$ and $\mathbf{B}$, $\mathbf{A} \cup \mathbf{B}$, is the class $\{x : x \in \mathbf{A} \vee x \in \mathbf{B}\}$.

Definition 1.1.8 (Intersection)**.** The *intersection* of classes $\mathbf{A}$ and $\mathbf{B}$, $\mathbf{A} \cap \mathbf{B}$, is the class $\{x : x \in \mathbf{A} \wedge x \in \mathbf{B}\}$.

Definition 1.1.9 (Relative Complement)**.** Given classes $\mathbf{A}$ and $\mathbf{B}$, the *relative complement* $\mathbf{A} - \mathbf{B}$ is the class $\{x \in \mathbf{A} : x \notin \mathbf{B}\}$.

Definition 1.1.10 (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 $\bigcap\{t[x_1, \ldots, x_n] : P[x_1, \ldots, x_n]\}$.

1.2 Primitive Notions

Let there be *sets*.

Let there be a binary relation called *membership*, $\in$.

1.3 The Axiom of Extensionality

Axiom 1.3.1 (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 1.3.2. 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 1.3.3 (Subset)**.** If A is a set and $\mathbf{B}$ is a class, we say A is a *subset* of $\mathbf{B}$ iff $A \subseteq \mathbf{B}$.

If A is a set and $\mathbf{B}$ is a class, we say A is a *superset* of $\mathbf{B}$ iff $A \supseteq \mathbf{B}$.

If A is a set and $\mathbf{B}$ is a class, we say A is a *proper subset* of $\mathbf{B}$ iff $A \subset \mathbf{B}$.

If A is a set and $\mathbf{B}$ is a class, we say A is a *proper superset* of $\mathbf{B}$ iff $A \supset \mathbf{B}$.

Definition 1.3.4 (Power Class)**.** For any class $\mathbf{A}$, the *power class* of $\mathbf{A}$, $\mathcal{P}\mathbf{A}$, is the class of all subsets of $\mathbf{A}$.

Definition 1.3.5 (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 $\bigcup\{t[x_1, \ldots, x_n] : P[x_1, \ldots, x_n]\}$.

1.4 The Zermelo-Fraenkel Axioms

Axiom Schema 1.4.1 (Replacement)**.** *For any property $P(x, y)$, the following is an axiom:*

Let A be a set. Assume that, for all $x \in A$, there is at most one y such that $P(x, y)$. Then $\{y : \exists x \in A. P(x, y)\}$ is a set.

Axiom 1.4.2 (Power Set). *For any set A, the power class $\mathcal{P}A$ is a set.*

Definition 1.4.3 (Power Set). For any set A, we call $\mathcal{P}A$ the *power set* of A.

Axiom 1.4.4 (Union). *For any set A, the union $\bigcup A$ is a set.*

Axiom 1.4.5 (Regularity). *For every nonempty set A, there exists $m \in A$ such that $m \cap A = \emptyset$.*

Axiom 1.4.6 (Infinity). *There exists a nonempty set A such that $\forall x \in A.\exists y \in A.x \subset y$.*

1.5 Constructions of Sets

Theorem Schema 1.5.1. *For any class $\mathbf{A}$ and set B, if $\mathbf{A} \subseteq B$ then $\mathbf{A}$ is a set.*

PROOF:
$\langle 1 \rangle 1$. LET: B be a set.
$\langle 1 \rangle 2$. $(\forall x \in B)\forall y_1, y_2((x \in \mathbf{A} \wedge y_1 = x) \wedge (x \in \mathbf{A} \wedge y_2 = x) \Rightarrow y_1 = y_2)$
$\langle 1 \rangle 3$. $\{y : \exists x \in B(x \in \mathbf{A} \wedge y = x)\}$ is a set.
  PROOF: By a Replacement Axiom.
$\langle 1 \rangle 4$. $\mathbf{A}$ is a set.
$\square$

Theorem 1.5.2 (Empty Set). *The empty class is a set.*

PROOF:
$\langle 1 \rangle 1$. PICK a set a
  PROOF: By the Axiom of Infinity, a set exists.
$\langle 1 \rangle 2$. $\emptyset \subseteq a$
$\langle 1 \rangle 3$. $\emptyset$ is a set.
  PROOF: Theorem Schema 1.5.1.
$\square$

Definition 1.5.3 (Empty Set). Henceforth we call $\emptyset$ the *empty set*.

Theorem 1.5.4 (Pairing). *For any sets a and b, the class $\{a, b\}$ is a set.*

PROOF:Let $P(x, y)$ be the formula $(x = \emptyset \wedge y = a) \vee (x = \mathcal{P}\emptyset \wedge y = b)$. Then we reason:
$\langle 1 \rangle 1$. LET: a and b be sets.
$\langle 1 \rangle 2$. $(\forall x \in \mathcal{P}\mathcal{P}\emptyset)\forall y_1 \forall y_2 (P(x, y_1) \wedge P(x, y_2) \Rightarrow y_1 = y_2)$
  $\langle 2 \rangle 1$. $\emptyset \neq \mathcal{P}\emptyset$
    PROOF: Since $\emptyset \in \mathcal{P}\emptyset$ and $\emptyset \notin \emptyset$.
$\langle 1 \rangle 3$. LET: $A = \{y : \exists x \in \mathcal{P}\mathcal{P}\emptyset.P(x, y)\}$
  PROOF: This is a set by a Replacement Axiom.
$\langle 1 \rangle 4$. $A = \{a, b\}$
  $\langle 2 \rangle 1$. $a \in A$

PROOF: Since $\emptyset \in \mathcal{P}\mathcal{P}\emptyset$.
$\langle 2\rangle 2.$ $b \in A$
PROOF: Since $\mathcal{P}\emptyset \in \mathcal{P}\mathcal{P}\emptyset$.
$\langle 2\rangle 3.$ $\forall x \in A(x = a \vee x = b)$
∎

Proposition 1.5.5. *For any sets A and B, the class $A \cup B$ is a set.*

PROOF: It is $\bigcup\{A, B\}$. ∎

Proposition Schema 1.5.6. *For any objects $a_1, \ldots, a_n$, the class $\{a_1, \ldots, a_n\}$ is a set.*

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

Proposition 1.5.7. *For any set A and class $\mathbf{B}$, the intersection $A \cap \mathbf{B}$ is a set.*

PROOF: By Theorem Schema 1.5.1 since it is a subclass of A. ∎

Proposition 1.5.8. *For any set A and class $\mathbf{B}$, the relative complement $A - \mathbf{B}$ is a set.*

PROOF: By Theorem Schema 1.5.1 since it is a subclass of A. ∎

Proposition 1.5.9. *For any nonempty class of sets $\mathbf{A}$, the intersection $\bigcap \mathbf{A}$ is a set.*

PROOF: Pick $A \in \mathbf{A}$. Then $\bigcap \mathbf{A} \subseteq A$ and the result follows by Theorem 1.5.1. ∎

1.6 Basic Properties

Theorem 1.6.1. *The universal class $\mathbf{V}$ is a proper class.*

PROOF:
$\langle 1\rangle 1.$ ASSUME: $\mathbf{V}$ is a set.
$\langle 1\rangle 2.$ LET: $R = \{x : x \notin x\}$
$\langle 1\rangle 3.$ R is a set.
PROOF: By Theorem 1.5.1.
$\langle 1\rangle 4.$ $R \in R$ if and only if $R \notin R$
$\langle 1\rangle 5.$ Q.E.D.
PROOF: This is a contradiction.
∎

Theorem 1.6.2. *No set is a member of itself.*

PROOF: If $A \in A$ then there is no $m \in \{A\}$ such that $m \cap \{A\} = \emptyset$. ∎

Theorem 1.6.3. *There are no sets a and b with $a \in b$ and $b \in a$.*

PROOF: If there were, then there would be no $m \in \{a, b\}$ such that $m \cap \{a, b\} = \emptyset$. ∎

1.7 The Axiom of Choice

Definition 1.7.1 (Axiom of Choice)**.** The *Axiom of Choice* is the statement:

Let $\mathcal{A}$ be a set such that (a) every member of $\mathcal{A}$ is a nonempty set, and (b) any two distinct members of $\mathcal{A}$ are disjoint. Then there exists a set C such that, for all $B \in \mathcal{A}$, we have $C \cap B$ is a singleton.

Chapter 2

Relations and Functions

2.1 Ordered Pairs

Theorem 2.1.1. *There exists a predicate* $\mathbf{Pair}(x, y, z)$ *such that the following is a theorem:*

1. $\forall x, y \exists! z.\mathbf{Pair}(x, y, z)$
2. $\forall x, y, z, w, p.(\mathbf{Pair}(x, y, p) \wedge \mathbf{Pair}(z, w, p) \Rightarrow x = z \wedge y = w)$

Let $\mathbf{Pair}(x, y, z)$ be the predicate $z = \{\{x\}, \{x, y\}\}$. Proof:
$\langle 1 \rangle 1.$ $\forall x, y \exists! z.\mathbf{Pair}(x, y, z)$
$\langle 1 \rangle 2.$ $\forall a, b, c, d, p.(\mathbf{Pair}(a, b, p) \wedge \mathbf{Pair}(c, d, p) \Rightarrow x = z \wedge y = w)$
  $\langle 2 \rangle 1.$ Assume: $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$
  $\langle 2 \rangle 2.$ $a = c$
    Proof: Since $\{a\} = \bigcap(a, b) = \bigcap(c, d) = \{c\}$.
  $\langle 2 \rangle 3.$ $\{a, b\} = \{c, d\}$
    Proof: $\{a, b\} = \bigcup(a, b) = \bigcup(c, d) = \{c, d\}$.
  $\langle 2 \rangle 4.$ $b = c$ or $b = d$
  $\langle 2 \rangle 5.$ Case: $b = c$
    $\langle 3 \rangle 1.$ $a = b$
    $\langle 3 \rangle 2.$ $\{c, d\} = \{a\}$
    $\langle 3 \rangle 3.$ $b = d$
  $\langle 2 \rangle 6.$ Case: $b = d$
    Proof: We have $a = c$ and $b = d$ as required.

□

Pick a predicate $\mathbf{Pair}(x, y, z)$ such that the following is a theorem:

1. $\forall x, y \exists! z.\mathbf{Pair}(x, y, z)$
2. $\forall x, y, z, w, p.(\mathbf{Pair}(x, y, p) \wedge \mathbf{Pair}(z, w, p) \Rightarrow x = z \wedge y = w)$

Definition 2.1.2 (Ordered Pair)**.** For any objects a and b, the *ordered pair* (a, b) is the object such that $\mathbf{Pair}(a, b, (a, b))$. We call a its *first coordinate* and b its *second coordinate.*

Definition 2.1.3 (Cartesian Product)**.** The *Cartesian product* of classes $\mathbf{A}$ and $\mathbf{B}$ is the class
$$\mathbf{A} \times \mathbf{B} = \{(x, y) : x \in \mathbf{A}, y \in \mathbf{B}\} \ .$$

Theorem 2.1.4. *For any sets A and B, the Cartesian product $A \times B$ is a set.*

PROOF: By an Axiom of Replacement, for all $a \in A$, the class $B_a = \{(a, b) : b \in B\}$ is a set. Hence by an Axiom of Replacement, $\{B_a : a \in A\}$ is a set. Now $A \times B = \bigcup\{B_a : a \in A\}$.

2.2 Relations

Definition 2.2.1 (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 2.2.2 (Domain)**.** The *domain* of a class $\mathbf{R}$ is $\operatorname{dom}\mathbf{R} = \{x : \exists y.(x, y) \in \mathbf{R}\}$.

Definition 2.2.3 (Range)**.** The *range* of a class $\mathbf{R}$ is $\operatorname{ran}\mathbf{R} = \{y : \exists x.(x, y) \in \mathbf{R}\}$.

Definition 2.2.4 (Field)**.** The *field* of a class $\mathbf{R}$ is $\operatorname{fld}\mathbf{R} = \operatorname{dom}\mathbf{R} \cup \operatorname{ran}\mathbf{R}$.

Proposition 2.2.5. *If R is a set then* $\operatorname{dom} R$*,* $\operatorname{ran} R$ *and* $\operatorname{fld} R$ *are sets.*

PROOF: Apply an Axiom of Replacement for $\operatorname{dom} R$ and $\operatorname{ran} R$. $\square$

Definition 2.2.6 (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 2.2.7 (Inverse)**.** The *inverse* of a class $\mathbf{F}$ is the class $\mathbf{F}^{-1} = \{(y, x) \mid (x, y) \in \mathbf{F}\}$.

Definition 2.2.8 (Composition)**.** The *composition* of classes $\mathbf{F}$ and $\mathbf{G}$ is the class $\mathbf{G} \circ \mathbf{F} = \{(x, z) \mid \exists y.(x, y) \in \mathbf{F} \wedge (y, z) \in \mathbf{G}\}$.

Definition 2.2.9 (Restriction)**.** The *restriction* of the class $\mathbf{F}$ to the class $\mathbf{A}$ is the class $\mathbf{F} \upharpoonright \mathbf{A} = \{(x, y) : x \in A \wedge (x, y) \in \mathbf{F}\}$.

Definition 2.2.10 (Image)**.** The *image* of the class $\mathbf{A}$ under the class $\mathbf{F}$ is the class $\mathbf{F}(\mathbf{A}) = \{y : \exists x \in \mathbf{A}.(x, y) \in \mathbf{F}\}$.

Definition 2.2.11 (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 2.2.12 (Ireflexive)**.** A binary relation $\mathbf{R}$ on $\mathbf{A}$ is *irreflexive* on $\mathbf{A}$ if and only if $\forall x \in \mathbf{A}.\neg x\mathbf{R}x$.

Definition 2.2.13 (Symmetric)**.** A binary relation $\mathbf{R}$ is *symmetric* iff, whenever $x\mathbf{R}y$, then $y\mathbf{R}x$.

Definition 2.2.14 (Asymmetric)**.** A binary relation $\mathbf{R}$ is *asymmetric* iff, whenever $x\mathbf{R}y$, then $\neg y\mathbf{R}x$.

Definition 2.2.15 (Antisymmetric)**.** A binary relation $\mathbf{R}$ is *antisymmetric* iff, whenever $x\mathbf{R}y$ and $y\mathbf{R}x$, then $x = y$.

Definition 2.2.16 (Transitive)**.** A binary relation $\mathbf{R}$ is *transitive* iff, whenever $x\mathbf{R}y$ and $y\mathbf{R}z$, then $x\mathbf{R}z$.

Definition 2.2.17 (Minimal)**.** Let R be a relation on D. An element $m \in D$ is *R-minimal* iff there is no $x \in D$ such that xRm.

Definition 2.2.18 (Maximal)**.** Let R be a relation on D. An element $m \in D$ is *R-maximal* iff there is no $x \in D$ such that mRx.

Definition 2.2.19 (Least)**.** Let R be a relation on D. An element $m \in D$ is *least*, *smallest* or the *minimum* iff $\forall x \in D.(mRx \vee m = x)$.

Definition 2.2.20 (Greatest)**.** Let R be a relation on D. An element $m \in D$ is *greatest*, *largest* or the *maximum* iff $\forall x \in D(xRm \vee x = m)$.

2.3 n-ary Relations

Definition 2.3.1. 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 2.3.2 (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 $\mathbf{A}$.

2.4 Functions

Definition 2.4.1 (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 2.4.2. *Let $\mathbf{F}, \mathbf{G} : \mathbf{A} \to \mathbf{B}$. If $\forall x \in \mathbf{A}.\mathbf{F}(x) = \mathbf{G}(x)$ then $\mathbf{F} = \mathbf{G}$.*

PROOF: Easy. □

Theorem 2.4.3. *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 2.4.4 (One-to-one)**.** A function $\mathbf{F}$ is *one-to-one* or an *injection* iff it is single-rooted.

Theorem 2.4.5. *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 2.4.6. *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 2.4.7 (Identity Function)**.** For any class $\mathbf{A}$, the *identity* function on $\mathbf{A}$ is $\mathrm{id}_{\mathbf{A}} = \{(x, x) \mid x \in \mathbf{A}\}$.

Theorem 2.4.8. *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* $G \circ F = \mathrm{id}_A$*) if and only if* F *is one-to-one.*

PROOF:
⟨1⟩1. If F is one-to-one then F has a left inverse.
  ⟨2⟩1. ASSUME: F is one-to-one.
  ⟨2⟩2. $F^{-1} : \operatorname{ran} F \to A$
  ⟨2⟩3. PICK $a \in A$
  ⟨2⟩4. Define $G : B \to A$ by:

$$G(x) = \begin{cases} F^{-1}(x) & \text{if } x \in \operatorname{ran} F \\ a & \text{if } x \in B - \operatorname{ran} F \end{cases}$$

  ⟨2⟩5. $\forall x \in A. G(F(x)) = x$
⟨1⟩2. If F has a left inverse then F is one-to-one.
  ⟨2⟩1. ASSUME: F has a left inverse G.
  ⟨2⟩2. LET: $x, y \in A$ with $F(x) = F(y)$
  ⟨2⟩3. $x = y$
    PROOF: $x = G(F(x)) = G(F(y)) = y$.

□

Definition 2.4.9 (Binary Operation)**.** A *binary operation* on a set A is a function from $A \times A$ into A.

