# Mathematics

Robin Adams

August 2, 2023

# Chapter 1

# Sets and Classes

## 1.1 Classes

Our language is the language of first-order logic with equality over one primitive binary predicate $\in$. We call all the objects we reason about *sets*. When $a \in b$, we say $a$ is a *member* or *element* of $b$, or $b$ *contains* $a$. We write $b \ni a$ for $a \in b$, and $a \notin b$ for $\neg(a \in b)$. We write $\forall x \in a.\phi$ as an abbreviation for $\forall x(x \in a \to \phi)$, and $\exists x \in a.\phi$ as an abbreviation for $\exists x(x \in a \wedge \phi)$.

We shall speak informally of *classes* as an abbreviation for talking about predicates. A *class* is determined by a unary predicate $\phi[x]$ (possibly with parameters). We write $\{x \mid \phi[x]\}$ or $\{x : \phi[x]\}$ for the class determined by $\phi[x]$. We write '$a$ is an element of $\{x \mid \phi[x]\}$' or '$a \in \{x \mid \phi[x]\}$' for $\phi[a]$.

We write $\{t[x_1, \ldots, x_n] \mid P[x_1, \ldots, x_n]\}$ for

$$\{y \mid \exists x_1, \ldots, x_n(y = t[x_1, \ldots, x_n] \wedge P[x_1, \ldots, x_n])\} \ .$$

We say two classes $\mathbf{A}$ and $\mathbf{B}$ are *equal*, and write $\mathbf{A} = \mathbf{B}$, iff $\forall x(x \in \mathbf{A} \leftrightarrow x \in \mathbf{B})$.

**Proposition Schema 1.1.1.** *For any class $\mathbf{A}$, the following is a theorem.*

$$\mathbf{A} = \mathbf{A}$$

PROOF: We have $\forall x(x \in \mathbf{A} \Leftrightarrow x \in \mathbf{A})$. $\square$

**Proposition Schema 1.1.2.** *For any classes $\mathbf{A}$ and $\mathbf{B}$, the following is a theorem.*
*If $\mathbf{A} = \mathbf{B}$ then $\mathbf{B} = \mathbf{A}$.*

PROOF: If $\forall x(x \in \mathbf{A} \Leftrightarrow x \in \mathbf{B})$ then $\forall x(x \in \mathbf{B} \Leftrightarrow x \in \mathbf{A})$. $\square$

**Proposition Schema 1.1.3.** *For any classes $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$, the following is a theorem.*
*If $\mathbf{A} = \mathbf{B}$ and $\mathbf{B} = \mathbf{C}$ then $\mathbf{A} = \mathbf{C}$.*

PROOF: If $\forall x(x \in \mathbf{A} \Leftrightarrow x \in \mathbf{B})$ and $\forall x(x \in \mathbf{B} \Leftrightarrow x \in \mathbf{C})$ then $\forall x(x \in \mathbf{A} \Leftrightarrow x \in \mathbf{C})$. $\square$

## 1.1.1 Subclasses

**Definition 1.1.4** (Subclass)**.** We say a class **A** is a *subclass* of **B**, or **B** is a *superclass* of **A**, or **B** *includes* **A**, and write **A** ⊆ **B** or **B** ⊇ **A**, iff every element of **A** is an element of **B**. Otherwise we write **A** ⊈ **B** or **B** ⊉ **A**.

We say **A** is a *proper* subclass of **B**, **B** is a *proper* superclass of **A**, or **B** *properly* includes **A**, and write **A** ⊊ **B** or **B** ⊋ **A**, iff **A** ⊆ **B** and **A** ≠ **B**.

**Proposition Schema 1.1.5.** *For any class* **A**, *the following is a theorem.*

$$\mathbf{A} \subseteq \mathbf{A}$$

PROOF: Every element of **A** is an element of **A**. □

**Proposition Schema 1.1.6.** *For any classes* **A** *and* **B**, *the following is a theorem.*
*If* **A** ⊆ **B** *and* **B** ⊆ **A** *then* **A** = **B**.

PROOF: If every element of **A** is an element of **B**, and every element of **B** is an element of **A**, then **A** and **B** have exactly the same elements. □

**Proposition Schema 1.1.7.** *For any classes* **A**, **B** *and* **C**, *the following is a theorem.*
*If* **A** ⊆ **B** *and* **B** ⊆ **C** *then* **A** ⊆ **C**.

PROOF: If every element of **A** is an element of **B** and every element of **B** is an element of **C** then every element of **A** is an element of **C**. □

## 1.1.2 Constructions of Classes

**Definition 1.1.8** (Empty Class)**.** The *empty class* ∅ is $\{x \mid \bot\}$. Every other class is *nonempty*.

**Definition 1.1.9** (Universal Class)**.** The *universal class* **V** is $\{x \mid \top\}$.

**Definition 1.1.10** (Enumeration)**.** Given objects $a_1$, ..., $a_n$, we define the class $\{a_1, \ldots, a_n\}$ to be the class $\{x \mid x = a_1 \vee \cdots \vee x = a_n\}$.

**Definition 1.1.11** (Intersection)**.** For any classes **A** and **B**, the *intersection* **A** ∩ **B** is $\{x \mid x \in \mathbf{A} \wedge x \in \mathbf{B}\}$.

**Definition 1.1.12** (Union)**.** For any classes **A** and **B**, the *union* **A** ∪ **B** is $\{x \mid x \in \mathbf{A} \vee x \in \mathbf{B}\}$.

**Definition 1.1.13** (Relative Complement)**.** Let **A** and **B** be classes. The *relative complement* of **B** in **A** is the class $\mathbf{A} - \mathbf{B} := \{x \in \mathbf{A} \mid x \notin \mathbf{B}\}$.

**Definition 1.1.14** (Symmetric Difference)**.** For any classes **A** and **B**, the *symmetric difference* is the class $\mathbf{A} + \mathbf{B} := (\mathbf{A} - \mathbf{B}) \cup (\mathbf{B} - \mathbf{A})$.

**Definition 1.1.15** (Pairwise disjoint)**.** Let **A** be a class. We say the elements of **A** are *pairwise disjoint* iff, for all $x, y \in \mathbf{A}$, if $x \cap y \neq \emptyset$ then $x = y$.

## 1.2 Sets and the Axiom of Extensionality

**Axiom 1.2.1** (Extensionality)**.** *If two sets have exactly the same members, they are equal.*

Thanks to this axiom, we may identify a set $a$ with the class $\{x \mid x \in a\}$. Our use of the symbols $\in$ and $=$ is consistent. We say a class $\mathbf{A}$ *is a set* iff there exists a set $a$ such that $a = \mathbf{A}$; that is, $\{x \mid \phi[x]\}$ is a set iff $\exists a \forall x (x \in a \leftrightarrow \phi[x])$. Otherwise, $\mathbf{A}$ is a *proper class*.

**Definition 1.2.2** (Subset)**.** If $A$ is a set and $A \subseteq \mathbf{B}$, we say $A$ is a *subset* of $\mathbf{B}$.

**Definition 1.2.3** (Union)**.** The *union* of a class $\mathbf{A}$ is $\{x \mid \exists X \in \mathbf{A}.x \in X\}$. We write $\bigcup_{P(x)} t(x)$ for $\bigcup\{t(x) \mid P(x)\}$.

**Definition 1.2.4** (Intersection)**.** The *intersection* of a class $\mathbf{A}$ is $\{x \mid \forall X \in \mathbf{A}.x \in X\}$. We write $\bigcap_{P(x)} t(x)$ for $\bigcap\{t(x) \mid P(x)\}$.

**Definition 1.2.5** (Power Class)**.** For any class $\mathbf{A}$, the *power class* $\mathcal{P}\mathbf{A}$ is $\{X \mid X \subseteq \mathbf{A}\}$.

## 1.3 The Other Axioms

**Axiom 1.3.1** (Union)**.** *The union of a set is a set.*

**Axiom 1.3.2** (Power Set)**.** *The power class of a set is a set, which we call a* power set*.*

**Axiom 1.3.3** (Infinity)**.** *There exists a set $I$ such that:*

- *There exists an element of $I$ that has no members*

- *For every $x \in I$, there exists a set $y \in I$ such that the elements of $y$ are exactly $x$ and the members of $x$.*

**Axiom 1.3.4** (Choice)**.** *For any set $A$ of pairwise disjoint, nonempty sets, there exists a set $C$ such that, for all $x \in A$, we have $x \cap C$ has exactly one element.*

**Axiom Schema 1.3.5** (Replacement)**.** *For any predicate $P(x,y)$, the following is an axiom:*
*Let $A$ be a set. Assume that, for all $x \in A$, there exists at most one $y$ such that $P(x,y)$. Then $\{y \mid \exists x \in A.P(x,y)\}$ is a set.*

**Axiom 1.3.6** (Regularity)**.** *For any $A$, if $A$ has a member, then there exists $m \in A$ such that $m \cap A = \emptyset$.*

## 1.4    Consequences of the Axioms

**Proposition 1.4.1.**  *The empty class $\emptyset$ is a set.*

PROOF: Immediate from the Axiom of Infinity. $\square$

**Proposition 1.4.2** (Russell's Paradox)**.**  *The class $\{x \mid x \notin x\}$ is a proper class.*

PROOF: Assume for a contradiction $R = \{x \mid x \notin x\}$ is a set. Then $R \in R$ if and only if $R \notin R$, which is impossible. $\square$

**Proposition 1.4.3** (Pairing)**.**  *For any sets $a$ and $b$, the class $\{a, b\}$ is a set.*

PROOF:
$\langle 1 \rangle 1$.  LET:  $P(x, y)$ be the predicate $(x = \emptyset \wedge y = a) \vee (x = \mathcal{P}\emptyset \wedge y = b)$.
$\langle 1 \rangle 2$.  For all $x \in \mathcal{P}\mathcal{P}\emptyset$, there exists at most one $y$ such that $P(x, y)$.
$\quad \langle 2 \rangle 1$.  LET:  $x \in \mathcal{P}\mathcal{P}\emptyset$
$\quad \langle 2 \rangle 2$.  LET:  $y$ and $y'$ be sets.
$\quad \langle 2 \rangle 3$.  ASSUME:  $P(x, y)$ and $P(x, y')$
$\quad \langle 2 \rangle 4$.  $(x = \emptyset \wedge y = a) \vee (x = \mathcal{P}\emptyset \wedge y = b)$
$\quad \quad$ PROOF: From $\langle 2 \rangle 3$.
$\quad \langle 2 \rangle 5$.  $(x = \emptyset \wedge y' = a) \vee (x = \mathcal{P}\emptyset \wedge y' = b)$
$\quad \quad$ PROOF: From $\langle 2 \rangle 3$.
$\quad \langle 2 \rangle 6$.  $\emptyset \neq \mathcal{P}\emptyset$
$\quad \quad$ PROOF: Since $\emptyset \in \mathcal{P}\emptyset$ and $\emptyset \notin \emptyset$.
$\quad \langle 2 \rangle 7$.  $y = y'$
$\langle 1 \rangle 3$.  LET:  $A$ be the set $\{y \mid \exists x \in \mathcal{P}\mathcal{P}\emptyset . P(x, y)\}$.
$\langle 1 \rangle 4$.  $A = \{a, b\}$
$\square$