Theorem 2.4.10. *For any function* $F : A \to B$*, if* F *has a right inverse then* F *maps* A *onto* B*.*

PROOF: If $H : B \to A$ is a right inverse, then for any y in B, we have $y = F(H(y))$. □

2.5 Dependent Products

Definition 2.5.1. Let I be a set and H_i a set for all $i \in I$. Define

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

2.6 The Axiom of Choice

Definition 2.6.1 (Choice Function)**.** Let A be a set. A *choice function* for A is a function $F : \mathcal{P}A - \{\emptyset\} \to A$ such that $\forall X \in \mathcal{P}A - \{\emptyset\}.F(X) \in X$.

Theorem 2.6.2. *The following are equivalent.*

1. *The Axiom of Choice.*
2. *Every set has a choice function.*
3. *For any relation R there exists a function $H \subseteq R$ with $\operatorname{dom} H = \operatorname{dom} R$.*
4. *(**Multiplicative Axiom**) 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:
$\langle 1 \rangle 1.$ $1 \Rightarrow 2$
  $\langle 2 \rangle 1.$ ASSUME: the Axiom of Choice
  $\langle 2 \rangle 2.$ LET: A be a set.
  $\langle 2 \rangle 3.$ LET: $\mathcal{A} = \{\{B\} \times B : B \in \mathcal{P}A - \{\emptyset\}\}$
  $\langle 2 \rangle 4.$ PICK a set C such that $C \cap (\{B\} \times B)$ is a singleton for all $B \in \mathcal{P}A - \{\emptyset\}$
  $\langle 2 \rangle 5.$ LET: $F = C \cap \bigcup \mathcal{A}$
  $\langle 2 \rangle 6.$ $F : \mathcal{P}A - \{\emptyset\} \to A$ is a function and $F(X) \in X$ for all X
$\langle 1 \rangle 2.$ $2 \Rightarrow 3$
  $\langle 2 \rangle 1.$ ASSUME: 3
  $\langle 2 \rangle 2.$ LET: R be a relation
  $\langle 2 \rangle 3.$ PICK a choice function G for $\operatorname{ran} R$
  $\langle 2 \rangle 4.$ Define $F : \operatorname{dom} R \to \operatorname{ran} R$ by $F(x) = G(R(x))$
  $\langle 2 \rangle 5.$ $F \subseteq R$
$\langle 1 \rangle 3.$ $3 \Rightarrow 4$
  $\langle 2 \rangle 1.$ ASSUME: 2
  $\langle 2 \rangle 2.$ 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 $\langle 2 \rangle 1$.
  $\langle 2 \rangle 7.$ $\operatorname{dom} H = I$
   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 $iRF(i)$.
$\langle 1 \rangle 4.$ $4 \Rightarrow 1$
  PROOF: Let $\mathcal{A}$ be a set matching the two condtions. By the Multiplicative Axiom, pick a function $f \in \prod_{B \in \mathcal{A}} B$. Let $C = \operatorname{ran} f$. Then $C \cap B = \{f(B)\}$ for all $B \in \mathcal{A}$.

∎

Theorem 2.6.3. *The Axiom of Choice is equivalent to the statement: for any sets A and B and every fuction F that maps A onto B, F has a right inverse.*

PROOF:
⟨1⟩1. If the Axiom of Choice is true and F maps A onto B then F has a right inverse.
  ⟨2⟩1. ASSUME: The Axiom of Choice
  ⟨2⟩2. ASSUME: F maps A onto B.
  ⟨2⟩3. PICK a function H with $H \subseteq F^{-1}$ and $\operatorname{dom} H = \operatorname{dom} F^{-1}$
   PROOF: By the Axiom of Choice.
  ⟨2⟩4. $\operatorname{dom} H = B$
   PROOF: $\operatorname{dom} H = \operatorname{dom} F^{-1} = \operatorname{ran} F = B$ by ⟨2⟩2.
  ⟨2⟩5. For all $y \in B$ we have $F(H(y)) = y$
   ⟨3⟩1. LET: $y \in B$
   ⟨3⟩2. $(y, H(y)) \in F^{-1}$
   ⟨3⟩3. $F(H(y)) = y$
⟨1⟩2. If, for any sets A and B, any function F from A onto B has a right inverse, then the Axiom of Choice is true.
  ⟨2⟩1. ASSUME: For any sets A and B, any function F from A onto B has a right inverse.
  ⟨2⟩2. LET: R be any relation.
  ⟨2⟩3. LET: $F : R \to \operatorname{dom} R$ be the function $F(x, y) = x$
  ⟨2⟩4. F maps R onto $\operatorname{dom} R$
  ⟨2⟩5. PICK a right inverse $G : \operatorname{dom} R \to R$ to F.
  ⟨2⟩6. LET: $H = \{(x, y) : (x, (x, y)) \in G\}$
  ⟨2⟩7. H is a function
  ⟨2⟩8. $H \subseteq R$
  ⟨2⟩9. $\operatorname{dom} H = \operatorname{dom} R$
∎

2.7 Sets of Functions

Definition 2.7.1. Let A be a set and $\mathbf{B}$ be a class. Then $\mathbf{B}^A$ is the class of all functions $A \to \mathbf{B}$.

Theorem 2.7.2. *If A and B are sets then B^A is a set.*

PROOF: Since it is a subset of $\mathcal{P}(A \times B)$. ∎

2.8 Equivalence Relations

Definition 2.8.1 (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 2.8.2. *If* $\mathbf{R}$ *is a symmetric and transitive relation then* $\mathbf{R}$ *is an equivalence relation on* $\operatorname{fld}\mathbf{R}$.

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

Definition 2.8.3 (Equivalence Class)**.** If $\mathbf{R}$ is an equivalence relation and $x \in \operatorname{fld}\mathbf{R}$, the *equivalence class* of x modulo $\mathbf{R}$ is

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

Lemma 2.8.4. *Assume that* $\mathbf{R}$ *is an equivalence relation on* $\mathbf{A}$ *and that* x *and* y *belong to* $\mathbf{A}$. *Then*

$$[x]_{\mathbf{R}} = [y]_{\mathbf{R}} \textit{ iff } x\mathbf{R}y \enspace .$$

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

Definition 2.8.5 (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 2.8.6. *Let A be a set.*

For any equivalence relation R on the set A, the set of all equivalence classes is a partition of A.

Conversely, for any partition P, there exists a unique equivalence relation $\sim$ on A such that P is the set of all equivalence classes with respect to $\sim$, given by $x \sim y$ iff $\exists X \in P(x \in X \wedge y \in X)$.

PROOF:

⟨1⟩1. For every equivalence relation R on A, the set of equivalence classes forms a partition of A.

⟨2⟩1. LET: R be an equivalence relation on A.

⟨2⟩2. Every equivalence class is nonempty.

PROOF: For any $x \in A$ we have $x \in [x]_R$.

⟨2⟩3. Any two distinct equivalence classes are disjoint.

⟨3⟩1. LET: $x, y \in A$

⟨3⟩2. ASSUME: $z \in [x]_R \cap [y]_R$
PROVE: $[x]_R = [y]_R$

⟨3⟩3. xRy

⟨4⟩1. xRz

⟨4⟩2. yRz

⟨4⟩3. zRy

PROOF: By ⟨4⟩2 and symmetry.

⟨4⟩4. xRy

PROOF: By ⟨4⟩1, ⟨4⟩3 and transitivity.

⟨3⟩4. $[x]_R = [y]_R$

PROOF: By Lemma 3N.

⟨2⟩4. A is the union of all the equivalence classes.

PROOF: For any $x \in A$ we have $x \in [x]_R$.

⟨1⟩2. For any partition P, there exists a unique equivalence relation $\sim$ on A such that P is the set of all equivalence classes with respect to $\sim$, given by $x \sim y$ iff $\exists X \in P(x \in X \wedge y \in X)$.

⟨2⟩1. LET: P be a partition of A.

⟨2⟩2. LET: $\sim = \{(x, y) \in A^2 : \exists X \in P(x \in X \wedge y \in X)\}$

⟨2⟩3. $\sim$ is an equivalence relation on A.

⟨3⟩1. $\sim$ is reflexive.

⟨4⟩1. LET: $x \in A$

⟨4⟩2. There exists $X \in P$ such that $x \in X$

PROOF: Since $P = \bigcup A$

⟨4⟩3. $x \sim x$

PROOF: Since $\exists X \in P(x \in X \wedge x \in X)$.

⟨3⟩2. $\sim$ is symmetric.

PROOF: From the definition of $\sim$.

⟨3⟩3. $\sim$ is transitive.

⟨4⟩1. LET: $x, y, z \in A$

⟨4⟩2. ASSUME: $x \sim y$ and $y \sim z$

⟨4⟩3. PICK $X, Y \in P$ such that $x \in X$, $y \in X$, $y \in Y$ and $z \in Y$

$\langle 4 \rangle 4.$ $X = Y$

PROOF: Since the elements of P are pairwise disjoint.

$\langle 4 \rangle 5.$ $x \in X$ and $z \in X$

$\langle 4 \rangle 6.$ $x \sim z$

$\langle 2 \rangle 4.$ P is the set of $\sim$-equivalence classes.

$\langle 3 \rangle 1.$ $\forall X \in P . \forall x \in X . X = [x]_\sim$

$\langle 4 \rangle 1.$ LET: $X \in P$

$\langle 4 \rangle 2.$ LET: $x \in X$

$\langle 4 \rangle 3.$ $X \subseteq [x]_\sim$

$\langle 5 \rangle 1.$ LET: $y \in X$

$\langle 5 \rangle 2.$ $x \sim y$

$\langle 5 \rangle 3.$ $y \in [x]_\sim$

$\langle 4 \rangle 4.$ $[x]_\sim \subseteq X$

$\langle 5 \rangle 1.$ LET: $y \in [x]_\sim$

$\langle 5 \rangle 2.$ PICK $Y \in P$ such that $x \in Y$ and $y \in Y$

$\langle 5 \rangle 3.$ $X = Y$

PROOF: Since $x \in X$, $x \in Y$ and the elements of P are pairwise disjoint.

$\langle 5 \rangle 4.$ $y \in X$

$\langle 3 \rangle 2.$ $\forall X \in P . \exists x \in A . X = [x]_\sim$

$\langle 4 \rangle 1.$ LET: $X \in P$

$\langle 4 \rangle 2.$ PICK $x \in X$

PROOF: Since the elements of P are nonempty.

$\langle 4 \rangle 3.$ $X = [x]_\sim$

PROOF: From $\langle 3 \rangle 1$

$\langle 3 \rangle 3.$ $\forall x \in A . [x]_\sim \in P$

$\langle 4 \rangle 1.$ LET: $x \in A$

$\langle 4 \rangle 2.$ PICK $X \in P$ such that $x \in X$

$\langle 4 \rangle 3.$ $X = [x]_\sim$

PROOF: From $\langle 3 \rangle 1$

$\langle 2 \rangle 5.$ For any equivalence relation R on A, if P is the set of R-equivalence classes, then $R = \sim$.

$\langle 3 \rangle 1.$ LET: R be an equivalence relation on A

$\langle 3 \rangle 2.$ ASSUME: P is the set of R-equivalence classes.

$\langle 3 \rangle 3.$ $R \subseteq \sim$

$\langle 4 \rangle 1.$ LET: xRy

$\langle 4 \rangle 2.$ $[x]_R \in X$ and $x, y \in [x]_R$

$\langle 4 \rangle 3.$ $x \sim y$

$\langle 3 \rangle 4.$ $\sim \subseteq R$

$\langle 4 \rangle 1.$ LET: $x \sim y$

$\langle 4 \rangle 2.$ PICK $X \in P$ such that $x \in X$ and $y \in X$

$\langle 4 \rangle 3.$ PICK $z \in A$ such that $X = [z]_R$

$\langle 4 \rangle 4.$ zRx and zRy

$\langle 4 \rangle 5.$ xRy

$\square$

Definition 2.8.7 (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 2.8.8. *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 $\{([x], F(x)) : x \in A\}$. □

2.9 Well-Founded Relations

Definition 2.9.1 (Well Founded)**.** A relation R on a class D is *well-founded* iff every nonempty subset of D has an R-minimal element.

Theorem 2.9.2 (Transfinite Induction)**.** *Let R be a well-founded relation on A. Let $B \subseteq A$. Assume that, for all $x \in A$, if $\forall y \in A(yRx \Rightarrow y \in B)$, then $x \in B$. Then $B = A$.*

PROOF: If not, $A - B$ has an R-minimal element a_0, say. But then we have $\forall y.(yRa_0 \Rightarrow y \in B)$ and $a_0 \notin B$, which is a contradiction. □

Theorem 2.9.3 (Transfinite Recursion Theorem Schema)**.** *For any property $P(x, y, z)$ the following is a theorem:*

Assume that $<$ is a well-founded relation on A. Assume that $\forall x, y \exists! z P(x, y, z)$. Then there exists a unique function F with domain A such that

$$\forall t \in A.P(F \upharpoonright \operatorname{seg} t, t, F(t)) \enspace .$$

PROOF:

⟨1⟩1. Given $t \in A$, let us say that a function v is *P-constructed up to t* iff $\operatorname{dom} v = \{x \in A : x \leq t\}$ and $\forall x \in \operatorname{dom} v.P(v \upharpoonright \operatorname{seg} x, x, v(x))$

⟨1⟩2. Let $t_1, t_2 \in A$ with $t_1 \leq t_2$. Let v_1 be a function that is P-constructed up to t_1, and v_2 a function that is P-constructed up to t_2. Then $\forall x \leq t_1.v_1(x) = v_2(x)$

⟨2⟩1. LET: $x \leq t_1$

⟨2⟩2. ASSUME: $\forall y < x.v_1(y) = v_2(y)$

⟨2⟩3. $v_1 \upharpoonright \operatorname{seg} x = v_2 \upharpoonright \operatorname{seg} x$

⟨2⟩4. $P(v_1 \upharpoonright \operatorname{seg} x, v_1(x))$

⟨2⟩5. $P(v_2 \upharpoonright \operatorname{seg} x, v_2(x))$

⟨2⟩6. $v_1(x) = v_2(x)$

PROOF: Since there is only one y such that $P(v_1 \upharpoonright \operatorname{seg} x, x, y)$.

⟨2⟩7. Q.E.D.

PROOF: By transfinite induction.

⟨1⟩3. LET: $\mathcal{H} = \{v : \exists t \in A.v \text{ is } P\text{-constructed up to } t\}$

⟨1⟩4. $\mathcal{H}$ is a set.

PROOF: By a Replacement Axiom since, if v_1 and v_2 are both P-constructed up to t then $v_1 = v_2$ by ⟨1⟩2.

$\langle 1\rangle 5.$ LET: $F = \bigcup \mathcal{H}$
$\langle 1\rangle 6.$ F is a function
  $\langle 2\rangle 1.$ ASSUME: tFx and tFy
  $\langle 2\rangle 2.$ PICK $v_1, v_2 \in \mathcal{H}$ such that $v_1(t) = x$ and $v_2(t) = y$
  $\langle 2\rangle 3.$ PICK $t_1, t_2 \in A$ such that v_1 is P-constructed up to t_1 and v_2 is P-constructed up to t_2
  $\langle 2\rangle 4.$ ASSUME: w.l.o.g. $t_1 \leq t_2$
  $\langle 2\rangle 5.$ $v_1(t) = v_2(t)$
  PROOF: By $\langle 1\rangle 2$
  $\langle 2\rangle 6.$ $x = y$
$\langle 1\rangle 7.$ $\forall x \in \operatorname{dom} F. P(F \upharpoonright \operatorname{seg} x, x, F(x))$
  $\langle 2\rangle 1.$ LET: $x \in \operatorname{dom} F$
  $\langle 2\rangle 2.$ PICK $v \in \mathcal{H}$ such that $x \in \operatorname{dom} v$
  $\langle 2\rangle 3.$ $P(v \upharpoonright \operatorname{seg} x, x, v(x))$
  $\langle 2\rangle 4.$ $v \upharpoonright \operatorname{seg} x = F \upharpoonright \operatorname{seg} x$
  PROOF: $\forall y < x.(y, v(y)) \in \bigcup \mathcal{H} = F$
  $\langle 2\rangle 5.$ $v(x) = F(x)$
  PROOF: $(x, v(x)) \in \bigcup \mathcal{H} = F$
$\langle 1\rangle 8.$ $\operatorname{dom} F = A$
  $\langle 2\rangle 1.$ LET: $x \in A$
  $\langle 2\rangle 2.$ ASSUME: $\forall y < x. y \in \operatorname{dom} F$
  $\langle 2\rangle 3.$ LET: z be the object such that $P(F \upharpoonright \operatorname{seg} x, z)$
  $\langle 2\rangle 4.$ $F \upharpoonright \operatorname{seg} x \cup \{(x, z)\}$ is P-constructed up to x
  $\langle 2\rangle 5.$ $x \in \operatorname{dom} F$
  $\langle 2\rangle 6.$ Q.E.D.
  PROOF: By transfinite induction, this proves $\forall x \in A. x \in \operatorname{dom} F$.
$\langle 1\rangle 9.$ F is unique.
  $\langle 2\rangle 1.$ LET: G be a function with domain A such that $\forall x \in A. P(G \upharpoonright \operatorname{seg} x, x, G(x))$
  PROVE: $\forall x \in A. F(x) = G(x)$
  $\langle 2\rangle 2.$ LET: $x \in A$
  $\langle 2\rangle 3.$ ASSUME: $\forall y < x. F(y) = G(y)$
  $\langle 2\rangle 4.$ $F \upharpoonright \operatorname{seg} x = G \upharpoonright \operatorname{seg} x$
  $\langle 2\rangle 5.$ $F(x) = G(x)$
  $\langle 2\rangle 6.$ Q.E.D.
  PROOF: This completes the proof by transfinite induction.
$\square$

2.10 Transitive Closure

Theorem 2.10.1. *For any relation R on a set A, there exists a least transitive relation R^t such that $R \subseteq R^t$.*

PROOF: Define R^t to be the intersection of all the transitive relations Q such that $R \subseteq Q$. $\square$

Theorem 2.10.2. *The transitive closure of a well-founded relation is well-founded.*

PROOF: The R-minimal element of a nonempty set B is also the R^t-minimal element. □

Chapter 3

Order Theory

3.1 Partial Orders

Definition 3.1.1 (Strict Partial Order)**.** A *strict partial order* is an irreflexive, transitive relation.