**Proposition 1.4.4.**  *The union of two sets is a set.*

PROOF: Because $A \cup B = \bigcup \{A, B\}$. $\square$

**Proposition Schema 1.4.5.**  *For any number $n$, the following is a theorem:*
$\quad$ *For any sets $a_1$, ..., $a_n$, the class $\{a_1, \ldots, a_n\} = \{x \mid x = a_1 \vee \cdots \vee x = a_n\}$*
*is a set.*

PROOF: The case $n = 1$ follows from Pairing since $\{a\} = \{a, a\}$.
If we have proved the theorem for $n$ we have $\{a_1, \ldots, a_n, a_{n+1}\} = \{a_1, \ldots, a_n\} \cup \{a_{n+1}\}$. $\square$

**Proposition Schema 1.4.6** (Comprehension)**.**  *For any predicate $P(x)$, the following is a theorem:*
$\quad$ *For any set $A$, the class $\{x \in A \mid P(x)\}$ is a set.*

PROOF:
$\langle 1 \rangle 1$.  LET:  $A$ be a set.
$\langle 1 \rangle 2$.  LET:  $Q(x, y)$ be the predicate $P(x) \wedge y = x$.
$\langle 1 \rangle 3$.  For all $x \in A$, there exists at most one $y$ such that $Q(x, y)$.

$\langle 2 \rangle$1. LET: $x \in A$
$\langle 2 \rangle$2. LET: $y$ and $y'$ be sets.
$\langle 2 \rangle$3. ASSUME: $Q(x, y)$ and $Q(x, y')$
$\langle 2 \rangle$4. $x \in A \wedge P(x) \wedge y = x \wedge y' = x$
   PROOF: From $\langle 2 \rangle$3.
$\langle 2 \rangle$5. $y = y'$
   PROOF: From $\langle 2 \rangle$4.
$\langle 1 \rangle$4. LET: $B$ be the set $\{y \mid \exists x \in A.Q(x, y)\}$
  PROOF: This is a set by an Axiom of Replacement and $\langle 1 \rangle$3.
$\langle 1 \rangle$5. $B = \{y \in A \mid P(y)\}$
  PROOF:

$$\begin{aligned} y \in B &\Leftrightarrow \exists x \in A.Q(x, y) && (\langle 1 \rangle 4) \\ &\Leftrightarrow \exists x \in A(P(x) \wedge y = x) && (\langle 1 \rangle 2) \\ &\Leftrightarrow P(y) \end{aligned}$$

□

**Corollary Schema 1.4.6.1.** *For any class* **A**, *the following is a theorem:*
  *For any set B, if* **A** $\subseteq$ *B then* **A** *is a set.*

**Corollary 1.4.6.1.** *The universal class* **V** *is a proper class.*

**Corollary 1.4.6.2.** *The intersection of a set and a class is a set.*

**Corollary 1.4.6.3.** *The relative complement of a class in a set is a set.*

**Corollary 1.4.6.4.** *The symmetric difference of two sets is a set.*

**Corollary 1.4.6.5.** *The intersection of a nonempty class is a set.*

**Proposition Schema 1.4.7.** *For any classes* **A** *and* **B**, *the following is a theorem:*
  *If* **A** $\subseteq$ **B** *then* $\mathcal{P}$**A** $\subseteq$ $\mathcal{P}$**B**.

PROOF: Every subset of **A** is a subset of **B**. □

**Proposition Schema 1.4.8.** *For any classes* **A** *and* **B**, *the following is a theorem:*
  *If* **A** $\subseteq$ **B** *then* $\bigcup$**A** $\subseteq$ $\bigcup$**B**.

PROOF: If $x \in X \in$ **A** then $x \in X \in$ **B**. □

**Proposition Schema 1.4.9.** *For any class* **A**, *the following is a theorem:*

$$\mathbf{A} = \bigcup \mathcal{P}\mathbf{A}$$

PROOF:
$\langle 1 \rangle$1. **A** $\subseteq \bigcup \mathcal{P}$**A**
  PROOF: For all $x \in$ **A** we have $x \in \{x\} \in \mathcal{P}$**A**.
$\langle 1 \rangle$2. $\bigcup \mathcal{P}$**A** $\subseteq$ **A**

⟨2⟩1. LET: $x \in \bigcup \mathcal{P}\mathbf{A}$
⟨2⟩2. PICK $X \in \mathcal{P}\mathbf{A}$ such that $x \in X$
⟨2⟩3. $X \subseteq \mathbf{A}$
⟨2⟩4. $x \in \mathbf{A}$
□

**Proposition 1.4.10.** *No set is a member of itself.*

PROOF:
⟨1⟩1. LET: $x$ be any set.
⟨1⟩2. PICK $m \in \{x\}$ such that $m \cap \{x\} = \emptyset$.
⟨1⟩3. $m = x$
⟨1⟩4. $x \cap \{x\} = \emptyset$
⟨1⟩5. $x \notin x$
□

**Proposition 1.4.11.** *There are no sets $a$ and $b$ such that $a \in b$ and $b \in a$.*

PROOF:
⟨1⟩1. LET: $a$ and $b$ be any sets.
⟨1⟩2. PICK $m \in \{a, b\}$ such that $m \cap \{a, b\} = \emptyset$
⟨1⟩3. CASE: $m = a$
  PROOF: Then $b \notin a$.
⟨1⟩4. CASE: $m = b$
  PROOF: Then $a \notin b$.
□

## 1.5   Transitive Classes

**Definition 1.5.1** (Transitive Class)**.** A class $\mathbf{A}$ is a *transitive class* iff whenever $x \in y \in \mathbf{A}$ then $x \in \mathbf{A}$.

**Proposition Schema 1.5.2.** *For any class $\mathbf{A}$, the following is a theorem:*
  *The following are equivalent.*

1. $\mathbf{A}$ *is a transitive class.*

2. $\bigcup \mathbf{A} \subseteq \mathbf{A}$

3. *Every element of $\mathbf{A}$ is a subset of $\mathbf{A}$.*

4. $\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$

PROOF: Immediate from definitions. □

**Proposition Schema 1.5.3.** *For any class $\mathbf{A}$, the following is a theorem:*
  *If $\mathbf{A}$ is a transitive class then $\bigcup \mathbf{A}$ is a transitive class.*

PROOF:
⟨1⟩1. ASSUME: $\mathbf{A}$ is a transitive class.

⟨1⟩2. LET: $x \in y \in \bigcup \mathbf{A}$
⟨1⟩3. $y \in \mathbf{A}$
   PROOF: Since $\bigcup \mathbf{A} \subseteq \mathbf{A}$ by Proposition 1.5.2.
⟨1⟩4. $x \in \bigcup \mathbf{A}$
☐

**Proposition Schema 1.5.4.** *For any class* $\mathbf{A}$, *the following is a theorem:*
   *We have* $\mathbf{A}$ *is a transitive class if and only if* $\mathcal{P}\mathbf{A}$ *is a transitive class.*

PROOF:
⟨1⟩1. If $\mathbf{A}$ is a transitive class then $\mathcal{P}\mathbf{A}$ is a transitive class.
   ⟨2⟩1. ASSUME: $\mathbf{A}$ is a transitive class.
   ⟨2⟩2. $\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$
      PROOF: Proposition 1.5.2.
   ⟨2⟩3. $\mathcal{P}\mathbf{A} \subseteq \mathcal{P}\mathcal{P}\mathbf{A}$
      PROOF: Proposition 1.4.7.
   ⟨2⟩4. $\mathcal{P}\mathbf{A}$ is a transitive class.
      PROOF: Proposition 1.5.2.
⟨1⟩2. If $\mathcal{P}\mathbf{A}$ is a transitive class then $\mathbf{A}$ is a transitive class.
   ⟨2⟩1. ASSUME: $\mathcal{P}\mathbf{A}$ is a transitive class.
   ⟨2⟩2. $\bigcup \mathcal{P}\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$
      PROOF: Proposition 1.5.2.
   ⟨2⟩3. $\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$
      PROOF: Proposition 1.4.9.
   ⟨2⟩4. $\mathbf{A}$ is a transitive class.
      PROOF: Proposition 1.5.2.
☐

**Proposition Schema 1.5.5.** *For any class* $\mathbf{A}$, *the following is a theorem:*
   *If every member of* $\mathbf{A}$ *is a transitive set then* $\bigcup \mathbf{A}$ *is a transitive class.*

PROOF:
⟨1⟩1. ASSUME: Every member of $\mathbf{A}$ is a transitive set.
⟨1⟩2. LET: $x \in y \in \bigcup \mathbf{A}$
⟨1⟩3. PICK $A \in \mathbf{A}$ such that $y \in A$.
⟨1⟩4. $x \in A$
   PROOF: Since $A$ is a transitive set.
⟨1⟩5. $x \in \bigcup \mathbf{A}$
☐

**Proposition Schema 1.5.6.** *For any class* $\mathbf{A}$, *the following is a theorem:*
   *If every member of* $\mathbf{A}$ *is a transitive set then* $\bigcap \mathbf{A}$ *is a transitive class.*

PROOF:
⟨1⟩1. ASSUME: Every member of $\mathbf{A}$ is a transitive set.
⟨1⟩2. LET: $x \in y \in \bigcap \mathbf{A}$
     PROVE:   $x \in \bigcap \mathbf{A}$
⟨1⟩3. LET: $A \in \mathbf{A}$

⟨1⟩4.  $y \in A$
⟨1⟩5.  $x \in A$
   PROOF: Since $A$ is a transitive set.
☐

# Chapter 2

# Relations

## 2.1 Ordered Pairs

**Definition 2.1.1** (Ordered Pair)**.** For any sets $a$ and $b$, the *ordered pair* $(a, b)$ is defined to be $\{\{a\}, \{a, b\}\}$.