If $<$ is a strict partial order, we write $x \leq y$ for $x < y \vee x = y$.

Theorem 3.1.2. *Assume that $<$ is a partial order. Then for any x, y and z:*

1. At most *one of the three alternatives,*
$$x < y, x = y, y < x,$$
can hold.
2. $x \leq y \leq x \Rightarrow x = y$.

PROOF: Easy. □

Proposition 3.1.3. *If R is a partial ordering on D then so is R^{-1}.*

PROOF: Easy. □

Definition 3.1.4 (Upper Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. An *upper bound* for C is an element $b \in A$ such that $\forall x \in C. x \leq b$.

Definition 3.1.5 (Least Upper Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. The *least upper bound* or *supremum* for C is the least element in the set of upper bounds for C.

Definition 3.1.6 (Lower Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. A *lower bound* for C is an element $b \in A$ such that $\forall x \in C. b \leq x$.

Definition 3.1.7 (Greatest Lower Bound)**.** Let $<$ be a partial order on A and $C \subseteq A$. The *greatest lower bound* or *infimum* for C is the greatest element in the set of lower bounds for C.

Definition 3.1.8 (Initial Segment)**.** Let $<$ be a partial order on A and $t \in A$. The *initial segment* up to t is

$$\operatorname{seg} t = \{x \in A : x < t\} \ .$$

Definition 3.1.9 (Isomorphism)**.** Let A and B be posets. An *isomorphism* between A and B is a bijection f between A and B such that, for all $x, y \in A$, we have $x < y$ if and only if $f(x) < f(y)$.

Proposition 3.1.10. *Isomorphism is an equivalence relation on the class of posets.*

PROOF: Easy. □

Proposition 3.1.11. *Let $(A, <)$ be a poset and $B \subseteq A$. Then $< \cap B^2$ is a partial order on B.*

PROOF: Easy. □

Theorem 3.1.12. *Let R be a well-founded relation on A. The transitive closure of R is a partial order on A.*

PROOF: It is well founded, hence irreflexive. □

Definition 3.1.13. Let P and Q be partial orders and $f : P \to Q$. Then f is *increasing* iff, whenever $x \leq y$, then $f(x) \leq f(y)$.

Definition 3.1.14. Let P and Q be partial orders and $f : P \to Q$. Then f is *strictly increasing* iff, whenever $x < y$, then $f(x) < f(y)$.

Definition 3.1.15. Let P and Q be partial orders and $f : P \to Q$. Then f is *decreasing* iff, whenever $x \leq y$, then $f(x) \geq f(y)$.

Definition 3.1.16. Let P and Q be partial orders and $f : P \to Q$. Then f is *strictly decreasing* iff, whenever $x < y$, then $f(x) > f(y)$.

Definition 3.1.17. Let P and Q be partial orders and $f : P \to Q$. Then f is *monotone* iff it is either increasing or decreasing.

Definition 3.1.18 (Open Interval)**.** Let P be a poset and $a, b \in P$ with $a < b$. The *open interval* (a, b) is the set $\{x \in P : a < x < b\}$.

The *open interval* $(a, +\infty)$ is the set $\{x \in P : a < x\}$.

The *open interval* $(-\infty, a)$ is the set $\{x \in P : x < a\}$.

Definition 3.1.19 (Closed Interval)**.** Let P be a poset and $a, b \in P$ with $a < b$. The *open interval* $[a, b]$ is the set $\{x \in P : a \leq x \leq b\}$.

The *closed interval* $[a, +\infty)$ is the set $\{x \in P : a \leq x\}$.

The *closed interval* $(-\infty, a]$ is the set $\{x \in P : x \leq a\}$.

Definition 3.1.20 (Half-Open Interval)**.** Let P be a poset and $a, b \in P$ with $a < b$. The *half-open intervals* $[a, b)$ and $(a, b]$ are defined by

$$[a, b) = \{x \in P : a \leq x < b\}$$
$$(a, b] = \{x \in O : a < x \leq b\}$$

Definition 3.1.21 (Interval)**.** Let P be a poset. The *intervals* in P are the sets of the following forms:

- $\emptyset$
- a singleton
- P
- the open intervals
- the closed intervals
- the half-open intervals

3.2 Linear Orders

Definition 3.2.1 (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 3.2.2. *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. $\square$

Definition 3.2.3 (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 3.2.4. *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 $f(y) \nless f(x)$ by trichotomy, hence $x \neq y$ and $y \nless x$ since f is strictly monotone, hence $x < y$ by trichotomy. $\square$

Theorem 3.2.5. *Every strictly monotone function is injective.*

Proof: If $f(x) = f(y)$, then we have $f(x) \nless f(y)$ and $f(y) \nless f(x)$ by trichotomy, hence $x \nless y$ and $y \nless x$ since f is strictly monotone, hence $x = y$ by trichotomy. $\square$

Proposition 3.2.6. *Let* $(A, <)$ *be a linearly ordered set and* $B \subseteq A$. *Then* $< \cap B^2$ *is a linear order on* B.

PROOF: Easy. □

Definition 3.2.7. Let A and B be disjoint linearly ordered sets. The *concatenation* of A and B, $A \oplus B$, is the set $A \cup B$ under the order given by: $x < y$ iff

- $x, y \in A$ and $x < y$; or
- $x, y \in B$ and $x < y$; or
- $x \in A$ and $y \in B$.

It is easy to check this is a linear ordering.

Proposition 3.2.8.

$$A \oplus (B \oplus C) = (A \oplus B) \oplus C$$

PROOF: Easy. □

Proposition 3.2.9.

$$A \oplus \emptyset = \emptyset \oplus A = A$$

PROOF: Easy. □

Definition 3.2.10. Let A and B be linearly ordered sets. The *lexicographic order* on $A \times B$ is defined by: $(a_1, b_1) < (a_2, b_2)$ iff $a_1 < a_2$ or ($a_1 = a_2$ and $b_1 < b_2$).

Proposition 3.2.11. *These two orders on* $A \times B \times C$ *are equal:*

- *lexicographic order formed from (lexicographic order on* $A \times B$*) and order on* C
- *lexicographic order formed from order on* A *and (lexicographic order on* $B \times C$*)*

PROOF: Easy. □

Proposition 3.2.12.

$$A \times 1 = 1 \times A = A$$

PROOF: Easy. □

Proposition 3.2.13. $A \times (B \oplus C) = (A \times B) \oplus (A \times C)$

PROOF: Easy. □

3.3 Well Orderings

Definition 3.3.1 (Well Ordering)**.** A *well ordering* on a set A is a linear ordering on A such that every nonempty subset of A has a least element.

Theorem 3.3.2. *Assume that $<$ is a linear ordering on A. Assume that the only $<$-inductive subset of A is A itself. Then $<$ is a well ordering on A.*

PROOF:
$\langle 1\rangle 1.$ ASSUME: for a contradiction $B \subseteq A$ has no least element.
$\langle 1\rangle 2.$ $A - B$ is $<$-inductive.
  $\langle 2\rangle 1.$ LET: $t \in A$
  $\langle 2\rangle 2.$ ASSUME: $\operatorname{seg} t \subseteq A - B$
  $\langle 2\rangle 3.$ $t \notin B$
    PROOF: If it were, it would be the least element of B.
  $\langle 2\rangle 4.$ $t \in A - B$
$\langle 1\rangle 3.$ $A - B = A$
$\langle 1\rangle 4.$ $B = \emptyset$
□

Proposition 3.3.3. *Let $(A, <)$ be a well ordered set and $B \subseteq A$. Then $< \cap B^2$ is a well order on B.*

PROOF: Easy. □

Theorem 3.3.4. *Let A and B be well-ordered sets. Then one of the following holds:*

- $A \cong B$
- $\exists b \in B. A \cong \operatorname{seg} b$
- $\exists a \in A. \operatorname{seg} a \cong B$

PROOF:
$\langle 1\rangle 1.$ PICKe that is not a member of A or B
$\langle 1\rangle 2.$ Define $F : A \to B \cup \{e\}$ by:
$$F(t) = \begin{cases} \text{the least element of } B - F(\operatorname{seg} t) & \text{if } B - F(\operatorname{seg} t) \neq \emptyset \\ e & \text{if } B - F(\operatorname{seg} t) = \emptyset \end{cases}$$
$\langle 1\rangle 3.$ CASE: $e \in \operatorname{ran} F$
  $\langle 2\rangle 1.$ LET: $a \in A$ be least such that $B - F(\operatorname{seg} a) = \emptyset$
  $\langle 2\rangle 2.$ $F \upharpoonright \operatorname{seg} a : \operatorname{seg} a \cong B$
$\langle 1\rangle 4.$ CASE: $\operatorname{ran} F = B$
  PROOF: In this case $F : A \cong B$.
$\langle 1\rangle 5.$ CASE: $\operatorname{ran} F \subset B$
  $\langle 2\rangle 1.$ LET: $b \in B$ be least such that $b \notin \operatorname{ran} F$
  $\langle 2\rangle 2.$ $F : A \cong \operatorname{seg} b$
□

Theorem 3.3.5. *The concatenation of two well-orderings is a well ordering.*

PROOF: Easy. □

Theorem 3.3.6. *The lexicographic ordering on the product of two well-ordered sets is a well ordering.*

PROOF: Easy. □

Chapter 4

Ordinal Numbers

Theorem 4.0.1. *There exists a function* **Ord** *from the class of all well-ordered sets to* $\mathbf{V}$ *such that* $\mathbf{Ord}(A) = \mathbf{Ord}(B)$ *if and only if* $A \cong B$.

Let $\mathbf{Ord}(x, y)$ be the proposition: x is a well-ordered set (A, R) and there exists a surjective function $E : A \twoheadrightarrow y$ such that, for all $t \in A$, we have $E(t) = \{E(s) : s \in A, sRt\}$. We reason as follows:

PROOF:

$\langle 1 \rangle 1$. **Ord** is a function

$\langle 2 \rangle 1$. ASSUME: $\mathbf{Ord}((A, R), \alpha)$ and $\mathbf{Ord}((A, R), \beta)$

$\langle 2 \rangle 2$. PICK surjective functions $E_1 : A \twoheadrightarrow \alpha$ and $E_2 : A \twoheadrightarrow \beta$ such that, for all $t \in A$, we have $E_1(t) = \{E_1(s) : sRt\}$ and $E_2(t) = \{E_2(s) : sRt\}$

$\langle 2 \rangle 3$. $E_1 = E_2$

PROOF: Prove $E_1(t) = E_2(t)$ by R-induction on t.

$\langle 2 \rangle 4$. $\alpha = \beta$

PROOF: We have $\alpha = \operatorname{ran} E_1 = \operatorname{ran} E_2 = \beta$.

$\langle 1 \rangle 2$. dom **Ord** is the class of all well-ordered sets

$\langle 2 \rangle 1$. If $\mathbf{Ord}(x, y)$ then x is a well-ordered set.

PROOF: Immediate.

$\langle 2 \rangle 2$. For any well-ordered set (A, R), there exists α such that $\mathbf{Ord}((A, R), \alpha)$

$\langle 3 \rangle 1$. LET: (A, R) be a well-ordered set.

$\langle 3 \rangle 2$. Define the function $E : A \to \mathbf{V}$ by transfinite recursion by: $E(t) = \{E(s) : sRt\}$

$\langle 3 \rangle 3$. LET: $\alpha = \operatorname{ran} E$

$\langle 3 \rangle 4$. $\mathbf{Ord}((A, R), \alpha)$

$\langle 1 \rangle 3$. Given well-ordered sets A and B, we have $\mathbf{Ord}(A) = \mathbf{Ord}(B)$ if and only if $A \cong B$.

$\langle 2 \rangle 1$. LET: (A, R) and (B, S) be well-ordered sets.

$\langle 2 \rangle 2$. If $\mathbf{Ord}(A, R) = \mathbf{Ord}(B, S)$ then $(A, R) \cong (B, S)$

$\langle 3 \rangle 1$. ASSUME: $\mathbf{Ord}(A, R) = \mathbf{Ord}(B, S) = \alpha$, say

$\langle 3 \rangle 2$. PICK surjective function $E : (A, R) \twoheadrightarrow \alpha$ and $E' : (B, S) \twoheadrightarrow \alpha$ such that $\forall t \in A. E(t) = \{E(s) : sRt\}$ and $\forall t \in B. E'(t) = \{E'(s) : sSt\}$

⟨3⟩3. E' is a bijection
PROOF: If sSt then $E'(s) \in E'(t)$ hence $E'(s) \neq E'(t)$.
⟨3⟩4. Define $F : A \to B$ by $F = {E'}^{-1} \circ E$
⟨3⟩5. For $s, t \in A$ we have sRt iff $F(s)SF(t)$
PROOF:

$$\begin{aligned} sRt &\Leftrightarrow E(s) \in E(t) \\ &\Leftrightarrow {E'}^{-1}(E(s))S{E'}^{-1}(E(t)) \end{aligned}$$

⟨2⟩3. If $A \cong B$ then $\mathbf{Ord}(A) = \mathbf{Ord}(B)$
⟨3⟩1. LET: $F : (A, R) \cong (B, S)$
⟨3⟩2. LET: $\alpha = \mathbf{Ord}(A, R)$
⟨3⟩3. LET: $\beta = \mathbf{Ord}(B, S)$
⟨3⟩4. PICK a surjective function $E : A \to \alpha$ such that $\forall t \in A.E(t) = \{E(s) : sRt\}$
⟨3⟩5. PICK a surjective function $E' : B \to \beta$ such that $\forall t \in B.E'(t) = \{E'(s) : sSt\}$
⟨3⟩6. $\forall t \in A.E(t) = E'(F(t))$
PROOF: By R-induction on t.
⟨3⟩7. $\alpha = \beta$
PROOF: $\alpha = \operatorname{ran} E = \operatorname{ran} E' = \beta$

□

Theorem Schema 4.0.2. *Given any predicates* $\mathbf{Ord}(x, y)$ *and* $\mathbf{Ord}'(x, z)$*, there exists a predicate* $\mathbf{F}(y, z)$ *such that the following is a theorem.*

Assume $\mathbf{Ord}$ *and* $\mathbf{Ord}'$ *are functions from the class of all well-ordered sets to* $\mathbf{V}$ *such that, for all well-ordered sets* A *and* B*,* $\mathbf{Ord}(A) = \mathbf{Ord}(B)$ *if and only if* $\mathbf{Ord}'(A) = \mathbf{Ord}'(B)$ *if and only if* $A \cong B$*. Then* $\mathbf{F}$ *is a bijection between* $\operatorname{ran} \mathbf{Ord}$ *and* $\operatorname{ran} \mathbf{Ord}'$ *such that* $\mathbf{F} \circ \mathbf{Ord} = \mathbf{Ord}'$*.*

Take $\mathbf{F}(y, z)$ to be the predicate: There exists x such that $\mathbf{Ord}(x, y)$ and $\mathbf{Ord}'(x, z)$.
PROOF:
⟨1⟩1. $\mathbf{F}$ is a bijection between $\operatorname{ran} \mathbf{Ord}$ and $\mathbf{Ord}'$
⟨2⟩1. $\mathbf{F}$ is a function.
⟨3⟩1. ASSUME: $\mathbf{F}(y, z)$ and $\mathbf{F}(y, z')$
⟨3⟩2. PICK x such that $\mathbf{Ord}(x) = y$ and $\mathbf{Ord}'(x) = z$
⟨3⟩3. PICK x' such that $\mathbf{Ord}(x') = y$ and $\mathbf{Ord}'(x') = z'$
⟨3⟩4. $x \cong x'$
⟨3⟩5. $z = z'$
⟨2⟩2. $\operatorname{dom} \mathbf{F} = \operatorname{ran} \mathbf{Ord}$
⟨3⟩1. $\operatorname{dom} \mathbf{F} \subseteq \operatorname{ran} \mathbf{Ord}$
PROOF: Immediate.
⟨3⟩2. $\operatorname{ran} \mathbf{Ord} \subseteq \operatorname{dom} \mathbf{F}$
⟨4⟩1. LET: $y \in \operatorname{ran} \mathbf{Ord}$
⟨4⟩2. PICK x such that $\mathbf{Ord}(x) = y$
⟨4⟩3. $\mathbf{F}(y) = \mathbf{Ord}'(x)$
⟨2⟩3. $\operatorname{ran} \mathbf{F} = \operatorname{ran} \mathbf{Ord}'$

⟨3⟩1. ran $\mathbf{F} \subseteq$ ran $\mathbf{Ord}'$
PROOF: Immediate.
⟨3⟩2. ran $\mathbf{Ord}' \subseteq$ ran $\mathbf{F}$
⟨4⟩1. LET: $z \in$ ran $\mathbf{Ord}'$
⟨4⟩2. PICK x such that $\mathbf{Ord}'(x) = z$
⟨4⟩3. $\mathbf{F}(\mathbf{Ord}(x)) = z$
⟨2⟩4. $\mathbf{F}$ is one-to-one.
⟨3⟩1. ASSUME: $\mathbf{F}(y) = \mathbf{F}(y')$
⟨3⟩2. PICK x and x' such that $\mathbf{Ord}(x) = y$, $\mathbf{Ord}(x') = y'$, and $\mathbf{Ord}'(x) = \mathbf{Ord}'(x') = \mathbf{F}(y)$
⟨3⟩3. $x \cong x'$
⟨3⟩4. $y = y'$
⟨1⟩2. $\mathbf{F} \circ \mathbf{Ord} = \mathbf{Ord}'$
PROOF: Immediate.
□

Pick a function **Ord** such that dom **Ord** is the class of all well-ordered sets, and $\mathbf{Ord}(A) = \mathbf{Ord}(B)$ iff $A \cong B$.