**Theorem 2.1.2.** *For any sets $a$, $b$, $c$, $d$, we have $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.*

PROOF:
$\langle 1 \rangle 1$. If $(a, b) = (c, d)$ then $a = c$ and $b = d$.
  $\langle 2 \rangle 1$. ASSUME: $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$
  $\langle 2 \rangle 2$. $\bigcap\{\{a\}, \{a, b\}\} = \bigcap\{\{c\}, \{c, d\}\}$
  $\langle 2 \rangle 3$. $\{a\} = \{c\}$
  $\langle 2 \rangle 4$. $a = c$
  $\langle 2 \rangle 5$. $\bigcup\{\{a\}, \{a, b\}\} = \bigcup\{\{c\}, \{c, d\}\}$
  $\langle 2 \rangle 6$. $\{a, b\} = \{c, d\}$
  $\langle 2 \rangle 7$. $b = c$ or $b = d$
  $\langle 2 \rangle 8$. $a = d$ or $b = d$
  $\langle 2 \rangle 9$. If $b = c$ and $a = d$ then $b = d$
    PROOF: By $\langle 2 \rangle 4$.
  $\langle 2 \rangle 10$. $b = d$
    PROOF: From $\langle 2 \rangle 7$, $\langle 2 \rangle 8$, $\langle 2 \rangle 9$.
$\langle 1 \rangle 2$. If $a = c$ and $b = d$ then $(a, b) = (c, d)$.
  PROOF: First-order logic.
□

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

**Proposition 2.1.4.** *For any sets $A$ and $B$, the class $A \times B$ is a set.*

PROOF: It is a subset of $\mathcal{P}\mathcal{P}(A \cup B)$. □

**Proposition Schema 2.1.5.** *For any classes* **A***,* **B** *and* **C***, the following is a theorem:*

$$\mathbf{A} \times (\mathbf{B} \cup \mathbf{C}) = (\mathbf{A} \times \mathbf{B}) \cup (\mathbf{A} \times \mathbf{C})$$

PROOF:
$$
\begin{aligned}
(x,y) \in \mathbf{A} \times (\mathbf{B} \cup \mathbf{C}) &\Leftrightarrow x \in \mathbf{A} \wedge (y \in \mathbf{B} \vee y \in \mathbf{C}) \\
&\Leftrightarrow (x \in \mathbf{A} \wedge y \in \mathbf{B}) \vee (x \in \mathbf{A} \wedge y \in \mathbf{C}) \\
&\Leftrightarrow (x,y) \in (\mathbf{A} \times \mathbf{B}) \cup (\mathbf{A} \times \mathbf{C}) \qquad \square
\end{aligned}
$$

**Proposition Schema 2.1.6.** *For any classes* **A** *and* **B***, the following is a theorem:*
    *If* $\mathbf{A} \times \mathbf{B} = \mathbf{A} \times \mathbf{C}$ *and* **A** *is nonempty then* $\mathbf{B} = \mathbf{C}$.

PROOF:
$\langle 1 \rangle 1$. PICK $a \in \mathbf{A}$
$\langle 1 \rangle 2$. For all $x$ we have $x \in \mathbf{B}$ iff $x \in \mathbf{C}$.
    PROOF:
$$
\begin{aligned}
x \in \mathbf{B} &\Leftrightarrow (a,x) \in \mathbf{A} \times \mathbf{B} \\
&\Leftrightarrow (a,x) \in \mathbf{A} \times \mathbf{C} \\
&\Leftrightarrow x \in \mathbf{C}
\end{aligned}
$$

$\square$

**Proposition Schema 2.1.7.** *For any classes* **A** *and* **B***, the following is a theorem:*

$$\mathbf{A} \times \bigcup \mathbf{B} = \{(a,b) \mid \exists Y \in \mathbf{B}.(a \in \mathbf{A} \wedge b \in Y)\}$$

PROOF:
$$
\begin{aligned}
(x,y) \in A \times \bigcup \mathbf{B} &\Leftrightarrow x \in A \wedge \exists Y \in \mathbf{B}.y \in Y \\
&\Leftrightarrow \exists Y \in \mathbf{B}(x \in A \wedge y \in Y) \qquad \square
\end{aligned}
$$

## 2.2  Relations

**Definition 2.2.1** (Relation)**.**  A *relation* **R** between classes **A** and **B** is a subclass of $\mathbf{A} \times \mathbf{B}$.

    A *(binary) relation on* **A** is a relation between **A** and **A**.
    We write $x\mathbf{R}y$ for $(x,y) \in \mathbf{R}$.

### 2.2.1  Identity Functions

**Definition 2.2.2** (Identity Function)**.**  For any class **A**, the *identity function* or *diagonal relation* $\mathrm{id}_\mathbf{A}$ on **A** is

$$\mathrm{id}_\mathbf{A} := \{(x,x) \mid x \in \mathbf{A}\} \ .$$

### 2.2.2  Inverses

**Definition 2.2.3** (Inverse)**.** The *inverse* of a relation $\mathbf{R}$ between $\mathbf{A}$ and $\mathbf{B}$ is the relation $\mathbf{R}^{-1}$ between $\mathbf{B}$ and $\mathbf{A}$ defined by

$$b\mathbf{R}^{-1}a \Leftrightarrow a\mathbf{R}b \ .$$

**Proposition Schema 2.2.4.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{R}$*, the following is a theorem:*

If $\mathbf{R}$ *is a relation between* $\mathbf{A}$ *and* $\mathbf{B}$*, we have* $(\mathbf{R}^{-1})^{-1} = \mathbf{R}$*.*

PROOF:
$$x(\mathbf{R}^{-1})^{-1}y \Leftrightarrow y\mathbf{R}^{-1}x$$
$$\Leftrightarrow x\mathbf{R}y \qquad\qquad \Box$$

### 2.2.3  Composition

**Definition 2.2.5** (Composition)**.** Let $\mathbf{R}$ be a relation between $\mathbf{A}$ and $\mathbf{B}$, and $\mathbf{S}$ be a relation between $\mathbf{B}$ and $\mathbf{C}$. The *composition* $\mathbf{S} \circ \mathbf{R}$ is the relation between $\mathbf{A}$ and $\mathbf{C}$ defined by
$$a(\mathbf{S} \circ \mathbf{R})c \Leftrightarrow \exists b(a\mathbf{R}b \wedge b\mathbf{S}c) \ .$$

**Proposition Schema 2.2.6.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$*,* $\mathbf{C}$*,* $\mathbf{R}$ *and* $\mathbf{S}$*, the following is a theorem:*

If $\mathbf{R}$ *is a relation between* $\mathbf{A}$ *and* $\mathbf{B}$*, and* $\mathbf{S}$ *is a relation between* $\mathbf{B}$ *and* $\mathbf{C}$*, then*
$$(\mathbf{S} \circ \mathbf{R})^{-1} = \mathbf{R}^{-1} \circ \mathbf{S}^{-1} \ .$$

PROOF:
$$z(\mathbf{S} \circ \mathbf{R})^{-1}x \Leftrightarrow x(\mathbf{S} \circ \mathbf{R})z$$
$$\Leftrightarrow \exists y.(x\mathbf{R}y \wedge y\mathbf{S}z)$$
$$\Leftrightarrow \exists y.(y\mathbf{R}^{-1}x \wedge z\mathbf{S}^{-1}y)$$
$$\Leftrightarrow z(\mathbf{R}^{-1} \circ \mathbf{S}^{-1})x \qquad\qquad \Box$$

### 2.2.4  Properties of Relaitons

**Definition 2.2.7** (Reflexive)**.** Let $\mathbf{R}$ be a binary relation on $\mathbf{A}$. Then $\mathbf{R}$ is *reflexive* on $\mathbf{A}$ iff $\forall x \in \mathbf{A}.(x, x) \in \mathbf{R}$.

**Proposition Schema 2.2.8.** *For any classes* $\mathbf{A}$ *and* $\mathbf{R}$*, the following is a theorem:*

If $\mathbf{R}$ *is a reflexive relation on* $\mathbf{A}$ *then so is* $\mathbf{R}^{-1}$*.*

PROOF:
$\langle 1 \rangle 1.$ LET: $x \in \mathbf{A}$
$\langle 1 \rangle 2.$ $x\mathbf{R}x$
  PROOF: Since $\mathbf{R}$ is reflexive.

$\langle 1 \rangle 3. \ x\mathbf{R}^{-1}x$
$\square$

**Definition 2.2.9** (Irreflexive)**.** A relation $\mathbf{R}$ is *irreflexive* iff there is no $x$ such that $(x, x) \in \mathbf{R}$.

**Definition 2.2.10** (Symmetric)**.** A relation $\mathbf{R}$ is *symmetric* iff, whenever $x\mathbf{R}y$, then $y\mathbf{R}x$.

**Definition 2.2.11** (Antisymmetric)**.** A relation $\mathbf{R}$ is *antisymmetric* iff, whenever $x\mathbf{R}y$ and $y\mathbf{R}x$, then $x = y$.

**Proposition Schema 2.2.12.** *For any classes* $\mathbf{A}$ *and* $\mathbf{R}$*, the following is a theorem:*

*If* $\mathbf{R}$ *is an antisymmetric relation on* $\mathbf{A}$ *then so is* $\mathbf{R}^{-1}$*.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: $x\mathbf{R}^{-1}y$ and $y\mathbf{R}^{-1}x$
$\langle 1 \rangle 2.$ $y\mathbf{R}x$ and $x\mathbf{R}y$
$\langle 1 \rangle 3.$ $x = y$
   PROOF: Since $\mathbf{R}$ is antisymmetric.
$\square$

**Definition 2.2.13** (Transitive)**.** A relation $\mathbf{R}$ is *transitive* iff, whenever $x\mathbf{R}y$ and $y\mathbf{R}z$, then $x\mathbf{R}z$.

**Proposition Schema 2.2.14.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{R}$*, the following is a theorem:*

*If* $\mathbf{R}$ *is a transitive relation between* $\mathbf{A}$ *and* $\mathbf{B}$ *then* $\mathbf{R}^{-1}$ *is transitive.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: $(x, y), (y, z) \in \mathbf{R}^{-1}$
$\langle 1 \rangle 2.$ $(y, x), (z, y) \in \mathbf{R}$
$\langle 1 \rangle 3.$ $(z, x) \in \mathbf{R}$
$\langle 1 \rangle 4.$ $(x, z) \in \mathbf{R}^{-1}$
$\square$

**Proposition 2.2.15.** *For any relation* $R$ *on a set* $A$*, there exists a smallest transitive relation on* $A$ *that includes* $R$*.*

PROOF: The relation is $\bigcup \{S \in \mathcal{P}A^2 \mid R \subseteq S, S \text{ is transitive}\}$. $\square$

**Definition 2.2.16** (Transitive Closure)**.** For any relation $R$ on a set $A$, the *transitive closure* of $R$ is the smallest transitive relation that includes $R$.

**Definition 2.2.17** (Minimal)**.** Let $\mathbf{R}$ be a relation on $\mathbf{A}$. An element $m \in \mathbf{A}$ is *minimal* iff there is no $x \in \mathbf{A}$ such that $x\mathbf{R}m$.

**Definition 2.2.18** (Maximal)**.** Let $\mathbf{R}$ be a relation on $\mathbf{A}$. An element $m \in \mathbf{A}$ is *maximal* iff there is no $x \in \mathbf{A}$ such that $m\mathbf{R}x$.

## 2.3   n-ary Relations

**Definition Schema 2.3.1.** For any sets $a_1, \ldots, a_n$, define the *ordered n-tuple* $(a_1, \ldots, a_n)$ by

$$(a_1) := a_1$$
$$(a_1, \ldots, a_n, a_{n+1}) = ((a_1, \ldots, a_n), a_{n+1})$$

**Definition Schema 2.3.2.** An *n-ary relation on* **A** is a class of ordered *n*-tuples all of whose components are in **A**.

## 2.4   Well Founded Relations

**Definition 2.4.1** (Well Founded)**.** A relation **R** on a class **A** is *well founded* iff:

- for all $a \in A$, the class $\{x \in \mathbf{A} \mid x\mathbf{R}a\}$ is a set;

- every nonempty subset of **A** has an **R**-minimal element.

**Proposition 2.4.2.** *For any class* **A***, the relation* $\{(x,y) \in \mathbf{A}^2 \mid x \in y\}$ *is well founded.*

PROOF:
⟨1⟩1. For all $a \in \mathbf{A}$, the class $\{x \in \mathbf{A} \mid x \in a\}$ is a set.
    PROOF: It is a subclass of $a$.
⟨1⟩2. Every nonempty subset of **A** has an $\in$-minimal element.
    ⟨2⟩1. LET: $C$ be a nonempty subset of **A**
    ⟨2⟩2. PICK $m \in C$ such that $m \cap C = \emptyset$
        PROOF: Axiom of Regularity.
    ⟨2⟩3. $m$ is $\in$-minimal in $C$.
☐

**Proposition Schema 2.4.3.** *For any classes* **A***,* **B** *and* **R***, the following is a theorem:*
    *Assume* **R** *is a well founded relation on* **A** *and* **B** $\subseteq$ **A** *is nonempty. Then* **B** *has an* **R***-minimal element.*

PROOF:
⟨1⟩1. PICK $b \in \mathbf{B}$
⟨1⟩2. LET: $S = \{x \in \mathbf{B} \mid x\mathbf{R}b\}$
    PROOF: $S$ is a set because it is a subclass of $\{x \in \mathbf{A} \mid x\mathbf{R}b\}$.
⟨1⟩3. CASE: $S = \emptyset$
    PROOF: In this case $b$ is an **R**-minimal element of **B**.
⟨1⟩4. CASE: $S \neq \emptyset$
    PROOF: In this cases $S$ has an **R**-minimal element, which is an **R**-minimal element of **B**.
☐

**Theorem Schema 2.4.4** (Transfinite Induction Principle)**.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{R}$*, the following is a theorem:*

*Assume* $\mathbf{R}$ *is a well founded relation on* $\mathbf{A}$ *and* $\mathbf{B} \subseteq \mathbf{A}$*. Assume that, for all* $t \in \mathbf{A}$,

$$\{x \in \mathbf{A} \mid x\mathbf{R}t\} \subseteq \mathbf{B} \Rightarrow t \in \mathbf{B} \ .$$

*Then* $\mathbf{B} = \mathbf{A}$*.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: for a contradiction $\mathbf{B} \neq \mathbf{A}$

$\langle 1 \rangle 2$. PICK an $\mathbf{R}$-minimal element $m$ of $\mathbf{A} - \mathbf{B}$.
  PROOF: Proposition 2.4.3.

$\langle 1 \rangle 3$. $\{x \in \mathbf{A} \mid x\mathbf{R}m\} \subseteq \mathbf{B}$
  PROOF: By minimality of $m$.

$\langle 1 \rangle 4$. $m \in \mathbf{B}$

$\langle 1 \rangle 5$. Q.E.D.
  PROOF: This is a contradiction.

☐

**Theorem 2.4.5.** *The transitive closure of a well founded relation on a set is well founded.*

PROOF:

$\langle 1 \rangle 1$. LET: $R$ be a well founded relation on the set $A$.

$\langle 1 \rangle 2$. LET: $R^t$ be the transitive closure of $R$.

$\langle 1 \rangle 3$. For any $x, y \in A$, if $xR^t y$ then there exists $z \in A$ such that $zRy$.
  PROOF: $\{(x, y) \in A^2 \mid \exists z \in A.zRy\}$ is a transitive relation on $A$ that includes $R$.

$\langle 1 \rangle 4$. LET: $B$ be a nonempty subset of $A$.

$\langle 1 \rangle 5$. PICK an $R$-minimal element $b$ of $B$.

$\langle 1 \rangle 6$. $b$ is $R^t$-minimal in $B$.
  PROOF: If there exists $x$ such that $xR^t b$ then there exists $z$ such that $zRb$ by $\langle 1 \rangle 3$.

☐

**Definition 2.4.6** (Initial Segment)**.** Let $\mathbf{R}$ be a relation on $\mathbf{A}$ and $a \in \mathbf{A}$. The *initial segment* up to $a$ is

$$\operatorname{seg} a := \{x \in \mathbf{A} \mid x\mathbf{R}a\} \ .$$

**Theorem Schema 2.4.7** (Transfinite Recursion Theorem Schema)**.** *For any classes* $\mathbf{A}$*,* $\mathbf{R}$ *and any property* $G[x, y, z]$*, there exists a class* $\mathbf{F}$ *such that, for any class* $\mathbf{F}'$ *the following is a theorem:*

*Assume that* $\mathbf{R}$ *is a well-founded relation on* $\mathbf{A}$*. Assume that, for any* $f$ *and* $t$*, there exists a unique* $z$ *such that* $G[f, t, z]$*. Then* $\mathbf{F} : \mathbf{A} \to \mathbf{V}$ *such that, for all* $t \in \mathbf{A}$*, we have* $\mathbf{F} \upharpoonright \operatorname{seg} t$ *is a set and*

$$G[\mathbf{F} \upharpoonright \operatorname{seg} t, t, \mathbf{F}(t)] \ .$$

*If* $\mathbf{F}' : \mathbf{A} \to \mathbf{V}$ *satisfies that, for all* $t \in \mathbf{A}$*, we have* $\mathbf{F}' \upharpoonright \operatorname{seg} t$ *is a set and* $G[\mathbf{F}' \upharpoonright \operatorname{seg} t, t, \mathbf{F}'(t)]$*, then* $\mathbf{F}' = \mathbf{F}$*.*

PROOF:

⟨1⟩1. For $B$ a subset of $\mathbf{A}$, let us say a function $v : B \to \mathbf{V}$ is *acceptable* iff, for all $x \in B$, we have $\operatorname{seg} x \subseteq B$ and $G[v \restriction \operatorname{seg} x, x, v(x)]$

⟨1⟩2. LET: $\mathbf{K}$ be the class of all acceptable functions.

⟨1⟩3. LET: $\mathbf{F} = \bigcup \mathbf{K}$

⟨1⟩4. For all $B, C \subseteq \mathbf{A}$, given $v_1 : B \to \mathbf{V}$ and $v_2 : C \to \mathbf{V}$ acceptable and $x \in B \cap C$, we have $v_1(x) = v_2(x)$

  ⟨2⟩1. ASSUME: as transfinite induction hypothesis $\forall y \mathbf{R} x. y \in B \cap C \Rightarrow v_1(y) = v_2(y)$

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

  ⟨2⟩3. $G[v_1 \restriction \operatorname{seg} x, x, v_1(x)]$

  ⟨2⟩4. $G[v_2 \restriction \operatorname{seg} x, x, v_2(x)]$

  ⟨2⟩5. $v_1(x) = v_2(x)$

⟨1⟩5. $\mathbf{F}$ is a function.

  ⟨2⟩1. ASSUME: $(x, y), (x, z) \in \mathbf{F}$

  ⟨2⟩2. PICK acceptable $v_1 : B \to \mathbf{V}$ and $v_2 : C \to \mathbf{V}$ such that $v_1(x) = y$ and $v_2(x) = z$

  ⟨2⟩3. $y = z$

    PROOF: By ⟨1⟩4.

⟨1⟩6. For all $t \in \operatorname{dom} \mathbf{F}$, we have $\mathbf{F} \restriction \operatorname{seg} t$ is a set and $G[\mathbf{F} \restriction \operatorname{seg} t, t, \mathbf{F}(t)]$

  ⟨2⟩1. LET: $t \in \operatorname{dom} \mathbf{F}$

  ⟨2⟩2. PICK an acceptable $v : A \to \mathbf{V}$ such that $t \in A$

  ⟨2⟩3. For all $y \mathbf{R} x$ we have $v(y) = \mathbf{F}(y)$

  ⟨2⟩4. $\mathbf{F} \restriction \operatorname{seg} x = v \restriction \operatorname{seg} x$

  ⟨2⟩5. $G[v \restriction \operatorname{seg} x, x, v(x)]$

  ⟨2⟩6. $G[\mathbf{F} \restriction \operatorname{seg} x, x, \mathbf{F}(x)]$

⟨1⟩7. $\operatorname{dom} \mathbf{F} = \mathbf{A}$

  ⟨2⟩1. LET: $x \in \mathbf{A}$

  ⟨2⟩2. ASSUME: as transfinite induction hypothesis $\forall y \mathbf{R} x. y \in \mathbf{A}$

  ⟨2⟩3. ASSUME: for a contradiction $x \notin \mathbf{A}$

  ⟨2⟩4. $\mathbf{F} \restriction \operatorname{seg} x$ is a set

  ⟨2⟩5. $\mathbf{F} \restriction \operatorname{seg} x$ is acceptable

  ⟨2⟩6. LET: $y$ be the unique object such that $G[\mathbf{F} \restriction \operatorname{seg} x, x, y]$

  ⟨2⟩7. $\mathbf{F} \restriction \operatorname{seg} x \cup \{(x, y)\}$ is acceptable

  ⟨2⟩8. $x \in \operatorname{dom} \mathbf{F}$

  ⟨2⟩9. Q.E.D.