Definition 4.0.3 (Ordinal Number)**.** The class **On** of *ordinal numbers* is ran **Ord**.

Definition 4.0.4 (Well-ordered by Epsilon)**.** A set A is *well-ordered by epsilon* iff $\{(x, y) : x, y \in A, x \in y\}$ is a well ordering on A.

Definition 4.0.5 (Transitive Set)**.** A set A is a *transitive set* iff every member of a member of A is a member of A.

Theorem 4.0.6. *A set is an ordinal number if and only if it is a transitive set that is well-ordered by epsilon.*

PROOF:
⟨1⟩1. Every ordinal number is a transitive set.
PROOF: Lemma **??**.
⟨1⟩2. Every ordinal number is well-ordered by epsilon.
PROOF: Corollary **??**.
⟨1⟩3. Every transitive set that is well-ordered by epsilon is an ordinal number.
⟨2⟩1. LET: α be a transitive set well-ordered by epsilon.
⟨2⟩2. LET: β be the epsilon-image of $(\alpha, \in)$ with $E : \alpha \cong \beta$ the canonical isomorphism.
⟨2⟩3. $\forall x \in \alpha. E(x) = x$
⟨3⟩1. LET: $x \in \alpha$
⟨3⟩2. ASSUME: $\forall y < x. E(y) = y$
⟨3⟩3. $E(x) = x$
PROOF:

$$\begin{aligned} E(x) &= \{E(y) : y \in \alpha, y \in x\} \\ &= \{E(y) : y \in x\} && (\alpha \text{ is a transitive set}) \\ &= \{y : y \in x\} && (\langle 3 \rangle 2) \\ &= x \end{aligned}$$

⟨2⟩4. $\alpha = \beta$
□

Theorem 4.0.7. *Every member of an ordinal number is an ordinal number.*

PROOF:
⟨1⟩1. LET: α be an ordinal number.
⟨1⟩2. LET: $\beta \in \alpha$
⟨1⟩3. β is a transitive set.
⟨2⟩1. LET: $x \in y \in \beta$
⟨2⟩2. $y \in \alpha$
PROOF: Since α is a transitive set.
⟨2⟩3. $x \in \alpha$
PROOF: Since α is a transitive set.
⟨2⟩4. $x \in \beta$
PROOF: Since α is a partially ordered by epsilon.
⟨1⟩4. β is well-ordered by epsilon.
PROOF: Since $\{(x, y) : x, y \in \beta, x \in y\}$ is the restriction of $\{(x, y) : x, y \in \alpha, x \in y\}$ to β.
⟨1⟩5. β is an ordinal number.
PROOF: Theorem 4.0.6.
□

Proposition 4.0.8. *The class of ordinals is well-ordered by epsilon.*

PROOF:
⟨1⟩1. For any ordinals α, β, γ, if $\alpha \in \beta \in \gamma$ then $\alpha \in \gamma$.
PROOF: Since γ is a transitive set (Lemma **??**).
⟨1⟩2. For any ordinal α we have $\alpha \notin \alpha$.
PROOF: Since α is well-ordered by epsilon.
⟨1⟩3. For any ordinals α, β, exactly one of $\alpha \in \beta$, $\beta \in \alpha$, $\alpha = \beta$ holds.
⟨2⟩1. LET: α, β be ordinals.
⟨2⟩2. Either $\alpha \cong \beta$ or $\exists \gamma \in \beta . \alpha \cong \gamma$ or $\exists \gamma \in \alpha . \gamma \cong \alpha$
PROOF: Theorem 3.3.4.
⟨2⟩3. Either $\alpha = \beta$ or $\exists \gamma \in \beta . \alpha = \gamma$ or $\exists \gamma \in \alpha . \gamma = \alpha$
PROOF: Since any ordinal is its own epsilon-image, and isomorphic well-orderings have equal epsilon-images.
⟨1⟩4. Any nonempty set of ordinals has a least element.
⟨2⟩1. LET: A be a nonempy set of ordinals.
⟨2⟩2. PICK $\alpha \in A$
⟨2⟩3. CASE: $A \cap \alpha = \emptyset$
PROOF: In this case, α is least in A.
⟨2⟩4. CASE: $A \cap \alpha \neq \emptyset$
PROOF: In this case, the least element of $A \cap \alpha$ is the least element in A.
□

Corollary 4.0.8.1. *Any transitive set of ordinal numbers is an ordinal number.*

Corollary 4.0.8.2. $\emptyset$ *is an ordinal number.*

We write 0 for $\emptyset$ considered as an ordinal number.

Definition 4.0.9 (Successor)**.** The *successor* of a set a is the set $a^+ = a \cup \{a\}$.

Corollary 4.0.9.1. *The successor of an ordinal number is an ordinal number.*

Corollary 4.0.9.2. *For any set A of ordinal numbers, the set $\bigcup A$ is an ordinal number.*

Theorem 4.0.10 (Burali-Forti)**.** *The class of ordinal numbers is not a set.*

PROOF:
⟨1⟩1. ASSUME: for a contradiction the class **On** is a set.
⟨1⟩2. **On** is an ordinal number.
  PROOF: Corollary 4.0.8.1.
⟨1⟩3. **On** $\in$ **On**
⟨1⟩4. Q.E.D.
  PROOF: This contradicts Lemma **??**.
□

Theorem 4.0.11 (Hartogs)**.** *For any set A, there exists an ordinal not dominated by A.*

PROOF:
⟨1⟩1. LET: A be a set.
⟨1⟩2. LET: $\alpha = \{\beta : \beta \text{ is an ordinal }, \beta \preccurlyeq A\}$.
⟨1⟩3. LET: $W = \{(B, <) : B \subseteq A, < \text{ is a well ordering on } B\}$
⟨1⟩4. $\forall \beta \in \alpha . \exists (B, <) \in W . \beta$ is the epsilon-image of $(B, <)$
  ⟨2⟩1. LET: $\beta \in \alpha$
  ⟨2⟩2. PICK an injection $f : \beta \to A$
  ⟨2⟩3. Define $<$ on $f(\beta)$ by: $f(\gamma) < f(\delta)$ iff $\gamma \in \delta$
  ⟨2⟩4. $<$ well orders $f(\beta)$
  ⟨2⟩5. β is the epsilon-image of $(f(\beta), <)$ with f^{-1} the canonical isomorphism.
⟨1⟩5. α is a set.
  PROOF: By a Replacement Axiom applied to W.
⟨1⟩6. α is an ordinal.
  ⟨2⟩1. α is a transitive set.
    ⟨3⟩1. LET: $\beta \in \gamma \in \alpha$
    ⟨3⟩2. $\beta \subseteq \gamma \preccurlyeq A$
    ⟨3⟩3. $\beta \preccurlyeq A$
    ⟨3⟩4. $\beta \in \alpha$
  ⟨2⟩2. Q.E.D.
    PROOF: By Corollary 4.0.8.1.
⟨1⟩7. $\alpha \not\preccurlyeq A$
  PROOF: Because $\alpha \notin \alpha$.
□

Theorem 4.0.12. *The following statements are equivalent:*

1. *The Axiom of Choice*

2. ***Well-Ordering Theorem*** *For any set A, there exists a well ordering on A.*

3. ***Zorn's Lemma*** *Let $\mathcal{A}$ be a set such that, for every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$. Then $\mathcal{A}$ has a maximal element.*

PROOF:
⟨1⟩1. If the Axiom of Choice is true then the Well-Ordering Theorem is true.
  ⟨2⟩1. ASSUME: The Axiom of Choice
  ⟨2⟩2. LET: A be any set.
  ⟨2⟩3. PICK an ordinal α not dominated by A.
  ⟨2⟩4. PICK an object e such that $e \notin A$.
  ⟨2⟩5. PICK a choice function $G : \mathcal{P}A - \{\emptyset\} \to A$ for A.
  ⟨2⟩6. Define the function $F : \alpha \to A \cup \{e\}$ by transfinite recursion thus:
$$F(\gamma) = \begin{cases} G(A - \{F(\delta) : \delta < \gamma\}) & \text{if } A - \{F(\delta) : \delta < \gamma\} \neq \emptyset \\ e & \text{if } A - \{F(\delta) : \delta < \gamma\} = \emptyset \end{cases}$$
  ⟨2⟩7. LET: δ be least such that $F(\delta) = e$
    PROOF: There is such a δ, otherwise F would be a bijection between α and A.
  ⟨2⟩8. $F \restriction \delta$ is a bijection between δ and A
  ⟨2⟩9. Define $<$ on A by: $F(\gamma) < F(\beta)$ iff $\gamma \in \beta$ for $\gamma, \beta \in \delta$
  ⟨2⟩10. $<$ is a well ordering on A.
⟨1⟩2. If the Well-Ordering Theorem is true then Zorn's Lemma is true.
  ⟨2⟩1. ASSUME: The Well-Ordering Theorem
  ⟨2⟩2. LET: $\mathcal{A}$ be a set that is closed under unions of chains.
  ⟨2⟩3. PICK a well ordering $<$ on $\mathcal{A}$
  ⟨2⟩4. Define the function $F : \mathcal{A} \to 2$ by transfinite recursion thus:
$$F(A) = \begin{cases} 1 & \text{if } \forall B < A. F(B) = 1 \Rightarrow B \subseteq A \\ 0 & \text{otherwise} \end{cases}$$
  ⟨2⟩5. LET: $\mathcal{C} = \{A \in \mathcal{A} : F(A) = 1\}$
  ⟨2⟩6. $\mathcal{C}$ is a chain.
    ⟨3⟩1. LET: $A, B \in \mathcal{C}$
    ⟨3⟩2. ASSUME: w.l.o.g. $A < B$
    ⟨3⟩3. $F(A) = 1$
    ⟨3⟩4. $F(B) = 1$
    ⟨3⟩5. $A \subseteq B$
  ⟨2⟩7. $\bigcup \mathcal{C} \in \mathcal{A}$
    PROOF: By ⟨2⟩2.
  ⟨2⟩8. $\bigcup \mathcal{C}$ is maximal in $\mathcal{A}$
    ⟨3⟩1. ASSUME: $\bigcup \mathcal{C} \subseteq D \in \mathcal{A}$
    ⟨3⟩2. $\forall B < D. F(B) = 1 \Rightarrow B \subseteq D$
      PROOF: If $F(B) = 1$ then $B \in \mathcal{C}$ so $B \subseteq \bigcup \mathcal{C} \subseteq D$.
    ⟨3⟩3. $F(D) = 1$
    ⟨3⟩4. $D \in \mathcal{C}$
    ⟨3⟩5. $D = \bigcup \mathcal{C}$

⟨1⟩3. If Zorn's Lemma is true then the Axiom of Choice is true.
  ⟨2⟩1. ASSUME: Zorn's Lemma
  ⟨2⟩2. LET: R be a relation.
  ⟨2⟩3. LET: $\mathcal{A}$ be the set of all functions that are subsets of R.
  ⟨2⟩4. For any chain $\mathcal{B} \subseteq \mathcal{A}$ we have $\bigcup \mathcal{B} \in \mathcal{A}$
  ⟨2⟩5. PICK $F \in \mathcal{A}$ maximal.
  ⟨2⟩6. $\operatorname{dom} F = \operatorname{dom} R$
□

Corollary 4.0.12.1 (Numeration Theorem (Choice))**.** *Any set is equinumerous to some ordinal number.*

Theorem 4.0.13 (Transfinite Recursion)**.** *Let* $\mathbf{F} : \mathbf{V} \to \mathbf{V}$*. Then there exists a function* $\mathbf{G} : \mathbf{On} \to \mathbf{V}$ *such that*

$$\forall \alpha \in \mathbf{On}.\mathbf{G}(\alpha) = \mathbf{F}(\mathbf{G} \upharpoonright \alpha) \ .$$

PROOF: Define $\mathbf{G} = \{(\alpha, y) : \exists f : \alpha^+ \to \mathbf{V}.\forall \beta \in \alpha^+.f(\beta) = \mathbf{F}(f \upharpoonright \beta)\}$. □

Definition 4.0.14 (Continuous)**.** A function $\mathbf{F} : \mathbf{On} \to \mathbf{On}$ is *continuous* iff $\mathbf{F}(\lambda) = \bigcup_{\beta \in \lambda} \mathbf{F}(\beta)$ for every limit ordinal λ.

Theorem 4.0.15. *Let* $\mathbf{F} : \mathbf{On} \to \mathbf{On}$ *be continuous. Suppose* $\forall \alpha \in \mathbf{On}.\mathbf{F}(\alpha) < \mathbf{F}(\alpha + 1)$*. Then* $\mathbf{F}$ *is strictly monotone.*

PROOF:
⟨1⟩1. LET: $P(\beta)$ be the statement: $\forall \alpha < \beta.\mathbf{F}(\alpha) < \mathbf{F}(\beta)$
⟨1⟩2. $P(0)$
  PROOF: Vacuous.
⟨1⟩3. $\forall \beta \in \mathbf{On}.P(\beta) \Rightarrow P(\beta^+)$
  PROOF: For $\alpha < \beta^+$ we have $\mathbf{F}(\alpha) \leq \mathbf{F}(\beta) < \mathbf{F}(\beta^+)$.
⟨1⟩4. For every limit ordinal λ, if $\forall \beta < \lambda.P(\beta)$ then $P(\lambda)$
  PROOF: For $\alpha < \lambda$ we have $\mathbf{F}(\alpha) < \mathbf{F}(\alpha^+) \leq \mathbf{F}(\lambda)$.
□

Definition 4.0.16 (Normal)**.** A function $\mathbf{F} : \mathbf{On} \to \mathbf{On}$ is *normal* iff it is strictly monotone and continuous.

Theorem 4.0.17. *Let* $\mathbf{F} : \mathbf{On} \to \mathbf{On}$ *be normal. Let* $t_0 \leq \beta$*. Then there exists a greatest* γ *such that* $\mathbf{F}(\gamma) \leq \beta$*.*

PROOF:
⟨1⟩1. LET: $\gamma = \{\alpha \in \mathbf{On} : \mathbf{F}(\alpha) \leq \beta\}$
⟨1⟩2. γ is an ordinal.
  ⟨2⟩1. γ is a set.
    PROOF: We have $\alpha \leq \mathbf{F}(\alpha)$ for all α, so $\gamma \subseteq \beta$.
  ⟨2⟩2. γ is a transitive set.
    PROOF: If $\alpha < \alpha'$ and $\mathbf{F}(\alpha') \leq \beta$ then $\mathbf{F}(\alpha) < \beta$ by monotonicity.
⟨1⟩3. $\gamma \neq 0$

PROOF: By hypothesis.
⟨1⟩4. CASE: γ is a successor ordinal.
PROOF: Let $\gamma = \alpha^+$. Then α is greatest such that $\mathbf{F}(\alpha) \leq \beta$.
⟨1⟩5. CASE: γ is a limit ordinal.
PROOF: This is impossible since then $\mathbf{F}(\gamma) = \bigcup_{\alpha \in \gamma} \mathbf{F}(\alpha) \leq \beta$ and so $\gamma \in \gamma$.
□

Theorem 4.0.18. *Let $\mathbf{F} : \mathbf{On} \to \mathbf{On}$ be normal. Let S be a nonempty set of ordinals. Then $\mathbf{F}(\sup S) = \sup \mathbf{F}(S)$.*

PROOF:
⟨1⟩1. $\mathbf{F}(\sup S) \geq \sup \mathbf{F}(S)$
PROOF: By monotonicity.
⟨1⟩2. $\mathbf{F}(\sup S) \leq \sup \mathbf{F}(S)$
⟨2⟩1. CASE: $\sup S \in S$
PROOF: Immediate.
⟨2⟩2. CASE: $\sup S \notin S$
⟨3⟩1. $\sup S$ is a limit ordinal.
⟨3⟩2. $\mathbf{F}(\sup S) = \sup\{\mathbf{F}(\beta) : \beta < \sup S\}$
⟨3⟩3. $\forall \beta < \sup S . \mathbf{F}(\beta) \leq \sup \mathbf{F}(S)$
□

Theorem 4.0.19 (Veblen Fixed-Point Theorem (1907))**.** *A normal operation on ordinals has arbitrarily large fixed points.*

That is, let $\mathbf{F} : \mathbf{On} \to \mathbf{On}$ be normal. For all $\alpha \in \mathbf{On}$, there exists $\beta \geq \alpha$ such that $\mathbf{F}(\beta) = \beta$.