    PROOF: This is a contradiction.

⟨1⟩8. If $\mathbf{F}' : \mathbf{A} \to \mathbf{V}$ satisfies the theorem, then $\mathbf{F}' = \mathbf{F}$.

  ⟨2⟩1. LET: $x \in \mathbf{A}$

    PROVE: $\mathbf{F}'(x) = \mathbf{F}(x)$

  ⟨2⟩2. ASSUME: as transfinite induction hypothesis $\forall y \mathbf{R} x. \mathbf{F}'(y) = \mathbf{F}(y)$

  ⟨2⟩3. $\mathbf{F} \restriction x = \mathbf{F}' \restriction x$

  ⟨2⟩4. $G[\mathbf{F} \restriction x, x, \mathbf{F}(x)]$

  ⟨2⟩5. $G[\mathbf{F}' \restriction x, x, \mathbf{F}'(x)]$

  ⟨2⟩6. $\mathbf{F}(x) = \mathbf{F}'(x)$

☐

# Chapter 3

# Functions

## 3.1 Functions

**Definition 3.1.1** (Function)**.** A *function* from $\mathbf{A}$ to $\mathbf{B}$ is a relation $\mathbf{F}$ between $\mathbf{A}$ and $\mathbf{B}$ such that, for all $x \in \mathbf{A}$, there is only one $y$ such that $x\mathbf{F}y$. We denote this $y$ by $\mathbf{F}(x)$.

    A *binary operation* on a class $\mathbf{A}$ is a function $\mathbf{A}^2 \to \mathbf{A}$.

**Definition 3.1.2** (Closed)**.** Let $\mathbf{F} : \mathbf{A} \to \mathbf{A}$ be a function and $\mathbf{B} \subseteq \mathbf{A}$. Then $\mathbf{B}$ is *closed* under $\mathbf{F}$ iff $\forall x \in \mathbf{B}.\mathbf{F}(x) \in \mathbf{B}$.

**Proposition 3.1.3.** *For any class* $\mathbf{A}$*, the following is a theorem:*

$$\mathrm{id}_{\mathbf{A}} : \mathbf{A} \to \mathbf{A}$$

PROOF: For all $x \in \mathbf{A}$, the only $y$ such that $(x, y) \in \mathrm{id}_{\mathbf{A}}$ is $y = x$. $\Box$

**Proposition Schema 3.1.4.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$*,* $\mathbf{C}$*,* $\mathbf{F}$ *and* $\mathbf{G}$*, the following is a theorem:*

    *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{G} : \mathbf{B} \to \mathbf{C}$*. Then* $\mathbf{G} \circ \mathbf{F} : \mathbf{A} \to \mathbf{C}$ *and, for all* $x \in \mathbf{A}$*, we have*

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

PROOF:
$\langle 1 \rangle 1.$ $\forall x \in \mathbf{A}.(x, \mathbf{G}(\mathbf{F}(x))) \in \mathbf{G} \circ \mathbf{F})$
   PROOF: Because $(x, \mathbf{F}(x)) \in \mathbf{F}$ and $(\mathbf{F}(x), \mathbf{G}(\mathbf{F}(x))) \in \mathbf{G}$.
$\langle 1 \rangle 2.$ If $(x, z) \in \mathbf{F} \circ \mathbf{G}$ then $z = \mathbf{G}(\mathbf{F}(x))$
   $\langle 2 \rangle 1.$ PICK $y \in \mathbf{B}$ such that $x\mathbf{F}y$ and $y\mathbf{G}z$
   $\langle 2 \rangle 2.$ $y = \mathbf{F}(x)$
   $\langle 2 \rangle 3.$ $z = \mathbf{G}(y)$
   $\langle 2 \rangle 4.$ $z = \mathbf{G}(\mathbf{F}(x))$
$\Box$

**Proposition 3.1.5.** *For any set $A$ there exists a function $F : \mathcal{P}A - \{\emptyset\} \to A$ (a* choice function *for $A$) such that, for every nonempty $B \subseteq A$, we have $F(B) \in B$.*

PROOF:

⟨1⟩1. LET: $A$ be a set.

⟨1⟩2. LET: $\mathcal{A} = \{\{B\} \times B \mid B \in \mathcal{P}A - \{\emptyset\}\}$

⟨1⟩3. Every member of $\mathcal{A}$ is nonempty.

⟨1⟩4. Any two distinct members of $\mathcal{A}$ are disjoint.

⟨1⟩5. PICK a set $C$ such that, for all $X \in \mathcal{A}$, we have $C \cap X$ is a singleton.
  PROOF: Axiom of Choice.

⟨1⟩6. LET: $F = C \cap \bigcup \mathcal{A}$

⟨1⟩7. $F : \mathcal{P}A - \{\emptyset\} \to A$

  ⟨2⟩1. $F$ is a function.

    ⟨3⟩1. LET: $(B, b), (B, b') \in F$

    ⟨3⟩2. $(B, b), (B, b') \in \{B\} \times B$
      PROOF: Since $(B, b), (B, b') \in \bigcup \mathcal{A}$.

    ⟨3⟩3. $(B, b), (B, b') \in C \cap (\{B\} \times B)$

    ⟨3⟩4. $(B, b) = (B, b')$
      PROOF: From ⟨1⟩5.

    ⟨3⟩5. $b = b'$

  ⟨2⟩2. $\operatorname{dom} F = \mathcal{P}A - \{\emptyset\}$
    PROOF:

$$B \in \operatorname{dom} F$$
$$\Leftrightarrow \exists b.(B, b) \in F$$
$$\Leftrightarrow \exists b.((B, b) \in \bigcup \mathcal{A} \wedge (B, b) \in C)$$
$$\Leftrightarrow \exists b.\exists B' \in \mathcal{P}A - \{\emptyset\}.((B, b) \in \{B'\} \times B' \wedge (B, b) \in C)$$
$$\Leftrightarrow B \in \mathcal{P}A - \{\emptyset\} \wedge \exists b \in B.(B, b) \in C$$
$$\Leftrightarrow B \in \mathcal{P}A - \{\emptyset\} \qquad\qquad\qquad (⟨1⟩5)$$

  ⟨2⟩3. $\operatorname{ran} F \subseteq A$

⟨1⟩8. For every nonempty $B \subseteq A$ we have $F(B) \in B$

▯

**Proposition 3.1.6.** *For any relation $R$ between $A$ and $B$, there exists a function $H : A \to B$ such that $H \subseteq R$ (i.e. $\forall x \in A.xRH(x)$).*

PROOF:

⟨1⟩1. LET: $R$ be a relation between $A$ and $B$.

⟨1⟩2. PICK a choice function $G$ for $B$.

⟨1⟩3. Define $H : A \to B$ by $H(x) = G(\{y \mid xRy\})$

⟨1⟩4. $H \subseteq R$

▯

### 3.1.1   Injective Functions

**Definition 3.1.7** (Injective)**.** A function $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ is *one-to-one*, *injective* or an *injection*, $\mathbf{F} : \mathbf{A} \rightarrowtail \mathbf{B}$, iff, for all $x, y \in \mathbf{A}$, if $\mathbf{F}(x) = \mathbf{F}(y)$, then $x = y$.

**Proposition 3.1.8.** *For any class $\mathbf{A}$, the following is a theorem:*
  $\operatorname{id}_{\mathbf{A}} : \mathbf{A} \to \mathbf{A}$ *is injective.*

PROOF: If $\mathrm{id}_{\mathbf{A}}(x) = \mathrm{id}_{\mathbf{A}}(y)$ then immediately $x = y$. □

**Proposition Schema 3.1.9.** *For any classes* **A**, **B**, **C**, **F**, **G**, *the following is a theorem:*

   *Assume* $\mathbf{F} : \mathbf{A} \rightarrowtail \mathbf{B}$ *and* $\mathbf{G} : \mathbf{B} \rightarrowtail \mathbf{C}$. *Then* $\mathbf{G} \circ \mathbf{F} : \mathbf{A} \rightarrowtail \mathbf{C}$.

PROOF:
⟨1⟩1. LET: $x, y \in \mathbf{A}$
⟨1⟩2. ASSUME: $(\mathbf{G} \circ \mathbf{F})(x) = (\mathbf{G} \circ \mathbf{F})(y)$
⟨1⟩3. $\mathbf{G}(\mathbf{F}(x)) = \mathbf{G}(\mathbf{F}(y))$
⟨1⟩4. $\mathbf{F}(x) = \mathbf{F}(y)$
   PROOF: Since **G** is injective.
⟨1⟩5. $x = y$
   PROOF: Since **F** is injective.
□

**Proposition 3.1.10.** *Let* $F : A \rightarrow B$ *where* $A$ *is nonempty. There exists* $G : B \rightarrow A$ *(a* left inverse*) such that* $G \circ F = \mathrm{id}_A$ *if and only if* $F$ *is one-to-one.*

PROOF:
⟨1⟩1. If there exists $G : B \rightarrow A$ such that $G \circ F = \mathrm{id}_A$ then $F$ is one-to-one.
   ⟨2⟩1. ASSUME: $G : B \rightarrow A$ and $G \circ F = I_A$
   ⟨2⟩2. LET: $x, y \in A$
   ⟨2⟩3. ASSUME: $F(x) = F(y)$
   ⟨2⟩4. $x = y$
      PROOF: $x = G(F(x)) = G(F(y)) = y$
⟨1⟩2. If $F$ is one-to-one then there exists $G : B \rightarrow A$ such that $G \circ F = I_A$.
   ⟨2⟩1. ASSUME: $F$ is one-to-one.
   ⟨2⟩2. PICK $a \in A$
   ⟨2⟩3. LET: $G : B \rightarrow A$ be the function defined by: $G(b)$ is the (unique) $x \in A$
               such that $F(x) = b$ if there exists such an $x$, $G(b) = a$ otherwise.
   ⟨2⟩4. For all $x \in A$ we have $G(F(x)) = x$.
□

### 3.1.2  Surjective Functions

**Definition 3.1.11** (Surjective)**.** Let $F : A \rightarrow B$. We say that $F$ is *surjective*, or maps $A$ *onto* $B$, and write $F : A \twoheadrightarrow B$, iff for all $y \in B$ there exists $x \in A$ such that $F(x) = y$.

**Proposition Schema 3.1.12.** *For any class* **A**, *the following is a theorem:*
   $\mathrm{id}_{\mathbf{A}} : \mathbf{A} \rightarrow \mathbf{A}$ *is surjective.*

PROOF: For any $y \in \mathbf{A}$ we have $\mathrm{id}_{\mathbf{A}}(y) = y$. □

**Proposition Schema 3.1.13.** *For any classes* **A**, **B**, **C**, **F** *and* **G**, *the following is a theorem:*
   *If* $\mathbf{F} : \mathbf{A} \twoheadrightarrow \mathbf{B}$ *and* $\mathbf{G} : \mathbf{B} \twoheadrightarrow \mathbf{C}$, *then* $\mathbf{G} \circ \mathbf{F} : \mathbf{A} \twoheadrightarrow \mathbf{C}$.

Proof:

⟨1⟩1. Let:  $c \in \mathbf{C}$
⟨1⟩2. Pick $b \in \mathbf{B}$ such that $\mathbf{G}(b) = c$.
⟨1⟩3. Pick $a \in \mathbf{A}$ such that $\mathbf{F}(a) = b$.
⟨1⟩4. $(\mathbf{G} \circ \mathbf{F})(a) = c$
□

**Proposition 3.1.14.** *Let* $F : A \to B$. *There exists* $H : B \to A$ *(a* right inverse*) such that* $F \circ H = \mathrm{id}_B$ *if and only if* $F$ *maps* $A$ *onto* $B$.

Proof:

⟨1⟩1. If $F$ has a right inverse then $F$ is surjective.
  ⟨2⟩1. Assume:  $F$ has a right inverse $H : B \to A$.
  ⟨2⟩2. Let:  $y \in B$
  ⟨2⟩3. $F(H(y)) = y$
  ⟨2⟩4. There exists $x \in A$ such that $F(x) = y$
⟨1⟩2. If $F$ is surjective then $F$ has a right inverse.
  ⟨2⟩1. Assume:  $F$ is surjective.
  ⟨2⟩2. Pick a function $H : B \to A$ such that $H \subseteq F^{-1}$
    Proof: Proposition 3.1.6.
  ⟨2⟩3. $F \circ H = \mathrm{id}_B$
    ⟨3⟩1. Let:  $y \in B$
    ⟨3⟩2. $(y, H(y)) \in F^{-1}$
    ⟨3⟩3. $F(H(y)) = y$
□

### 3.1.3   Bijections

**Definition 3.1.15** (Bijection)**.** Let $\mathbf{F} : \mathbf{A} \to \mathbf{B}$. Then $\mathbf{F}$ is *bijective* or a *bijection*, $\mathbf{F} : \mathbf{A} \approx \mathbf{B}$, iff it is injective and surjective.

**Proposition Schema 3.1.16.** *For any class* $\mathbf{A}$*, the following is a theorem:*
    *The identity function* $\mathrm{id}_\mathbf{A} : \mathbf{A} \approx \mathbf{A}$ *is a bijection.*

Proof: Proposition 3.1.8 and 3.1.12. □

**Proposition Schema 3.1.17.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{F}$*, the following is a theorem:*
    *If* $\mathbf{F} : \mathbf{A} \approx \mathbf{B}$ *then* $\mathbf{F}^{-1} : \mathbf{B} \approx \mathbf{A}$*.*

Proof:

⟨1⟩1. $\mathbf{F}^{-1} : \mathbf{B} \to \mathbf{A}$
  ⟨2⟩1. Let:  $b \in \mathbf{B}$
  ⟨2⟩2. Pick $a \in \mathbf{A}$ such that $\mathbf{F}(a) = b$.
    Proof: Since $\mathbf{F}$ is surjective.
  ⟨2⟩3. $(b, a) \in \mathbf{F}^{-1}$
  ⟨2⟩4. If $(b, a') \in \mathbf{F}^{-1}$ then $a' = a$.
    ⟨3⟩1. Let:  $a' \in \mathbf{A}$ such that $(b, a') \in \mathbf{F}^{-1}$

⟨3⟩2.  $\mathbf{F}(a') = \mathbf{F}(a)$
⟨3⟩3.  $a' = a$
    PROOF: Since $\mathbf{F}$ is injective.
⟨1⟩2.  $\mathbf{F}^{-1}$ is injective.
  ⟨2⟩1.  LET:  $x, y \in \mathbf{B}$
  ⟨2⟩2.  ASSUME:  $\mathbf{F}^{-1}(x) = \mathbf{F}^{-1}(y)$
  ⟨2⟩3.  $x = y$
      PROOF: $x = \mathbf{F}(\mathbf{F}^{-1}(x)) = \mathbf{F}(\mathbf{F}^{-1}(y)) = y$.
⟨1⟩3.  $\mathbf{F}^{-1}$ is surjective.
  PROOF: For all $a \in \mathbf{A}$ we have $\mathbf{F}^{-1}(\mathbf{F}(a)) = a$.
□

**Proposition Schema 3.1.18.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{F}$ *and* $\mathbf{G}$, *the following is a theorem:*

   *If* $\mathbf{F} : \mathbf{A} \approx \mathbf{B}$ *and* $\mathbf{G} : \mathbf{B} \approx \mathbf{C}$ *then* $\mathbf{G} \circ \mathbf{F} : \mathbf{A} \approx \mathbf{C}$.

PROOF: Propositions 3.1.9 and 3.1.13. □

### 3.1.4   Restrictions

**Definition 3.1.19** (Restriction)**.** Let $\mathbf{F} : \mathbf{A} \to \mathbf{B}$. Let $\mathbf{C} \subseteq \mathbf{A}$. The *restriction* of $\mathbf{F}$ to $\mathbf{C}$, denoted $\mathbf{F} \upharpoonright \mathbf{C}$, is the function

$$\mathbf{F} \upharpoonright \mathbf{C} : \mathbf{C} \to \mathbf{B}$$
$$(\mathbf{F} \upharpoonright \mathbf{C})(x) = \mathbf{F}(x) \qquad\qquad (x \in \mathbf{C})$$

### 3.1.5   Images

**Definition 3.1.20** (Image)**.** Let $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ and $\mathbf{C} \subseteq \mathbf{A}$. The *image* of $\mathbf{C}$ under $\mathbf{F}$ is the class

$$\mathbf{F}(\mathbf{C}) := \{ \mathbf{F}(x) \mid x \in \mathbf{C} \} \ .$$

**Proposition Schema 3.1.21.** *For any classes* $\mathbf{F}$, $\mathbf{A}$ *and* $\mathbf{B}$, *the following is a theorem.*

   *If* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$, *then for any subset* $S \subseteq \mathbf{A}$, *the class* $\mathbf{F}(S)$ *is a set.*

PROOF: By an Axiom of Replacement. □

**Proposition Schema 3.1.22.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *and* $\mathbf{F}$, *the following is a theorem:*

   *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C} \subseteq \mathcal{P}\mathbf{A}$. *Then*

$$\mathbf{F}\left( \bigcup \mathbf{C} \right) = \{ y \mid \exists X \in \mathbf{C}.y \in \mathbf{F}(X) \}$$

PROOF:
$$y \in \mathbf{F}\left( \bigcup \mathbf{C} \right) \Leftrightarrow \exists x \in \bigcup \mathbf{C}.y = \mathbf{F}(x)$$
$$\Leftrightarrow \exists x. \exists X. X \in \mathbf{C} \wedge x \in X \wedge y = \mathbf{F}(x)$$
$$\Leftrightarrow \exists X \in \mathbf{C}.y \in \mathbf{F}(X) \qquad\qquad □$$

**Proposition Schema 3.1.23.** *For any classes* **A**, **B**, **C**, **D** *and* **F**, *the following is a theorem:*

   *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C}, \mathbf{D} \subseteq \mathbf{A}$. *Then*

$$\mathbf{F}(\mathbf{C} \cup \mathbf{D}) = \mathbf{F}(\mathbf{C}) \cup \mathbf{F}(\mathbf{D}) \ .$$

Proof:
$$
\begin{aligned}
y \in \mathbf{F}(\mathbf{C} \cup \mathbf{D}) &\Leftrightarrow \exists x \in \mathbf{C} \cup \mathbf{D}.y = \mathbf{F}(x) \\
&\Leftrightarrow \exists x \in \mathbf{C}.y = \mathbf{F}(x) \vee \exists x \in \mathbf{D}.y = \mathbf{F}(x) \\
&\Leftrightarrow y \in \mathbf{F}(\mathbf{C}) \cup \mathbf{F}(\mathbf{D})
\end{aligned}
$$ □

**Proposition 3.1.24.** *For any classes* **F**, **A**, **B**, **C** *and* **D**, *the following is a theorem:*

   *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C}, \mathbf{D} \subseteq \mathbf{A}$. *Then*

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

   *Equality holds if* **F** *is injective.*

Proof:
⟨1⟩1. $\mathbf{F}(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$
  ⟨2⟩1. Let: $y \in \mathbf{F}(\mathbf{A} \cap \mathbf{B})$
  ⟨2⟩2. Pick $x \in \mathbf{A} \cap \mathbf{B}$ such that $y = \mathbf{F}(x)$
  ⟨2⟩3. $y \in \mathbf{F}(\mathbf{A})$
    Proof: Since $x \in \mathbf{A}$.
  ⟨2⟩4. $y \in \mathbf{F}(\mathbf{B})$
    Proof: Since $x \in \mathbf{B}$.
⟨1⟩2. If **F** is injective then $\mathbf{F}(\mathbf{A} \cap \mathbf{B}) = \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$.
  ⟨2⟩1. Assume: **F** is injective.
  ⟨2⟩2. Let: $y \in \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$
  ⟨2⟩3. Pick $x \in \mathbf{A}$ such that $y = \mathbf{F}(x)$
  ⟨2⟩4. Pick $x' \in \mathbf{B}$ such that $y = \mathbf{F}(x')$
  ⟨2⟩5. $x = x'$
    Proof: ⟨2⟩1
  ⟨2⟩6. $x \in \mathbf{A} \cap \mathbf{B}$
  ⟨2⟩7. $y \in \mathbf{F}(\mathbf{A} \cap \mathbf{B})$
□