PROOF: Let $\beta = \sup_{n \in \omega} F^n(\alpha)$. Then $\alpha \leq \beta$ using monotonicity, and
$$\begin{aligned} F(\beta) &= \sup_{n \in \omega} F^{n+1}(\alpha) \\ &= \beta \end{aligned}$$
□

Definition 4.0.20 (Addition)**.** The *sum* of two ordinal numbers is the ordinal number of their concatenation.

Theorem 4.0.21. *Addition is associative.*

PROOF: Easy. □

Theorem 4.0.22.
$$\alpha + 0 = 0 + \alpha = \alpha$$

PROOF: Easy. □

Theorem 4.0.23.
$$\alpha + \beta^+ = (\alpha + \beta)^+$$

PROOF: Easy. □

Theorem 4.0.24. *For λ a limit ordinal, $\alpha + \lambda = \sup_{\beta < \lambda}(\alpha + \beta)$.*

PROOF: Easy. □

Theorem 4.0.25. *For any ordinal α, the function that maps β to $\alpha + \beta$ is normal.*

PROOF: Easy. □

Corollary 4.0.25.1.

$$\beta < \gamma \Leftrightarrow \alpha + \beta < \alpha + \gamma$$

Corollary 4.0.25.2. *If $\alpha + \beta = \alpha + \gamma$ then $\beta = \gamma$.*

Theorem 4.0.26. *If $\beta \leq \gamma$ then $\beta + \alpha \leq \gamma + \alpha$.*

PROOF: Transfinite induction on α. □

Theorem 4.0.27 (Subtraction Theorem)**.** *If $\alpha \leq \beta$ then there exists a unique ordinal γ such that $\alpha + \gamma = \beta$.*

PROOF: Let γ be greatest such that $\alpha + \gamma \leq \beta$. □

Definition 4.0.28 (Multiplication)**.** The *product* of two ordinal numbers α and β is the ordinal number of $\alpha \times \beta$ under the lexicographic ordering.

Theorem 4.0.29. *Multiplication is associative.*

PROOF: Easy. □

Theorem 4.0.30.

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$$

PROOF: Easy. □

Theorem 4.0.31.

$$\alpha 1 = 1\alpha = \alpha$$

PROOF: Easy. □

Theorem 4.0.32.

$$\alpha 0 = 0\alpha = 0$$

PROOF: Easy. □

Theorem 4.0.33.

$$\alpha\beta^{+} = \alpha\beta + \alpha$$

PROOF: Easy. □

Theorem 4.0.34. *For λ a limit ordinal, $\alpha\lambda = \sup_{\beta<\lambda}(\alpha\beta)$.*

PROOF: Easy. □

Theorem 4.0.35. *For any ordinal $\alpha > 0$, the function that maps β to $\alpha\beta$ is normal.*

PROOF: Easy. □

Corollary 4.0.35.1. *For $\alpha > 0$ we have*

$$\beta < \gamma \Leftrightarrow \alpha\beta < \alpha\gamma$$

Corollary 4.0.35.2. *For $\alpha > 0$, if $\alpha\beta = \alpha\gamma$ then $\beta = \gamma$.*

Theorem 4.0.36. *If $\beta \leq \gamma$ then $\beta\alpha \leq \gamma\alpha$.*

PROOF: Transfinite induction on α. □

Theorem 4.0.37 (Division Theorem)**.** *Let $\delta \neq 0$. For any α, there exist unique ordinals β, γ such that $\alpha = \delta\beta + \gamma$ and $\gamma < \delta$.*

PROOF: Let β be largest such that $\delta\beta \leq \alpha$, and let γ be as given by the Subtraction Theorem. □

PROOF: Let γ be greatest such that $\alpha + \gamma \leq \beta$. □

Definition 4.0.38 (Exponentiation)**.** Define α^β by transfinite recursion thus:

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^{\beta^+} &= \alpha^\beta\alpha \\
\alpha^\lambda &= \sup_{\beta<\lambda} \alpha^\beta
\end{aligned}$$

for λ a limit ordinal.

Theorem 4.0.39. *For $\alpha > 1$, the function that maps β to α^β is normal.*

PROOF: Easy. □

Corollary 4.0.39.1. *For $\alpha > 1$ we have*

$$\beta < \gamma \Leftrightarrow \alpha^\beta < \alpha^\gamma$$

Corollary 4.0.39.2. *For $\alpha > 1$, if $\alpha^\beta = \alpha^\gamma$ then $\beta = \gamma$.*

Theorem 4.0.40. *If $\beta \leq \gamma$ then $\beta^\alpha \leq \gamma^\alpha$.*

PROOF: Transfinite induction on α. □

Theorem 4.0.41 (Logarithm Theorem)**.** *Let $\alpha \neq 0$ and $\beta > 1$. Then there exist unique ordinals γ, δ, ρ such that $\alpha = \beta^\gamma\delta + \rho$, $0 < \delta < \beta$ and $\rho < \beta^\gamma$.*

PROOF: Let γ be greatest such that $\beta^\gamma \leq \alpha$, and then apply the Division Theorem. □

Theorem 4.0.42.

$$\alpha^{\beta+\gamma} = \alpha^\beta\alpha^\gamma$$

PROOF: Transfinite induction on γ. □

Theorem 4.0.43.

$$\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$$

PROOF: Transfinite induction on γ. □

Chapter 5

Natural Numbers

5.1 Natural Numbers

Definition 5.1.1 (Peano System)**.** A *Peano system* is a triple $\langle N, S, 0\rangle$ consisting of a set N, a function $S : N \to N$ and an element $0 \in N$ such that:

1. $0 \notin \operatorname{ran} S$
2. S is one-to-one
3. Any subset $A \subseteq N$ that contains 0 and is closed under S equals N.

We call 0 *zero* and $S(x)$ the *successor* of x.

Theorem 5.1.2. *In any Peano system, every element is either 0 or a successor.*

Proof: The set of elements that are either 0 or a successor contains 0 and is closed under successor. □

Theorem 5.1.3 (Iteration Theorem)**.** *Let $(N, S, 0)$ be any Peano system. Let W be a set, $c \in W$ and $g : W \to W$. Then there exists a unique function $F : N \to W$ such that $F(0) = c$ and $\forall x \in N.F(S(x)) = g(F(x))$.*

Proof:
$\langle 1\rangle 1$. S is a well-founded relation.
  $\langle 2\rangle 1$. Let: $A \subseteq N$
  $\langle 2\rangle 2$. Assume: A has no S-minimal element
      Prove: $A = \emptyset$
  $\langle 2\rangle 3$. $0 \in N - A$
    Proof: Otherwise 0 would be an S-minimal element of A.
  $\langle 2\rangle 4$. $\forall x \in N - A.S(x) \in N - A$
    Proof: Otherwise $S(x)$ would be an S-minimal element of A.
  $\langle 2\rangle 5$. $N - A = N$
    Proof: By induction.
$\langle 1\rangle 2$. Q.E.D.

PROOF: By Transfinite Recursion.
∎

Definition 5.1.4 (Inductive)**.** A class $\mathbf{A}$ is *inductive* iff $\emptyset \in \mathbf{A}$ and $\forall a \in \mathbf{A}.a^+ \in \mathbf{A}$.

Definition 5.1.5 (Natural Number)**.** A *natural number* is a set that belongs to every inductive set.

We write ω for the class of all natural numbers.

Theorem 5.1.6. *The class ω is a set.*

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

Theorem 5.1.7. *The set ω is inductive, and is a subset of every inductive set.*

PROOF: Easy. ∎

Corollary 5.1.7.1 (Proof by Induction)**.** *Any inductive subclass of ω is equal to ω.*

Theorem 5.1.8. *Every natural number except 0 is the successor of some natural number.*

PROOF: Easy proof by induction. ∎

Theorem 5.1.9. *For any transitive set a, $\bigcup(a^+) = a$.*

PROOF:

$$\begin{aligned}\bigcup(a^+) &= \bigcup(a \cup \{a\}) \\ &= \bigcup a \cup \bigcup\{a\} \\ &= \bigcup a \cup a \\ &= a\end{aligned}$$

since $\bigcup a \subseteq a$. ∎

Theorem 5.1.10. *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 5.1.9.

∎

Theorem 5.1.11. $\langle \omega, \sigma, 0\rangle$ *is a Peano system, where* $0 = \emptyset$ *and* $\sigma = \{\langle n, n^+\rangle : n \in \omega\}$.

PROOF:
⟨1⟩1. $0 \notin \operatorname{ran} \sigma$
PROOF: For any $n \in \omega$ we have $0 \neq n^+$ since $n \in n^+$ and $n \notin 0$.
⟨1⟩2. σ is one-to-one.
PROOF: If $m^+ = n^+$ then $m = \bigcup(m^+) = \bigcup(n^+) = n$ using Theorems 5.1.9 and 5.1.10.
⟨1⟩3. Any subset $A \subseteq \omega$ that contains 0 and is closed under σ equals ω.
□

Theorem 5.1.12. *The set ω is a transitive set.*

PROOF:
⟨1⟩1. For every natural number n we have $\forall m \in n.\ m$ is a natural number.
⟨2⟩1. $\forall m \in 0.\ m$ is a natural number.
PROOF: Vacuous.
⟨2⟩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 5.1.13. *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 ω 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:
⟨1⟩1. There exists a function h that satisfies those two conditions.
PROOF: By the Recursion Theorem.
⟨1⟩2. For all $m, n \in \omega$, if $m \neq n$ then $h(m) \neq h(n)$
⟨2⟩1. For all $n \in \omega$, if $n \neq 0$ then $h(n) \neq h(0)$
⟨3⟩1. LET: $n \in \omega$
⟨3⟩2. ASSUME: $n \neq 0$
⟨3⟩3. PICK p such that $n = p^+$
⟨3⟩4. $h(n) \neq h(0)$
PROOF: $h(n) = S(h(p)) \neq e = h(0)$.
⟨2⟩2. For all $m \in \omega$, if $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$ then $\forall n(m^+ \neq n \Rightarrow h(m^+) \neq h(n))$
⟨3⟩1. LET: $m \in \omega$
⟨3⟩2. ASSUME: $\forall n(m \neq n \Rightarrow h(m) \neq h(n))$
⟨3⟩3. LET: $n \in \omega$
⟨3⟩4. ASSUME: $m^+ \neq n$
PROVE: $h(m^+) \neq h(n)$
⟨3⟩5. CASE: $n = 0$

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

⟨3⟩6. CASE: $n = p^+$

⟨4⟩1. $m \neq p$

⟨4⟩2. $h(m) \neq h(p)$

⟨4⟩3. $S(h(m)) \neq S(h(p))$

⟨4⟩4. $h(m^+) \neq h(p^+)$

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

PROOF: An easy induction on x.

□

Theorem 5.1.14 (Choice)**.** *Let R be a relation on A. Then R is well founded iff there does not exist any function $f : \omega \to A$ such that $f(n+1)Rf(n)$ for all $n \in \omega$.*

PROOF:

⟨1⟩1. If R is well founded then there does not exist any function $f : \omega \to A$ such that $f(n+1)Rf(n)$ for all $n \in \omega$.

PROOF: If there is such a function f then $\operatorname{ran} f$ is a nonempty subset of A with no R-minimal element.

⟨1⟩2. If there does not exist any function $f : \omega \to A$ such that $f(n+1)Rf(n)$ for all $n \in \omega$ then R is well founded.

⟨2⟩1. LET: $X \subseteq A$ be a nonempty subset of A with no R-minimal element.

PROVE: There exists a function $f : \omega \to A$ such that $f(n+1) < f(n)$ for all $n \in \omega$

⟨2⟩2. PICK $a_0 \in X$

⟨2⟩3. $\forall x \in X. \exists y \in X. yRx$

⟨2⟩4. PICK a function $g : X \to X$ such that $\forall x \in X. g(x)Rx$

PROOF: By the Axiom of Choice.

⟨2⟩5. Define $f : \omega \to A$ recursively by:

$$f(0) = a_0$$
$$f(n^+) = g(f(n))$$

⟨2⟩6. $\forall n \in \omega. f(n^+)Rf(n)$

□

Alternative proof for Theorem 2.10.1 Define $f : \omega \to \mathcal{P}A^2$ by $f(0) = R$ and $f(n^+) = f(n) \circ R$. Define $R^t = \bigcup_{n \in \omega} f(n)$.

Theorem 5.1.15. *For any set A, there exists the smallest transitive set B such that $A \subseteq B$.*

PROOF: Define $f : \omega \to \mathbf{V}$ by

$$f(0) = A$$
$$f(n^+) = f(n) \cup \bigcup f(n)$$

Then $\bigcup_n f(n)$ is the smallest transitive set that includes A. □

Definition 5.1.16 (Transitive Closure)**.** The *transitive closure* of a set A is the least transitive set that includes A.

Theorem 5.1.17. *Addition on natural numbers is commutative.*

Theorem 5.1.18. *Multiplication on natural numbers is commutative.*

Definition 5.1.19 (Sequence)**.** A *sequence* in a set A is a function $\mathbb{N} \to A$.

Definition 5.1.20 (Subsequence)**.** Let (a_n) be a sequence in a set A. A *subsequence* of (a_n) is a sequence of the form (a_{n_r}) where (n_r) is a strictly increasing sequence in $\mathbb{N}$.

Definition 5.1.21 (Nested Sequence)**.** Let P be a partial order and $([a_n, b_n])$ a sequence of closed intervals in P. The sequence is *nested* iff $\forall n. a_n \leq a_{n+1}$ and $\forall n. b_{n+1} \leq b_n$.

5.2 Finite Sets

Definition 5.2.1 (Finite)**.** A set is *finite* iff it is equinumerous with a natural number. Otherwise it is infinite.

Theorem 5.2.2. *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 $n \in \operatorname{ran} f$.
□

Corollary 5.2.2.1. *No finite set is equinumerous with a proper subset of itself.*

Corollary 5.2.2.2. *The set ω is infinite.*

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

Corollary 5.2.2.3. *Every finite set is equinumerous with a unique natural number.*

Lemma 5.2.3. *Let n be a natural number and $C \subseteq n$. Then there exists $m \underline{\in} n$ such that $C \approx m$.*

PROOF:
$\langle 1 \rangle 1$. For all $C \subseteq 0$, there exists $m \underline{\in} 0$ 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 $m \underline{\in} n$ such that $C \approx m$. Let $C \subseteq n^+$. Then there exists $m \underline{\in} n^+$ 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 $m \underline{\in} n$ 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 $m \underline{\in} n$ 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 $m \underline{\in} n$.
□

Corollary 5.2.3.1. *Any subset of a finite set is finite.*

Chapter 6

Cardinal Numbers

6.1 Cardinal Numbers

Definition 6.1.1 (Cardinality (Choice))**.** For any set A, define the *cardinal number* of A, $|A|$, to be the least ordinal that is equinumerous with A.

Theorem 6.1.2. *For any sets A and B, $|A| = |B|$ if and only if $A \approx B$.*

Proof: Easy. $\square$

Theorem 6.1.3. *For any finite set A, $|A|$ is the natural number such that $A \approx |A|$.*

Proof: Immediate from definitions. $\square$

Definition 6.1.4. We write $\aleph_0$ for $|\omega$.

6.2 Cardinal Arithmetic

Definition 6.2.1 (Addition)**.** Let κ and λ be any cardinal numbers. Then $\kappa + \lambda = |K \cup L|$, where K and L are any disjoint sets of cardinality κ and λ 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 6.2.2. *For any cardinal number κ we have $\kappa + 0 = \kappa$.*

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

Lemma 6.2.3. *For any natural number n we have $n + \aleph_0 = \aleph_0$.*

Proof: Easy. $\square$

Lemma 6.2.4.

$$\aleph_0 + \aleph_0 = \aleph_0$$

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 6.2.5.

$$\kappa + \lambda = \lambda + \kappa$$

PROOF: Easy. □

Theorem 6.2.6.

$$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$$

PROOF: Easy. □

Definition 6.2.7 (Multiplication)**.** Let κ and λ be any cardinal numbers. Then $\kappa\lambda = |K \times L|$, where K and L are any sets of cardinality κ and λ respectively.

It is easy to prove this well-defined.

Lemma 6.2.8. *For any cardinal number κ we have $\kappa 0 = 0$.*

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

Lemma 6.2.9. *For any natural number n we have $n\aleph_0 = \aleph_0$.*

PROOF: Induction on n using Lemma 6.2.4. □

Lemma 6.2.10.

$$\aleph_0 \aleph_0 = \aleph_0$$

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

Lemma 6.2.11.

$$\kappa 1 = \kappa$$

PROOF: Easy. □

Theorem 6.2.12.

$$\kappa\lambda = \lambda\kappa$$

PROOF: Easy. □

Theorem 6.2.13.

$$\kappa(\lambda\mu) = (\kappa\lambda)\mu$$

PROOF: Easy. □

Theorem 6.2.14.

$$\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$$

PROOF: Easy. □

Definition 6.2.15 (Exponentiation)**.** Let κ and λ be any cardinal numbers. Then $\kappa^\lambda = |K^L|$, where K and L are any sets of cardinality κ and λ respectively.

It is easy to prove this well-defined.