**Proposition Schema 3.1.25.** *For any classes* **F**, **A**, **B**, *and* **C**, *the following is a theorem:*

   *Let* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C} \subseteq \mathcal{P}\mathbf{A}$. *Then*

$$\mathbf{F}\left(\bigcap \mathbf{C}\right) \subseteq \bigcap \{\mathbf{F}(X) \mid X \in \mathbf{A}\} \ .$$

   *Equality holds if* **F** *is injective and* **A** *is nonempty.*

Proof:
⟨1⟩1. $\mathbf{F}\left(\bigcap \mathbf{A}\right) \subseteq \bigcap \{\mathbf{F}(X) \mid X \in \mathbf{A}\}$

$\langle 2 \rangle 1$. LET: $y \in \mathbf{F}(\bigcap \mathbf{A})$
$\langle 2 \rangle 2$. PICK $x \in \bigcap \mathbf{A}$ such that $y = \mathbf{F}(x)$
$\langle 2 \rangle 3$. LET: $X \in \mathbf{A}$
$\langle 2 \rangle 4$. $x \in X$
$\langle 2 \rangle 5$. $y \in \mathbf{F}(X)$
$\langle 1 \rangle 2$. If $\mathbf{F}$ is injective then $\mathbf{F}(\bigcap \mathbf{A}) = \bigcap \{\mathbf{F}(X) \mid X \in \mathbf{A}\}$
 $\langle 2 \rangle 1$. ASSUME: $\mathbf{F}$ is injective.
 $\langle 2 \rangle 2$. ASSUME: $\mathbf{A}$ is nonempty.
 $\langle 2 \rangle 3$. LET: $y \in \bigcap \{\mathbf{F}(X) \mid X \in \mathbf{A}\}$
 $\langle 2 \rangle 4$. PICK $X_0 \in \mathbf{A}$
 $\langle 2 \rangle 5$. PICK $x \in X_0$ such that $(x, y) \in \mathbf{F}$
 $\langle 2 \rangle 6$. $x \in \bigcap \mathbf{A}$
  $\langle 3 \rangle 1$. LET: $X \in \mathbf{A}$
  $\langle 3 \rangle 2$. PICK $x' \in X$ such that $(x', y) \in \mathbf{F}$.
  $\langle 3 \rangle 3$. $x = x'$
   PROOF: $\langle 2 \rangle 1$
  $\langle 3 \rangle 4$. $x \in X$
 $\langle 2 \rangle 7$. $y \in \mathbf{F}(\bigcap \mathbf{A})$
□

**Proposition 3.1.26.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ *and* $\mathbf{F}$, *the following is a theorem:*

 *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C}, \mathbf{D} \subseteq \mathbf{A}$. *Then*

$$\mathbf{F}(\mathbf{C}) - \mathbf{F}(\mathbf{D}) \subseteq \mathbf{F}(\mathbf{C} - \mathbf{D}) \ .$$

*Equality holds if* $\mathbf{F}$ *is injective.*

PROOF:
$\langle 1 \rangle 1$. $\mathbf{F}(\mathbf{C}) - \mathbf{F}(\mathbf{D}) \subseteq \mathbf{F}(\mathbf{A} - \mathbf{B})$
 $\langle 2 \rangle 1$. LET: $y \in \mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B})$
 $\langle 2 \rangle 2$. PICK $x \in \mathbf{A}$ such that $y = \mathbf{F}(x)$
 $\langle 2 \rangle 3$. $x \notin \mathbf{B}$
 $\langle 2 \rangle 4$. $x \in \mathbf{A} - \mathbf{B}$
 $\langle 2 \rangle 5$. $y \in \mathbf{F}(\mathbf{A} - \mathbf{B})$
$\langle 1 \rangle 2$. If $\mathbf{F}$ is injective then $\mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B}) = \mathbf{F}(\mathbf{A} - \mathbf{B})$
 $\langle 2 \rangle 1$. ASSUME: $\mathbf{F}$ is injective.
 $\langle 2 \rangle 2$. LET: $y \in \mathbf{F}(\mathbf{A} - \mathbf{B})$
 $\langle 2 \rangle 3$. PICK $x \in \mathbf{A} - \mathbf{B}$ such that $y = \mathbf{F}(x)$
 $\langle 2 \rangle 4$. $y \in \mathbf{F}(\mathbf{A})$
 $\langle 2 \rangle 5$. $y \notin \mathbf{F}(\mathbf{B})$
  $\langle 3 \rangle 1$. ASSUME: for a contradiction $y \in \mathbf{F}(\mathbf{B})$
  $\langle 3 \rangle 2$. PICK $x' \in \mathbf{B}$ such that $y = \mathbf{F}(x')$
  $\langle 3 \rangle 3$. $x = x'$
   PROOF: $\langle 2 \rangle 1$
  $\langle 3 \rangle 4$. $x \in \mathbf{B}$
  $\langle 3 \rangle 5$. Q.E.D.

PROOF: This contradicts ⟨2⟩3.

☐

### 3.1.6   Inverse Images

**Definition 3.1.27** (Inverse Image). Let $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ and $\mathbf{C} \subseteq \mathbf{B}$. Then the *inverse image* of $\mathbf{C}$ under $\mathbf{F}$ is

$$\mathbf{F}^{-1}(\mathbf{C}) = \{x \in \mathbf{A} \mid \mathbf{F}(x) \in \mathbf{C}\} \ .$$

**Proposition Schema 3.1.28.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *and* $\mathbf{F}$, *the following is a theorem:*
    *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C} \subseteq \mathcal{P}\mathbf{B}$. *Then*

$$\mathbf{F}^{-1}\left(\bigcap \mathbf{C}\right) = \bigcap\{\mathbf{F}^{-1}(X) \mid X \in \mathbf{C}\} \ .$$

PROOF:

$$\begin{aligned}
x \in \mathbf{F}^{-1}\left(\bigcap \mathbf{C}\right) &\Leftrightarrow \mathbf{F}(x) \in \bigcap \mathbf{C} \\
&\Leftrightarrow \forall X \in \mathbf{C}.\mathbf{F}(x) \in X \\
&\Leftrightarrow \forall X \in \mathbf{C}.x \in \mathbf{F}^{-1}(X) \qquad\qquad ☐
\end{aligned}$$

**Proposition Schema 3.1.29.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ *and* $\mathbf{F}$, *the following is a theorem:*
    *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{C}, \mathbf{D} \subseteq \mathbf{B}$. *Then*

$$\mathbf{F}^{-1}(\mathbf{C} - \mathbf{D}) = \mathbf{F}^{-1}(\mathbf{C}) - \mathbf{F}^{-1}(\mathbf{D}) \ .$$

PROOF:

$$\begin{aligned}
x \in \mathbf{F}^{-1}(\mathbf{C} - \mathbf{D}) &\Leftrightarrow \mathbf{F}(x) \in \mathbf{C} - \mathbf{D} \\
&\Leftrightarrow \mathbf{F}(x) \in \mathbf{C} \wedge \mathbf{F}(x) \notin \mathbf{D} \\
&\Leftrightarrow x \in \mathbf{F}^{-1}(\mathbf{C}) \wedge x \in \mathbf{F}^{-1}(\mathbf{D}) \\
&\Leftrightarrow x \in \mathbf{F}^{-1}(\mathbf{C}) - \mathbf{F}^{-1}(\mathbf{D}) \qquad\qquad ☐
\end{aligned}$$

### 3.1.7   Function Sets

**Proposition 3.1.30.** *For any classes* $\mathbf{B}$ *and* $\mathbf{F}$, *the following is a theorem:*
    *Let $A$ be a set. If* $\mathbf{F} : A \to \mathbf{B}$ *then* $\mathbf{F}$ *is a set.*

PROOF: By an Axiom of Replacement, we have $R = \{\mathbf{F}(x) \mid x \in A\}$ is a set. Hence $\mathbf{F}$ is a set since $\mathbf{F} \subseteq A \times R$. ☐

**Definition 3.1.31** (Dependent Product Class). Let $I$ be a set and let $\mathbf{H}(i)$ be a class for all $i \in I$. We write $\prod_{i \in I} \mathbf{H}(i)$ for the class of all functions $f : I \to \bigcup_{i \in I} \mathbf{H}(i)$ such that $\forall i \in I.f(i) \in \mathbf{H}(i)$.
    We write $\mathbf{B}^I$ for $\prod_{i \in I} \mathbf{B}$ where $\mathbf{B}$ does not depend on $I$.

**Proposition Schema 3.1.32.** *Let $I$ be a set. Let $H(i)$ be a set for every $i \in I$. Then $\prod_{i \in I} \mathbf{H}(i)$ is a set.*

PROOF:
$\langle 1 \rangle 1.$ $\{\mathbf{H}(i) \mid i \in I\}$ is a set.
   PROOF: By an Axiom of Replacement.
$\langle 1 \rangle 2.$ $\bigcup_{i \in I} \mathbf{H}(i)$ is a set.
$\langle 1 \rangle 3.$ $\prod_{i \in I} \mathbf{H}(i)$ is a set.
   PROOF: It is a subset of $\mathcal{P}\left(I \times \bigcup_{i \in I} \mathbf{H}(i)\right)$.
☐

**Proposition 3.1.33.** *Let $I$ be a set. Let $H(i)$ be a set for all $i \in I$. If $\forall i \in I.H(i) \neq \emptyset$ then $\prod_{i \in I} H(i) \neq \emptyset$.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: $\forall i \in I.H(i) \neq \emptyset$
$\langle 1 \rangle 2.$ LET: $R = \{(i,x) \mid i \in I, x \in H(i)\}$
$\langle 1 \rangle 3.$ PICK a function $f : I \to \bigcup_{i \in I} H(i)$ such that $f \subseteq R$
   PROOF: Proposition 3.1.6.
$\langle 1 \rangle 4.$ $f \in \prod_{i \in I} H(i)$
☐

## 3.2 Equinumerosity

**Definition 3.2.1** (Equinumerous)**.** Sets $A$ and $B$ are *equinumerous*, $A \approx B$, iff there exists a bijection between $A$ and $B$.

**Theorem 3.2.2** (Cantor 1873)**.** *No set is equinumerous to its power set.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: for a contradiction $f : A \approx \mathcal{P}A$
$\langle 1 \rangle 2.$ LET: $S = \{x \in A \mid x \notin f(x)\}$
$\langle 1 \rangle 3.$ PICK $a \in A$ such that $f(a) = S$
$\langle 1 \rangle 4.$ $a \in S$ if and only if $a \notin S$
$\langle 1 \rangle 5.$ Q.E.D.
   PROOF: This is a contradiction.
☐

## 3.3 Domination

**Definition 3.3.1** (Dominate)**.** A set $A$ is *dominated* by a set $B$, $A \preccurlyeq B$, iff there exists an injection $A \to B$.