Theorem 6.2.16. *For any cardinal κ, $\kappa^0 = 1$.*

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

Theorem 6.2.17. *For any non-zero cardinal κ, we have $0^\kappa = 0$.*

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

Theorem 6.2.18. *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 6.2.18.1. *For any cardinal κ, we have $\kappa \neq 2^\kappa$.*

Theorem 6.2.19.

$$\kappa^{\lambda+\mu} = \kappa^\lambda \kappa^\mu$$

PROOF: Easy. ∎

Theorem 6.2.20.

$$(\kappa\lambda)^\mu = \kappa^\mu \lambda^\mu$$

PROOF: Easy. ∎

Theorem 6.2.21.

$$(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$$

PROOF: Easy. ∎

Lemma 6.2.22. *The union of a set of cardinal numbers is a cardinal number.*

PROOF:
$\langle 1 \rangle 1$. LET: A be a set of cardinal numbers.
$\langle 1 \rangle 2$. LET: $\alpha \in \bigcup A$
$\langle 1 \rangle 3$. PICK $\kappa \in A$ such that $\alpha \in \kappa$
$\langle 1 \rangle 4$. $\alpha \prec \kappa$
$\langle 1 \rangle 5$. $\alpha \prec \bigcup A$
∎

6.3 Alephs

Definition 6.3.1. Define the cardinal number $\aleph_\alpha$ for every ordinal α by transfinite recursion thus: $\aleph_\alpha$ is the least infinite cardinal different from $\aleph_\beta$ for every $\beta < \alpha$.

Theorem 6.3.2. *If $\alpha < \beta$ then $\aleph_\alpha < \aleph_\beta$.*

PROOF: By minimality of $\aleph_\alpha$. ∎

Theorem 6.3.3. *Every infinite cardinal is of the form $\aleph_\alpha$ for some α.*

PROOF:
$\langle 1 \rangle 1$. LET: κ be an infinite cardinal
$\langle 1 \rangle 2$. ASSUME: for every infinite cardinal $\lambda < \kappa$, there exists α such that $\lambda = \aleph_\alpha$
$\langle 1 \rangle 3$. LET: $\alpha = \{\beta : \aleph_\beta < \kappa\}$
$\langle 1 \rangle 4$. α is a set.
PROOF: The mapping $\beta \mapsto \aleph_\beta$ is an injection $\alpha \to \kappa$.
$\langle 1 \rangle 5$. α is a transitive set.
$\langle 1 \rangle 6$. α is an ordinal.
$\langle 1 \rangle 7$. $\aleph_\alpha$ is the least infinite cardinal different from $\aleph_\beta$ for all β such that $\aleph_\beta < \kappa$.
$\langle 1 \rangle 8$. $\aleph_\alpha$ is the least infinite cardinal different from λ for every infinite cardinal $\lambda < \kappa$.
PROOF: By $\langle 1 \rangle 2$.
$\langle 1 \rangle 9$. $\aleph_\alpha = \kappa$
∎

6.4 Arithmetic

Lemma 6.4.1. *For any natural numbers m and n, we have $m+n^+ = (m+n)^+$.*

PROOF: Easy. ∎

Corollary 6.4.1.1. *The union of two finite sets is finite.*

Lemma 6.4.2. *For any natural numbers m and n we have $mn^+ = mn + m$.*

PROOF: Easy. ∎

Corollary 6.4.2.1. *The Cartesian product of two finite sets is finite.*

Lemma 6.4.3. *For any natural numbers m and n we have $m^{n^+} = m^n m$.*

PROOF: Easy. ∎

Corollary 6.4.3.1. *If A and B are finite sets then A^B is finite.*

6.5 Ordering on the Natural Numbers

Lemma 6.5.1. *For any natural numbers m and n, $m \in n$ if and only if $m^+ \in n^+$.*

PROOF:
$\langle 1 \rangle 1$. $\forall m, n \in \omega (m \in n \Rightarrow m^+ \in n^+)$
$\langle 2 \rangle 1$. $\forall m \in \omega (m \in 0 \Rightarrow m^+ \in 0^+)$
PROOF: Vacuous.
$\langle 2 \rangle 2$. For all $n \in \omega$, if $\forall m \in n . m^+ \in n^+$ then $\forall m \in n^+ . m^+ \in n^{++}$

$\langle 3\rangle 1.$ LET: $n \in \omega$
$\langle 3\rangle 2.$ ASSUME: $\forall m \in n . m^+ \in n^+$
$\langle 3\rangle 3.$ LET: $m \in n^+$
$\langle 3\rangle 4.$ CASE: $m \in n$
$\langle 4\rangle 1.$ $m^+ \in n^+$
PROOF: By $\langle 3\rangle 2$
$\langle 4\rangle 2.$ $m^+ \in n^{++}$
$\langle 3\rangle 5.$ CASE: $m = n$
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 5.1.10).
$\square$

Lemma 6.5.2. *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 5.1.10).
$\square$

Theorem 6.5.3 (Trichotomy Law for ω)**.** *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 6.5.2.
If $m \in n$ and $n \in m$ then $m \in m$ by Theorem 5.1.10, contradicting Lemma 6.5.2.
$\langle 1\rangle 2.$ 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 $0 \in n^+$

⟨2⟩2. For all $m \in \omega$, if $\forall n \in \omega(m \in n \vee m = n \vee n \in m)$ then $\forall n \in \omega(m^+ \in n \vee m^+ = n \vee n \in m^+)$

⟨3⟩1. LET: $m \in \omega$

⟨3⟩2. ASSUME: $\forall n \in \omega(m \in n \vee m = n \vee n \in m)$

⟨3⟩3. LET: $n \in \omega$

⟨3⟩4. CASE: $m \in n$

PROOF: Then $m \in n^+$

⟨3⟩5. CASE: $m = n$

PROOF: Then $m \in n^+$

⟨3⟩6. CASE: $n \in m$

PROOF: Then $n^+ \in m^+$ by Lemma 6.5.1 so $n^+ \in m$ or $n^+ = m$.

□

Corollary 6.5.3.1. *The relation $\in$ is a linear ordering on ω.*

Corollary 6.5.3.2. *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 5.1.10.

⟨2⟩3. $m \neq n$

PROOF: Lemma 6.5.2.

⟨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 6.5.4. *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 6.5.1. □

Theorem 6.5.5. *For any non-zero natural number p, the function that maps n to np is strictly monotone.*

PROOF: Easy induction on p using Theorem 6.5.4. □

Theorem 6.5.6 (Strong Induction)**.** *Let A be a subset of ω 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. $\square$

Theorem 6.5.7 (Well-Ordering of ω)**.** *The ordering $<$ on ω is a well-ordering.*

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

Lemma 6.5.8. *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:
$\langle 1 \rangle 1$. For all m, p, we have $m \in m + p^+$
  PROOF: $m = m + 0 \in m + p^+$
$\langle 1 \rangle 2$. For all m, n, if $m \in n$ then there exists p such that $n = m + p^+$
  $\langle 2 \rangle 1$. For all m, if $m \in 0$ then there exists p such that $0 = m + p^+$
    PROOF: Vacuous.
  $\langle 2 \rangle 2$. For all $n \in \omega$, if $\forall m \in n . \exists p \in \omega . n = m + p^+$ then $\forall m \in n^+ . \exists p \in \omega . n^+ = m + p^+$
    $\langle 3 \rangle 1$. LET: $n \in \omega$
    $\langle 3 \rangle 2$. ASSUME: $\forall m \in n . \exists p \in \omega . n = m + p^+$
    $\langle 3 \rangle 3$. LET: $m \in n^+$
    $\langle 3 \rangle 4$. CASE: $m \in n$
      $\langle 4 \rangle 1$. PICK p such that $n = m + p^+$
      $\langle 4 \rangle 2$. $n^+ = m + p^{++}$
    $\langle 3 \rangle 5$. CASE: $m = n$
      PROOF: $n^+ = m + 0^+$

$\square$

Lemma 6.5.9. *For natural numbers m, n, p and q, if $m \in n$ and $p \in q$ then $mp + nq \in mq + np$.*

$\langle 1 \rangle 1$. PICK natural numbers a and b such that $n = m + a^+$ and $q = p + b^+$
  PROOF: Lemma 6.5.8.
$\langle 1 \rangle 2$. $mp + nq = mq + np + (a^+ + b)^+$
$\langle 1 \rangle 3$. $mp + nq \in mq + np$
  PROOF: Lemma 6.5.8.

Chapter 7

Integers

7.1 The Integers

Theorem 7.1.1. *The relation $\sim$ is an equivalence relation on $\omega \times \omega$, where $(m,n) \sim (p,q)$ iff $m+q=n+p$.*

PROOF:
$\langle 1 \rangle 1$. The relation $\sim$ is reflexive on ω^2
  PROOF: For any m, n, we have $m+n=m+n$ and so $(m,n) \sim (m,n)$.
$\langle 1 \rangle 2$. The relation $\sim$ is symmetric.
  PROOF: If $m+q=n+p$ then $p+n=q+m$.
$\langle 1 \rangle 3$. The relation $\sim$ is transitive.
  $\langle 2 \rangle 1$. ASSUME: $(m,n) \sim (p,q) \sim (r,s)$
  $\langle 2 \rangle 2$. $m+q=n+p$
  $\langle 2 \rangle 3$. $p+s=q+r$
  $\langle 2 \rangle 4$. $m+p+q+s=n+p+q+r$
  $\langle 2 \rangle 5$. $m+s=n+r$
    PROOF: By cancellation of addition in ω.
∎

Definition 7.1.2. The set $\mathbb{Z}$ of *integers* is the quotient set $(\omega \times \omega)/\sim$.

Lemma 7.1.3. *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 7.1.4 (Addition)**.** Addition $+$ on $\mathbb{Z}$ is the binary operation such that

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

Theorem 7.1.5. *Addition on $\mathbb{Z}$ is commutative.*

PROOF: From the definition. ∎

Theorem 7.1.6. *Addition on $\mathbb{Z}$ is associtative.*

PROOF: Easy. ∎

Definition 7.1.7 (Zero)**.** The zero in the integers is $0 = [(0, 0)]$.

Theorem 7.1.8. *For any integer a we have $a + 0 = 0$.*

PROOF: Easy. ∎

Theorem 7.1.9. *For any integer a, there exists an integer b such that $a+b = 0$.*

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

Lemma 7.1.10. *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:
⟨1⟩1. ASSUME: $m + n' = m' + n$ and $p + q' = p' + q$
⟨1⟩2. $mp + n'p = m'p + np$
⟨1⟩3. $m'q + nq = mq + n'q$
⟨1⟩4. $mp + mq' = mp' + mq$
⟨1⟩5. $n'p' + n'q = n'p + n'q'$
⟨1⟩6. $mp + n'p + m'q + nq + mp + mq' + n'p' + n'q = m'p + np + mq + n'q + mp' + mq + n'p + n'q'$
⟨1⟩7. $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$
∎

Definition 7.1.11 (Multiplication)**.** *Multiplication* $\cdot$ is the binary operation on $\mathbb{Z}$ such that

$$[(m, n)][(p, q)] = [(mp + nq, mq + np)]$$

Theorem 7.1.12. *Multiplication is commutative.*

PROOF: Easy. ∎

Theorem 7.1.13. *Multiplication is associative.*

PROOF: Easy. ∎

Theorem 7.1.14. *Multiplication is distributive over addition.*

PROOF: Easy. ∎

Definition 7.1.15. The integer one is $1 = [(1, 0)]$.

Theorem 7.1.16. *For any integer a we have $a1 = a$.*

PROOF: Easy. ∎

Theorem 7.1.17. $0 \neq 1$

PROOF: Easy. ∎

Lemma 7.1.18. *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:
$$\begin{aligned} m + q \in p + n &\Leftrightarrow m + q + n' + q' \in p + n + n' + q' \\ &\Leftrightarrow m' + n + q + q' \in p' + n + n' + q \\ &\Leftrightarrow m' + q' \in p' + n' \end{aligned}$$
∎

Definition 7.1.19 (Ordering)**.** The ordering $<$ on $\mathbb{Z}$ is defined by: $[(m, n)] < [(p, q)]$ iff $m + q \in n + p$.

Theorem 7.1.20. *The relation* $<$ *is a linear ordering on* $\mathbb{Z}$.

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

Theorem 7.1.21. *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 ω.

Corollary 7.1.21.1. *If* $a + c = b + c$ *then* $a = b$.

Theorem 7.1.22. *If* $0 < c$, *then the function that maps an integer* a *to* ac *is strictly monotone.*

PROOF:
$\langle 1 \rangle 1$. LET: a, b and c be integers.
$\langle 1 \rangle 2$. ASSUME: $0 < c$ and $a < b$
$\langle 1 \rangle 3$. LET: $a = [(m, n)]$
$\langle 1 \rangle 4$. LET: $b = [(p, q)]$
$\langle 1 \rangle 5$. LET: $c = [(r, s)]$
$\langle 1 \rangle 6$. $s \in r$
$\langle 1 \rangle 7$. $m + q \in p + n$
$\langle 1 \rangle 8$. $(m + q)r + (p + n)s \in (m + q)s + (p + n)r$
  PROOF: Lemma 6.5.9.
$\langle 1 \rangle 9$. $ac < bc$
∎

Lemma 7.1.23. *For integers* a *and* b, $a(-b) = -(ab)$

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

Theorem 7.1.24. *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 7.1.25. *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 7.1.26. *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 7.1.27 (Positive)**.** An integer a is *positive* iff $0 < a$.

Theorem 7.1.28. *Define $E : \omega \to \mathbb{Z}$ by $E(n) = [(n, 0)]$. Then E maps ω 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. □

Lemma 7.1.29. *For any positive integer a and integer b, there exists a natural number k such that $b < ak$.*

Proof: Take $k = |b| + 1$. □

Chapter 8

Cardinal Numbers

8.1 Equinumerosity

Definition 8.1.1 (Equinumerous)**.** Two sets A and B are *equinumerous*, $A \approx B$, iff there exists a bijection between them.

Theorem 8.1.2. *Equinumerosity is an equivalence relation on the class of sets.*

Proof: Easy. □

Theorem 8.1.3 (Cantor 1873)**.** *No set is equinumerous with its power set.*

Proof:
⟨1⟩1. Let: $g : A \to \mathcal{P}A$
Prove: g is not surjective.
⟨1⟩2. Let: $B = \{x \in A : x \notin g(x)\}$
⟨1⟩3. $\forall x \in A.g(x) \neq B$
Proof: Because $x \in B$ iff $x \notin g(x)$.
□

8.2 Ordering Cardinal Numbers

Definition 8.2.1 (Dominated)**.** A set A is *dominated* by a set B, $A \preccurlyeq B$, iff there exists an injection $f : A \to B$.

Lemma 8.2.2. *Domination is a preorder on the class of sets.*

Proof: Easy. □

Lemma 8.2.3. *If $A \subseteq B$ then $A \preccurlyeq B$.*

Proof: The inclusion from A to B is an injection. □

Lemma 8.2.4. *If $A \preccurlyeq B$, $A \approx A'$ and $B \approx B'$ then $A' \preccurlyeq B'$.*

PROOF: Easy. ∎

Definition 8.2.5. Given cardinal numbers κ and λ, we write $\kappa \leq \lambda$ iff $K \preccurlyeq L$, where K is any set of cardinality κ and L is any set of cardinality λ.

We write $\kappa < \lambda$ iff $\kappa \leq \lambda$ and $\kappa \neq \lambda$.

Theorem 8.2.6 (Schröder-Bernstein)**.** *If $A \preccurlyeq B$ and $B \preccurlyeq A$ then $A \approx B$.*

PROOF:
⟨1⟩1. LET: $f : A \to B$ and $g : B \to A$ be one-to-one.
⟨1⟩2. Define the sequence of sets $C_n \subseteq A$ by:

$$C_0 = A - \operatorname{ran} g$$
$$C_{n+1} = g(f(C_n))$$

⟨1⟩3. Define $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if } \exists n \in \mathbb{N}. x \in C_n \\ g^{-1}(x) & \text{otherwise} \end{cases}$$

⟨1⟩4. h is injective.
⟨2⟩1. LET: $x, y \in A$
⟨2⟩2. ASSUME: $h(x) = h(y)$
⟨2⟩3. CASE: $x \in C_m$, $y \in C_n$
PROOF: We have $f(x) = f(y)$ so $x = y$
⟨2⟩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 $y \in C_{m+1}$.
⟨2⟩5. CASE: $x, y \notin \bigcup_n C_n$
PROOF: We have $g^{-1}(x) = g^{-1}(y)$ so $x = y$.
⟨1⟩5. h is surjective.
⟨2⟩1. LET: $y \in B$
⟨2⟩2. ASSUME: $y \notin f(C_n)$ for all n
⟨2⟩3. $g(y) \notin C_n$ for all n
⟨2⟩4. $y = h(g(y))$
∎

Corollary 8.2.6.1. *The relation $\leq$ is a partial order on the class of cardinal numbers.*

Theorem 8.2.7. *Let κ, λ and μ be cardinal numbers.*

1. $\kappa \leq \lambda \Rightarrow \kappa + \mu \leq \lambda + \mu$
2. $\kappa \leq \lambda \Rightarrow \kappa\mu \leq \lambda\mu$
3. $\kappa \leq \lambda \Rightarrow \kappa^\mu \leq \lambda^\mu$
4. $\kappa \leq \lambda \Rightarrow \mu^\kappa \leq \mu^\lambda$ *if κ and μ are not both zero.*

PROOF: Parts 1–3 are easy. For part 4:
Let $|K| = \kappa$, $|L| = \lambda$ and $|M| = \mu$ with $K \subseteq L$.
If $M = \emptyset$ then $\kappa \neq 0$ so $\mu^\kappa = 0 \leq \mu^\lambda$.

Otherwise, pick $a \in M$. Define $\Phi : M^K \to M^L$ by:

$$\Phi(f)(x) = \begin{cases} f(x) & \text{if } x \in K \\ a & \text{if } x \notin K \end{cases}$$

Then Φ is an injection. ∎

Theorem 8.2.8 (Cardinal Comparability). *The Axiom of Choice is equivalent to the statement: for any sets C and D, either $C \preccurlyeq D$ or $D \preccurlyeq C$.*

Proof:
⟨1⟩1. If Zorn's Lemma then Cardinal Comparability.
  ⟨2⟩1. Assume: Zorn's Lemma
  ⟨2⟩2. Let: C and D be sets.
  ⟨2⟩3. Let: $\mathcal{A}$ be the set of all injective functions f with $\operatorname{dom} f \subseteq C$ and $\operatorname{ran} f \subseteq D$
  ⟨2⟩4. For every chain $\mathcal{B} \subseteq \mathcal{A}$ we have $\bigcup \mathcal{B} \in \mathcal{A}$
  ⟨2⟩5. Let: $f \in \mathcal{A}$ be maximal
  ⟨2⟩6. $\operatorname{dom} f = C$ or $\operatorname{ran} f = D$
  ⟨2⟩7. f is an injective function $C \to D$ or f^{-1} is an injective function $D \to C$
⟨1⟩2. If Cardinal Comparability then the Well-Ordering Theorem.
  ⟨2⟩1. Assume: Cardinal Comparability
  ⟨2⟩2. Let: A be any set
  ⟨2⟩3. Pick an ordinal α not dominated by A
    Proof: Hartogs' Theorem.
  ⟨2⟩4. $A \preccurlyeq \alpha$
  ⟨2⟩5. Pick an injective function $f : A \to \alpha$
  ⟨2⟩6. Define $<$ on A by: $x < y$ iff $f(x) \in f(y)$
  ⟨2⟩7. $<$ is a well ordering on A.
∎

Theorem 8.2.9 (Choice). *For any infinite set A, we have $\omega \preccurlyeq A$.*

Proof:
⟨1⟩1. Let: A be an infinite set.
⟨1⟩2. Pick a choice function F for A
⟨1⟩3. Define $f : \omega \to A$ by recursion by: $f(n) = F(A - \{f(0), f(1), \ldots, f(n-1)\})$
  Proof: $A - \{f(0), f(1), \ldots, f(n-1)\}$ is nonempty because A is infinite.
⟨1⟩4. f is injective.
∎

Corollary 8.2.9.1 (Choice). *For any infinite cardinal κ we have $\aleph_0 \leq \kappa$.*

Corollary 8.2.9.2 (Choice). *A set is infinite iff it is equinumerous to a proper subset of itself.*

Proposition 8.2.10 (Choice). *If there exists a surjection $A \to B$ then $B \preccurlyeq A$.*

Proof: Any surjection $A \to B$ has a right inverse which is an injection $B \to A$.

8.3 Countable Sets

Definition 8.3.1 (Countable)**.** A set is *countable* iff it is dominated by ω.

Proposition 8.3.2. *Any subset of a countable set is countable.*

PROOF: Easy. $\square$

The union of two countable sets is countable.

PROOF: Because $\aleph_0 + \aleph_0 = \aleph_0$ $\square$

Proposition 8.3.3. *The product of two countable sets is countable.*

PROOF: Because $\aleph_0 \aleph_0 = \aleph_0$. $\square$

Proposition 8.3.4 (Choice)**.** *For any infinite set A, the set $\mathcal{P}A$ is uncountable.*

PROOF: If $|A| \geq \aleph_0$ then $|\mathcal{P}A| \geq 2^{\aleph_0}$. $\square$

Theorem 8.3.5 (Choice)**.** *A countable union of countable sets is countable.*

PROOF:
⟨1⟩1. LET: $\mathcal{A}$ be a countable set of countable sets.
⟨1⟩2. ASSUME: w.l.o.g. $\mathcal{A} \neq \emptyset$ and $\emptyset \notin \mathcal{A}$
⟨1⟩3. PICK a surjection $G : \omega \to A$
⟨1⟩4. PICK a function F with domain ω such that, for all m, $F(m)$ is a surjection $\omega \to G(m)$
PROOF: By the Axiom of Choice.
⟨1⟩5. Define $f : \omega \times \omega \to \bigcup A$ by $f(m, n) = F(m)(n)$
⟨1⟩6. f is surjective.
⟨1⟩7. $A \preccurlyeq \omega \times \omega$
$\square$

8.4 Arithmetic of Infinite Cardinals

Lemma 8.4.1 (Choice)**.** *For any infinite cardinal κ we have $\kappa \cdot \kappa = \kappa$.*

PROOF:
⟨1⟩1. LET: κ be an infinite cardinal.
⟨1⟩2. LET: B be a set of cardinality κ.
⟨1⟩3. LET: $\mathcal{H} = \{f : f = \emptyset$ or for some infinite $A \subseteq B, f$ is a bijection between $A \times A$ and $A\}$
⟨1⟩4. For any chain $\mathcal{C} \subseteq \mathcal{H}$, we have $\bigcup \mathcal{C} \in \mathcal{H}$
⟨2⟩1. LET: $\mathcal{C} \subseteq \mathcal{H}$ be a chain.
⟨2⟩2. ASSUME: w.l.o.g. $\mathcal{C}$ has a nonempty element.
PROOF: Otherwise $\bigcup \mathcal{C} = \emptyset \in \mathcal{H}$.
⟨2⟩3. $\bigcup \mathcal{C}$ is an injective function.
⟨2⟩4. LET: $A = \operatorname{ran} \bigcup \mathcal{C}$
⟨2⟩5. A is infinite.
⟨2⟩6. $\bigcup \mathcal{C}$ is a bijection between $A \times A$ and A.

$\langle 3 \rangle 1.$ LET: $a_1, a_2 \in A$
$\langle 3 \rangle 2.$ PICK $f_1, f_2 \in \mathcal{C}$ such that $a_1 \in \operatorname{ran} f_1$ and $a_2 \in \operatorname{ran} f_2$
$\langle 3 \rangle 3.$ ASSUME: w.l.o.g. $f_1 \subseteq f_2$
$\langle 3 \rangle 4.$ $\langle a_1, a_2 \rangle \in \operatorname{dom} f_2$
$\langle 3 \rangle 5.$ $\langle a_1, a_2 \rangle \in \operatorname{dom} \bigcup \mathcal{C}$
$\langle 1 \rangle 5.$ PICK a maximal $f_0 \in \mathcal{H}$
PROOF: Zorn's Lemma.
$\langle 1 \rangle 6.$ $f_0 \neq \emptyset$
PROOF: B has a countable subset A, say, and $A \times A \approx A$.
$\langle 1 \rangle 7.$ PICK $A_0 \subseteq B$ infinite such that f_0 is a bijection between $A_0 \times A_0$ and A_0.
$\langle 1 \rangle 8.$ LET: $\lambda = |A_0|$
$\langle 1 \rangle 9.$ λ is infinite
$\langle 1 \rangle 10.$ $\lambda = \lambda \cdot \lambda$
$\langle 1 \rangle 11.$ $\lambda = \kappa$
$\langle 2 \rangle 1.$ $|B - A_0| < \lambda$
$\langle 3 \rangle 1.$ ASSUME: for a contradiction $\lambda \leq |B - A_0|$
$\langle 3 \rangle 2.$ PICK $D \subseteq B - A_0$ with $|D| = \lambda$
$\langle 3 \rangle 3.$ $(A_0 \cup D) \times (A_0 \cup D) = (A_0 \times A_0) \cup (A_0 \times D) \cup (D \times A_0) \cup (D \times D)$
$\langle 3 \rangle 4.$ $f_0 : A_0 \times A_0 \approx A_0$
$\langle 3 \rangle 5.$ $|(A_0 \times D) \cup (D \times A_0) \cup (D \times D)| = \lambda$
PROOF:

$$\begin{aligned} |(A_0 \times D) \cup (D \times A_0) \cup (D \times D)| &= \lambda \cdot \lambda + \lambda \cdot \lambda + \lambda \cdot \lambda \\ &= \lambda + \lambda + \lambda && (\langle 1 \rangle 10) \\ &= 3 \cdot \lambda \\ &\leq \lambda \cdot \lambda \\ &= \lambda && (\langle 1 \rangle 10) \end{aligned}$$

$\langle 3 \rangle 6.$ PICK a bijection $g : (A_0 \times D) \cup (D \times A_0) \cup (D \times D) \approx D$
$\langle 3 \rangle 7.$ $f_0 \cup g : (A_0 \cup D) \times (A_0 \cup D) \approx A_0 \cup D$
$\langle 3 \rangle 8.$ Q.E.D.
PROOF: This contradicts the maximality of f_0.
$\langle 2 \rangle 2.$ $\lambda = \kappa$
PROOF:

$$\begin{aligned} \kappa &= |B| \\ &= |A_0| + |B - A_0| \\ &\leq \lambda + \lambda \\ &= 2 \cdot \lambda \\ &\leq \lambda \cdot \lambda \\ &= \lambda \\ &\leq \kappa \end{aligned}$$

$\square$

Corollary 8.4.1.1 (Absorption Law of Cardinal Arithmetic (Choice))**.** *Let κ and λ be cardinal numbers, the larger of which is infinite and the smaller of* *which is nonzero. Then*

$$\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda) \ .$$

PROOF:
⟨1⟩1. ASSUME: w.l.o.g. $\kappa \leq \lambda$
⟨1⟩2. $\kappa + \lambda = \lambda$
PROOF:

$$\begin{aligned} \lambda &\leq \kappa + \lambda \\ &\leq \lambda + \lambda \\ &= 2 \cdot \lambda \\ &\leq \lambda \cdot \lambda \\ &= \lambda \end{aligned}$$

⟨1⟩3. $\kappa \cdot \lambda = \lambda$
PROOF:

$$\begin{aligned} \lambda &= 1 \cdot \lambda \\ &\leq \kappa \cdot \lambda \\ &\leq \lambda \cdot \lambda \\ &= \lambda \end{aligned}$$

□

8.5 Rank

Definition 8.5.1. Define the set V_α for every ordinal α by transfinite recursion thus:

$$V_\alpha = \bigcup \{\mathcal{P} V_\beta : \beta \in \alpha\} \ .$$

Lemma 8.5.2. *For any ordinal α, V_α is a transitive set.*

PROOF:
⟨1⟩1. LET: α be an ordinal.
⟨1⟩2. LET: $x \in y \in V_\alpha$
⟨1⟩3. PICK $\beta \in \alpha$ such that $y \in \mathcal{P} V_\beta$
⟨1⟩4. $x \in V_\beta$
⟨1⟩5. PICK $\gamma \in \beta$ such that $x \in \mathcal{P} V_\gamma$
⟨1⟩6. $\gamma \in \alpha$ and $x \in \mathcal{P} V_\gamma$
⟨1⟩7. $x \in V_\alpha$
□

Theorem 8.5.3. *For ordinals $\beta \in \alpha$ we have $V_\beta \subseteq V_\alpha$.*

PROOF:
$$\begin{aligned} V_\beta &= \bigcup_{\gamma\in\beta} \mathcal{P}V_\gamma \\ &\subseteq \bigcup_{\gamma\in\alpha} \mathcal{P}V_\gamma \\ &= V_\alpha \end{aligned}$$
□

Theorem 8.5.4.
$$V_0 = \emptyset$$

PROOF: Immediate from definitions. □

Theorem 8.5.5. *For any ordinal α, $V_{\alpha^+} = \mathcal{P}V_\alpha$.*

PROOF:
$$\begin{aligned} V_{\alpha^+} &= \bigcup_{\beta\leq\alpha} \mathcal{P}V_\beta \\ &= \mathcal{P}V_\beta \end{aligned}$$
by Theorem 8.5.3. □

Theorem 8.5.6. *For λ a limit ordinal, $V_\lambda = \bigcup_{\beta<\lambda} V_\beta$.*

PROOF:
$$\begin{aligned} V_\lambda &= \bigcup_{\beta<\lambda} \mathcal{P}V_\beta \\ &= \bigcup_{\beta<\lambda} V_{\beta+} \\ &= \bigcup_{\beta<\lambda} V_\beta \end{aligned}$$
since $\beta < \lambda$ iff $\beta^+ < \lambda$. □

Definition 8.5.7 (Grounded, Rank)**.** A set A is *grounded* iff $\exists\alpha.A \subseteq V_\alpha$. The *rank* of a grounded set A, $\operatorname{rank} A$, is then the least ordinal α such that $A \subseteq V_\alpha$.

Theorem 8.5.8. *If A is grounded and $a \in A$ then a is grounded and* $\operatorname{rank} a < \operatorname{rank} A$.

PROOF: We have $a \in A \subseteq V_{\operatorname{rank} A}$. So $a \in \mathcal{P}V_\alpha$ for some $\alpha < \operatorname{rank} A$, i.e. $a \subseteq V_\alpha$ for some $\alpha < \operatorname{rank} A$, as required.

Theorem 8.5.9. *If every member of A is grounded then A is grounded and*
$$\operatorname{rank} A = \sup_{a\in A} (\operatorname{rank} a)^+ \enspace .$$

PROOF:
$\langle 1\rangle 1.$ LET: $\alpha = \sup_{a\in A}(\operatorname{rank} a)^+$
$\langle 1\rangle 2.$ $A \subseteq V_\alpha$

⟨2⟩1. LET: $a \in A$
⟨2⟩2. $a \subseteq V_{\mathrm{rank}\, a}$
⟨2⟩3. $a \in V_{(\mathrm{rank}\, a)^+}$
⟨2⟩4. $a \in V_\alpha$
⟨1⟩3. If $A \subseteq V_\beta$ then $\alpha \leq \beta$
⟨2⟩1. ASSUME: $A \subseteq V_\beta$
⟨2⟩2. $\forall a \in A. a \in V_\beta$
⟨2⟩3. $\forall a \in A. \exists \gamma < \beta. a \subseteq V_\gamma$
⟨2⟩4. $\forall a \in A. \exists \gamma < \beta. \mathrm{rank}\, a \leq \gamma$
⟨2⟩5. $\forall a \in A. \mathrm{rank}\, a < \beta$
⟨2⟩6. $\forall a \in A. (\mathrm{rank}\, a)^+ \leq \beta$
⟨2⟩7. $\alpha \leq \beta$
□

Theorem 8.5.10. *Every set is grounded.*

PROOF:
⟨1⟩1. ASSUME: for a contradiction c is not grounded.
⟨1⟩2. LET: B be the transitive closure of $\{c\}$.
⟨1⟩3. LET: $A = \{x \in B : x \text{ is not grounded}\}$
⟨1⟩4. PICK $m \in A$ such that $m \cap A = \emptyset$
PROOF: By the Axiom of Regularity.
⟨1⟩5. Every member of m is grounded.
PROOF: Every member of m is in B by transitivity but not in A.
⟨1⟩6. m is grounded.
PROOF: Theorem 8.5.9.
⟨1⟩7. Q.E.D.
PROOF: This contradicts the fact that $m \in A$.
□

Theorem 8.5.11. *Let A be any set and A^t its transitive closure. Let M^t be the transitive closure of the relation $\{\langle x, y\rangle : x \in y \in A^t\}$. Define $E : A^t \to \mathbf{V}$ by transfinite recursion thus:*

$$E(a) = \{E(x) : xM^t a\} \qquad (a \in A^t) \ .$$

Then $E(a) = \mathrm{rank}\, a$ for all $a \in A^t$, and $\mathrm{ran}\, E = \mathrm{rank}\, A$.

PROOF:
⟨1⟩1. M^t is well-founded
PROOF: Theorem 2.10.2.
⟨1⟩2. $\forall a \in A^t. \mathrm{rank}\, a = \{\mathrm{rank}\, x : xM^t a\}$
⟨2⟩1. $\forall x, a \in A^t. xM^t a \Rightarrow \mathrm{rank}\, x < \mathrm{rank}\, a$
PROOF: Theorem 8.5.8.
⟨2⟩2. $\forall x \in A^t. \forall \alpha < \mathrm{rank}\, a. \exists x M^t a. \alpha = \mathrm{rank}\, x$
⟨3⟩1. LET: $a \in A^t$
⟨3⟩2. ASSUME: $\forall b M^t a. \forall \alpha < \mathrm{rank}\, b. \exists x M^t b. \alpha = \mathrm{rank}\, x$
⟨3⟩3. LET: $\alpha < \mathrm{rank}\, a$

⟨3⟩4. Pick $b \in a$ such that $\alpha \leq \operatorname{rank} b$

Proof: Theorem 8.5.9.

⟨3⟩5. Case: $\alpha < \operatorname{rank} b$

⟨4⟩1. Pick $xM^t b$ such that $\alpha = \operatorname{rank} x$

Proof: By ⟨3⟩2

⟨4⟩2. $xM^t a$

⟨3⟩6. Case: $\alpha = \operatorname{rank} b$

Proof: We have $bM^t a$ and $\alpha = \operatorname{rank} b$ as required.

⟨3⟩7. Q.E.D.

Proof: This concludes the proof by transfinite induction over M^t (⟨1⟩1).

⟨1⟩3. $\forall a \in A^t.E(a) = \operatorname{rank} a$

Proof: By transfinite induction on a.

⟨1⟩4. $\operatorname{ran} E = \operatorname{rank} A$

Proof: From ⟨1⟩3 substituting $\{A\}$ for A.

□

8.6 Models of Set Theory

Theorem 8.6.1. *For any limit ordinal $\lambda > \omega$, we have V_λ is a model of Zermelo set theory.*

Proof: Easy. □

Theorem 8.6.2 (Choice)**.** *For any ordinal α, we have V_α is a model of the Axiom of Choice.*

Proof: Easy. □

Lemma 8.6.3 (Choice)**.** *There exists a well-ordered structure in $V_{\omega 2}$ whose ordinal number is not in $V_{\omega 2}$.*

Proof: Pick an uncountable set $S \in V_{\omega 2}$. Pick a well-ordering R on S. Then $\langle S, R \rangle \in V_{\omega 2}$ but its ordinal is not, because every ordinal in $V_{\omega 2}$ is $< \omega 2$ hence countable. □

Corollary 8.6.3.1 (Choice)**.** *The set $V_{\omega 2}$ is not a model of ZFC.*

Corollary 8.6.3.2. *The Replacement Axioms are not provable from the Zermelo axioms.*

8.7 Cofinality

Definition 8.7.1 (Cofinal)**.** Let λ be a limit ordinal and S a set of smaller ordinals. Then S is *cofinal* in λ iff $\lambda = \sup S$.

Definition 8.7.2 (Cofinality)**.** The *cofinality* of a limit ordinal λ, $\operatorname{cf} \lambda$, is the least cardinal κ such that λ is the limit of κ smaller ordinals.

We also define $\operatorname{cf} 0 = 0$ and $\operatorname{cf} \alpha^+ = 1$.

Definition 8.7.3 (Regular Cardinal)**.** A cardinal κ is *regular* iff $\mathrm{cf}\,\kappa = \kappa$; otherwise κ is *singular.*

Theorem 8.7.4. *For every ordinal α, the cardinal $\aleph_{\alpha+1}$ is regular.*

Proof: If S is a set of fewer than $\aleph_{\alpha+1}$ smaller ordinals then $\forall \beta \in S . |\beta| \leq \aleph_\alpha$ and so

$$|\bigcup S| \leq |S| \cdot \aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha \ . \square$$

Theorem 8.7.5. *For every limit ordinal λ, we have* $\mathrm{cf}\,\aleph_\lambda = \mathrm{cf}\,\lambda$.

Proof:
⟨1⟩1. Let: λ be a limit ordinal.
⟨1⟩2. $\mathrm{cf}\,\aleph_\lambda \leq \mathrm{cf}\,\lambda$
  ⟨2⟩1. Pick a set S with $|S| = \mathrm{cf}\,\lambda$ and $\bigcup S = \lambda$
  ⟨2⟩2. $\aleph_\lambda = \sup_{\alpha \in S} \aleph_\alpha$
    Proof: Theorem 4.0.18.
⟨1⟩3. $\mathrm{cf}\,\lambda \leq \mathrm{cf}\,\aleph_\lambda$
  ⟨2⟩1. Let: A be a set of smaller ordinals such that $\aleph_\lambda = \sup A$
      Prove: $\mathrm{cf}\,\lambda \leq |A|$
  ⟨2⟩2. Let: $B = \{\gamma \in \lambda : \exists \alpha \in A . |\alpha| = \aleph_\gamma\}$
  ⟨2⟩3. $|B| \leq |A|$
  ⟨2⟩4. $\sup B = \lambda$
    ⟨3⟩1. $\forall \alpha \in A . \alpha \in \aleph_{\sup B+1}$
      ⟨4⟩1. Let: $\alpha \in A$
      ⟨4⟩2. $|\alpha| \leq \aleph_{\sup B}$
      ⟨4⟩3. $\alpha \in \aleph_{\sup B+1}$
    ⟨3⟩2. $\lambda \underline{\in} \sup B + 1$
      ⟨4⟩1. $\aleph_\lambda \leq \aleph_{\sup B+1}$
    ⟨3⟩3. $\lambda = \sup B$
      ⟨4⟩1. $\lambda \leq \sup B$
        Proof: From ⟨3⟩2 since λ is a limit ordinal.
      ⟨4⟩2. $\sup B \leq \lambda$
        Proof: From ⟨2⟩2.

$\square$

Definition 8.7.6 (Weakly Inaccessible)**.** An ordinal λ is *weakly inaccessible* iff $\aleph_\lambda$ is regular.

Lemma 8.7.7. *Let f be an α-sequence of ordinals. Then there exists an increasing β-sequence g for some $\beta \leq \alpha$ such that* $\sup \mathrm{ran}\, f = \sup \mathrm{ran}\, g$.

Proof:
⟨1⟩1. Let: h be the sequence defined by transfinite recursion thus: h_ξ is the least γ such that $\forall \delta < \xi . f_{h_\delta} < f_\gamma$ if any such γ exists; otherwise the sequence halts.
⟨1⟩2. Let: $\beta = \mathrm{dom}\, h$
⟨1⟩3. $g_\xi = f_{h_\xi}$ for $\xi < \beta$

$\langle 1\rangle 4.$ $\sup \operatorname{ran} g \leq \sup \operatorname{ran} f$
PROOF: Since g is a subsequence of f.
$\langle 1\rangle 5.$ $\sup \operatorname{ran} f \leq \sup \operatorname{ran} g$
$\langle 2\rangle 1.$ $\forall \xi < \beta . \forall \delta \leq h_\xi . f_\delta \leq g_\xi$
$\langle 3\rangle 1.$ LET: $\xi < \beta$
$\langle 3\rangle 2.$ LET: $\delta \leq h_\xi$
$\langle 3\rangle 3.$ $f_\delta \leq f_{h_\xi}$
$\langle 4\rangle 1.$ ASSUME: $\delta < h_\xi$
$\langle 4\rangle 2.$ PICK $\alpha < \xi$ such that $f_delta \leq f_{h_\alpha}$
$\langle 4\rangle 3.$ $f_\delta \leq f_{h_\alpha} \leq f_{h_\xi}$
$\langle 3\rangle 4.$ $f_{h_\xi} = g_\xi$
$\langle 2\rangle 2.$ $\forall \xi < \beta . f_\xi \leq g_\xi$
$\langle 2\rangle 3.$ CASE: $\beta = \alpha$
PROOF: Then $\sup \operatorname{ran} f \leq \sup \operatorname{ran} g$ immediately.
$\langle 2\rangle 4.$ CASE: $\beta < \alpha$
$\langle 3\rangle 1.$ There is no γ such that $g_\delta < f_\gamma$ for all $\delta < \beta$
PROOF: This is the condition for the sequence h to halt.
$\langle 3\rangle 2.$ For all γ, there exists δ such that $f_\gamma < g_\delta$
$\langle 3\rangle 3.$ $\sup \operatorname{ran} f \leq \sup \operatorname{ran} g$
□

Theorem 8.7.8. *Let λ be a limit ordinal. Then there exists an increasing $(\operatorname{cf} \lambda)$-sequence of ordinals that converges to λ.*

PROOF:
$\langle 1\rangle 1.$ PICK a set S with $|S| = \operatorname{cf} \lambda$ and $\lambda = \sup S$
$\langle 1\rangle 2.$ PICK a bijection $f : \operatorname{cf} \lambda \approx S$
$\langle 1\rangle 3.$ PICK an increasing β-sequence converging to λ with $\beta \leq \operatorname{cf} \lambda$
PROOF: Lemma 8.7.7.
$\langle 1\rangle 4.$ $\beta = \operatorname{cf} \lambda$
PROOF: By leastness of $\operatorname{cf} \lambda$.
□

Corollary 8.7.8.1. *For any limit ordinal λ, we have $\operatorname{cf} \lambda$ is the least ordinal α such that there exists an increasing α-sequence of ordinals $< \lambda$ that converges to λ.*

Theorem 8.7.9. *For any ordinal λ, we have $\operatorname{cf} \lambda$ is a regular cardinal.*

PROOF:
$\langle 1\rangle 1.$ ASSUME: w.l.o.g. λ is a limit ordinal.
$\langle 1\rangle 2.$ PICK an increasing $\operatorname{cf} \lambda$-sequence f of ordinals $< \lambda$ that converges to λ.
$\langle 1\rangle 3.$ LET: S be a set of ordinals $< \operatorname{cf} \lambda$ such that $\operatorname{cf} \lambda = \sup S$.
$\langle 1\rangle 4.$ $f(S)$ is cofinal in λ
$\langle 2\rangle 1.$ LET: $\alpha < \lambda$
$\langle 2\rangle 2.$ PICK $\beta < \operatorname{cf} \lambda$ such that $\alpha < f(\beta) < \lambda$
PROOF: Since f converges to λ.
$\langle 2\rangle 3.$ PICK $\gamma \in S$ such that $\beta < \gamma$

Proof: Since $\sup S = \mathrm{cf}\,\lambda$.
$\langle 2\rangle 4$. $\alpha < f(\gamma) \in f(S)$
$\langle 1\rangle 5$. $\mathrm{cf}\,\lambda \leq |S|$
Proof: We have $\mathrm{cf}\,\lambda \leq |f(S)| = |S|$
$\langle 1\rangle 6$. $\mathrm{cf}\,\mathrm{cf}\,\lambda = \mathrm{cf}\,\lambda$
□

Theorem 8.7.10. *Let λ be an infinite cardinal. Then $\mathrm{cf}\,\lambda$ is the least cardinal κ such that λ can be decomposed as the union of κ sets each with cardinality $< \lambda$.*

Proof:
$\langle 1\rangle 1$. λ can be decomposed as the union of $\mathrm{cf}\,\lambda$ sets each with cardinality $< \lambda$
Proof: Since λ is the union of a set of $\mathrm{cf}\,\lambda$ smaller ordinals.
$\langle 1\rangle 2$. If $\lambda = \bigcup \mathcal{A}$ where $\forall X \in \mathcal{A}.|X| < \lambda$ then $\mathrm{cf}\,\lambda \leq |\mathcal{A}$.
$\langle 2\rangle 1$. Let: $\kappa = |\mathcal{A}|$
$\langle 2\rangle 2$. Let: $\mathcal{A} = \{A_\xi : \xi < \kappa\}$
$\langle 2\rangle 3$. $\lambda = \bigcup_{\xi<\kappa} A_\xi$
$\langle 2\rangle 4$. $\forall \xi < \kappa.|A_\xi| < \lambda$
$\langle 2\rangle 5$. Let: $\mu = \sup_{\xi<\kappa} |A_\xi|$
$\langle 2\rangle 6$. $\lambda \leq \mu \cdot \kappa$
Proof: Since $\lambda = |\bigcup_{\xi<\kappa} A_\xi|$
$\langle 2\rangle 7$. Case: $\lambda \leq \kappa$
Proof: Then $\mathrm{cf}\,\lambda \leq \lambda \leq \kappa$
$\langle 2\rangle 8$. Case: $\kappa < \lambda$
$\langle 3\rangle 1$. $\lambda = \mu$
Proof: Since $\lambda \leq \mu \cdot \kappa \leq \lambda \cdot \lambda = \lambda$
$\langle 3\rangle 2$. λ is the supremum of κ smaller ordinals.
$\langle 3\rangle 3$. $\mathrm{cf}\,\lambda \leq \kappa$
□

Theorem 8.7.11 (König's Theorem (Choice))**.** *For any infinite cardinal κ we have $\kappa < \mathrm{cf}\,2^\kappa$*

Proof:
$\langle 1\rangle 1$. Assume: for a contradiction $\mathrm{cf}\,2^\kappa \leq \kappa$
$\langle 1\rangle 2$. Pick a set S with $|S| = 2^\kappa$
$\langle 1\rangle 3$. Pick a κ-sequence of sets A_ξ with $S^\kappa = \bigcup_{\xi<\kappa} A_\xi$ and $\forall \xi < \kappa.|A_\xi| < 2^\kappa$
Proof: Since $|S^\kappa| = 2^\kappa$
$\langle 1\rangle 4$. $\forall \xi < \kappa.\{g(\xi) : g \in A_\xi\} \subset S$
Proof: Since $|\{g(\xi) : g \in A_\xi\}| \leq |A_\xi| < 2^\kappa$
$\langle 1\rangle 5$. For all $\xi < \kappa$, Pick $s_\xi \in S - \{g(\xi) : g \in A_\xi\}$
$\langle 1\rangle 6$. $s \in S^\kappa$
$\langle 1\rangle 7$. $\forall \xi < \kappa.s \notin A_\xi$
$\langle 1\rangle 8$. Q.E.D.
Proof: This contradicts $\langle 1\rangle 3$.
□

Corollary 8.7.11.1. $2^{\aleph_0} \neq \aleph_\omega$

Proof: Since $\mathrm{cf}\,\aleph_\omega = \aleph_0$ and $\mathrm{cf}\,2^{\aleph_0} > \aleph_0$. □

8.8 Inaccessible Cardinals

Definition 8.8.1 (Inaccessible Cardinal)**.** A cardinal κ is *inaccessible* iff:

- $\kappa > \aleph_0$
- For every cardinal $\lambda < \kappa$ we have $2^\lambda < \kappa$
- κ is regular.

Lemma 8.8.2. *For any ordinal α and limit ordinal λ,*

$$V_{\alpha+\lambda} = \bigcup_{\delta<\lambda} V_{\alpha+\delta}$$

Proof:
⟨1⟩1. $V_{\alpha+\lambda} = \bigcup_{\delta<\lambda} V_{\alpha+\delta}$
  ⟨2⟩1. Let: $x \in V_{\alpha+\lambda}$
  ⟨2⟩2. Pick $\beta < \alpha + \lambda$ such that $x \in V_\beta$
  ⟨2⟩3. Case: $\beta < \alpha$
    Proof: Then $x \in V_{\alpha+0}$.
  ⟨2⟩4. Case: $\alpha \leq \beta$
    ⟨3⟩1. Let: δ be the ordinal such that $\beta = \alpha + \delta$
    ⟨3⟩2. $x \in V_{\alpha+\delta}$ and $\delta < \lambda$
⟨1⟩2. $\bigcup_{\delta<\lambda} V_{\alpha+\delta} \subseteq V_{\alpha+\lambda}$
□

Lemma 8.8.3. *For any ordinal α we have $|V_{\omega+\alpha}| = \beth_\alpha$.*

Proof:
⟨1⟩1. $|V_\omega| = \beth_0$
  Proof: Since V_ω is the union of an ω-sequence of finite sets of increasing size.
⟨1⟩2. For any ordinal α, if $|V_{\omega+\alpha}| = \beth_\alpha$ then $|V_{\omega+\alpha^+}| = \beth_{\alpha^+}$
⟨1⟩3. For any limit ordinal λ, if $\forall \alpha < \lambda. |V_{\omega+\alpha}| = \beth_\alpha$ then $|V_{\omega+\lambda}| = \beth_\lambda$
  ⟨2⟩1. Let: λ be a limit ordinal.
  ⟨2⟩2. Assume: $\forall \alpha < \lambda. |V_{\omega+\alpha}| = \beth_\alpha$
  ⟨2⟩3. $|V_{\omega+\lambda}| \geq \beth_\lambda$
    Proof:

$$\begin{aligned} |V_{\omega+\lambda}| &= |\bigcup_{\delta<\lambda} V_{\omega+\delta}| && \text{(Lemma 8.8.2)} \\ &\geq \sup_{\delta<\lambda} |V_{\omega+\delta}| \\ &= \sup_{\delta<\lambda} \beth_\delta \\ &= \beth_\lambda \end{aligned}$$

⟨2⟩4. $\beth_\lambda \leq |V_{\omega+\lambda}|$

Proof:

$$\begin{aligned} |V_{\omega+\lambda}| &= |\bigcup_{\delta<\lambda} V_{\omega+\delta}| \\ &\leq |\lambda| \cdot \beth_\lambda \\ &\leq \beth_\lambda \cdot \beth_\lambda \\ &= \beth_\lambda \end{aligned}$$

□

Lemma 8.8.4. *Let κ be an inaccessible cardinal. For any ordinal $\alpha < \kappa$, we have $\beth_\alpha < \kappa$.*

Proof:

⟨1⟩1. $\beth_0 < \kappa$

Proof: By definition of inaccessible.

⟨1⟩2. If $\beth_\alpha < \kappa$ then $\beth_{\alpha^+} < \kappa$

Proof: $\beth_{\alpha^+} = 2^{\beth_\alpha} < \kappa$

⟨1⟩3. If λ is a limit ordinal, $\lambda < \kappa$ and $\forall \alpha < \lambda . \beth_\alpha < \kappa$ then $\beth_\lambda < \kappa$

Proof: Since $\beth_\lambda = \sup_{\alpha<\lambda} \beth_\alpha$ is the supremum of fewer than κ smaller ordinals.

□

Lemma 8.8.5. *Let κ be an inaccessible cardinal. For all $A \in V_\kappa$ we have $|A| < \kappa$.*

Proof: Pick $\alpha < \kappa$ such that $A \subseteq V_\alpha$. Then $|A| \leq |V_\alpha| \leq \beth_\alpha < \kappa$. □

Theorem 8.8.6. *If κ is an inaccessible cardinal then V_κ is a model of ZF.*

Proof: Easy. □