**Proposition 3.3.2.** *Given sets $A$ and $B$, if $A \neq \emptyset$ or $B = \emptyset$, then we have $A \preccurlyeq B$ iff there exists a surjective function $B \to A$.*

PROOF:

$\langle 1 \rangle$1. If $A \preccurlyeq B$ and $A \neq \emptyset$ then there exists a surjective function $B \to A$.

    $\langle 2 \rangle$1. ASSUME: $f : A \to B$ be injective.

    $\langle 2 \rangle$2. PICK $a \in A$

    $\langle 2 \rangle$3. LET: $g : B \to A$ be the function defined by $g(b) = f^{-1}(b)$ if $b \in \operatorname{ran} f$,
           and $g(b) = a$ otherwise.

    $\langle 2 \rangle$4. $g$ is surjective.

$\langle 1 \rangle$2. If there exists a surjective function $B \to A$ then $A \preccurlyeq B$.

    $\langle 2 \rangle$1. ASSUME: there exists a surjective function $g : B \to A$

    $\langle 2 \rangle$2. $\forall a \in A.\exists b \in B.g(b) = a$

    $\langle 2 \rangle$3. Choose a function $f : A \to B$ such that $\forall a \in A.g(f(a)) = a$

    $\langle 2 \rangle$4. $f$ is injective.

□

# Chapter 4

# Equivalence Relations

**Definition 4.0.1** (Equivalence Relation)**.** An *equivalence relation* on a class $\mathbf{A}$ is a binary relation on $\mathbf{A}$ that is reflexive, symmetric and transitive.

**Proposition 4.0.2.** *Equinumerosity is an equivalence relation on the class of all sets.*

PROOF: Propositions 3.1.16, 3.1.17, 3.1.18. □

**Definition 4.0.3** (Respects)**.** Let $\mathbf{R}$ be an equivalence relation on $\mathbf{A}$ and $\mathbf{F} : \mathbf{A} \to \mathbf{B}$. Then $\mathbf{F}$ *respects* $\mathbf{A}$ iff, whenever $(x, y) \in \mathbf{R}$, then $\mathbf{F}(x) = \mathbf{F}(y)$.

**Definition 4.0.4** (Equivalence Class)**.** Let $\mathbf{R}$ be an equivalence relation on $\mathbf{A}$ and $a \in \mathbf{A}$. The *equivalence class* of *a modulo* $\mathbf{R}$ is

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

**Proposition Schema 4.0.5.** *For any classes* $\mathbf{A}$ *and* $\mathbf{R}$*, the following is a theorem.*

*Assume* $\mathbf{R}$ *be an equivalence relation on* $\mathbf{A}$*. Let* $a, b \in \mathbf{A}$*. Then* $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$ *if and only if* $a\mathbf{R}b$*.*

PROOF:
⟨1⟩1. If $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$ then $a\mathbf{R}b$.
  ⟨2⟩1. ASSUME: $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$
  ⟨2⟩2. $b\mathbf{R}b$
    PROOF: Reflexivity
  ⟨2⟩3. $b \in [b]_{\mathbf{R}}$
  ⟨2⟩4. $b \in [a]_{\mathbf{R}}$
  ⟨2⟩5. $a\mathbf{R}b$
⟨1⟩2. If $a\mathbf{R}b$ then $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$.
  ⟨2⟩1. For all $x, y \in \mathbf{A}$, if $x\mathbf{R}y$ then $[y]_{\mathbf{R}} \subseteq [x]_{\mathbf{R}}$
    ⟨3⟩1. LET: $x, y \in \mathbf{A}$
    ⟨3⟩2. ASSUME: $x\mathbf{R}y$

$\langle 3 \rangle 3$. LET:  $t \in [y]_{\mathbf{R}}$

$\langle 3 \rangle 4$.  $y \mathbf{R} t$

$\langle 3 \rangle 5$.  $x \mathbf{R} t$

    PROOF: Transitivity, $\langle 3 \rangle 2$, $\langle 3 \rangle 4$.

$\langle 3 \rangle 6$.  $t \in [x]_{\mathbf{R}}$

$\langle 2 \rangle 2$. ASSUME:  $a \mathbf{R} b$

$\langle 2 \rangle 3$.  $[b]_{\mathbf{R}} \subseteq [a]_{\mathbf{R}}$

    PROOF: $\langle 2 \rangle 1$, $\langle 2 \rangle 2$.

$\langle 2 \rangle 4$.  $b \mathbf{R} a$

    PROOF: Symmetry, $\langle 2 \rangle 2$.

$\langle 2 \rangle 5$.  $[a]_{\mathbf{R}} \subseteq [b]_{\mathbf{R}}$

    PROOF: $\langle 2 \rangle 1$, $\langle 2 \rangle 4$.

$\langle 2 \rangle 6$.  $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$

    PROOF: $\langle 2 \rangle 3$, $\langle 2 \rangle 5$.

☐

**Definition 4.0.6** (Partition)**.** A *partition* $\Pi$ of a set $A$ is a set of nonempty subsets of $A$ that is disjoint and exhaustive, i.e.

1.  no two different sets in $\Pi$ have any common elements, and

2.  each element of $A$ is in some set in $\Pi$.

**Definition 4.0.7.** Let $R$ be an equivalence relation on a set $A$. The *quotient set $A/R$* is the set of all equivalence classes.

**Theorem 4.0.8.** *Let $A$ be a set and $\mathbf{B}$ a class. Let $R$ be an equivalence relation on $A$ and $F : A \to \mathbf{B}$. Then $F$ respects $R$ if and only if there exists $\hat{F} : A/R \to \mathbf{B}$ such that*

$$\forall a \in A . \hat{F}([a]_R) = F(a) \ \ .$$

*In this case, $\hat{F}$ is unique.*

PROOF:

$\langle 1 \rangle 1$.  If $F$ respects $R$ then there exists $\hat{F} : A/R \to \mathbf{B}$ such that $\forall a \in A . \hat{F}([a]_R) = F(a)$.

  $\langle 2 \rangle 1$. ASSUME:  $F$ respects $R$.

  $\langle 2 \rangle 2$. LET:  $\hat{F} = \{([a]_R, F(a)) \mid a \in A\}$

  $\langle 2 \rangle 3$.  $\hat{F}$ is a function.

    $\langle 3 \rangle 1$. ASSUME:  $a, a' \in A$ and $[a]_R = [a']_R$

        PROVE:    $F(a) = F(a')$

    $\langle 3 \rangle 2$.  $(a, a') \in R$

      PROOF: Proposition 4.0.5.

    $\langle 3 \rangle 3$.  $F(a) = F(a')$

      PROOF: $\langle 2 \rangle 1$

  $\langle 2 \rangle 4$.  dom $\hat{F} = A/R$

  $\langle 2 \rangle 5$.  ran $\hat{F} \subseteq \mathbf{B}$

  $\langle 2 \rangle 6$.  $\forall a \in A . \hat{F}([a]_R) = F(a)$

$\langle 1 \rangle 2$. If there exists $\hat{F} : A/R \to \mathbf{B}$ such that $\forall a \in A.\hat{F}([a]_R) = F(a)$ then $F$ respects $R$.

   $\langle 2 \rangle 1$. ASSUME: $\hat{F} : A/R \to \mathbf{B}$ and $\forall a \in A.\hat{F}([a]_R) = F(a)$

   $\langle 2 \rangle 2$. LET: $a, a' \in A$

   $\langle 2 \rangle 3$. ASSUME: $(a, a') \in R$

   $\langle 2 \rangle 4$. $[a]_R = [a']_R$
     PROOF: Proposition 4.0.5.

   $\langle 2 \rangle 5$. $F(a) = F(a')$
     PROOF: $\langle 2 \rangle 1$

$\langle 1 \rangle 3$. If $G, H : A/R \to \mathbf{B}$ and $\forall a \in A.G([a]_R) = H([a]_R)$ then $G = H$.

☐

**Proposition 4.0.9.** *Let $R$ be an equivalence relation on a set $A$. Then $A/R$ is a partition of $A$.*

PROOF:

$\langle 1 \rangle 1$. Every member of $A/R$ is nonempty.
   PROOF: Since $a \in [a]_R$ by reflexivity.

$\langle 1 \rangle 2$. No two different sets in $A/R$ have any common elements.

   $\langle 2 \rangle 1$. LET: $[a]_R, [b]_R \in A/R$

   $\langle 2 \rangle 2$. LET: $c \in [a]_R \cap [b]_R$
     PROVE: $[a]_R = [b]_R$

   $\langle 2 \rangle 3$. $aRc$
     PROOF: $\langle 2 \rangle 2$

   $\langle 2 \rangle 4$. $bRc$
     PROOF: $\langle 2 \rangle 2$

   $\langle 2 \rangle 5$. $cRb$
     PROOF: Symmetry, $\langle 2 \rangle 4$

   $\langle 2 \rangle 6$. $aRb$
     PROOF: Transitivity, $\langle 2 \rangle 3$, $\langle 2 \rangle 5$

   $\langle 2 \rangle 7$. $[a]_R = [b]_R$
     PROOF: Proposition 4.0.5, $\langle 2 \rangle 6$

$\langle 1 \rangle 3$. Each element of $A$ is in some set in $A/R$.
   PROOF: Since $a \in [a]_R$ by reflexivity.

☐

**Proposition 4.0.10.** *For any partition $P$ of a set $A$, there exists a unique equivalence relation $R$ on $A$ such that $A/R = P$, namely $xRy$ iff $\exists X \in P(x \in X \land y \in X)$.*

PROOF: Easy. ☐

**Definition 4.0.11** (Natural Map)**.** Let $A$ be a set and $R$ an equivalence relation on $A$. The *natural map* $A \to A/R$ is the function that maps $a \in A$ to $[a]_R$.

# Chapter 5

# Ordering Relations

## 5.1 Partial Orders

**Definition 5.1.1** (Partial Ordering). Let $\mathbf{A}$ be a class. A *partial ordering* on $\mathbf{A}$ is a relation $\mathbf{R}$ on $\mathbf{A}$ that is reflexive, antisymmetric and transitive.

We often write $\leq$ for a partial ordering, and then write $x < y$ for $x \leq y \wedge x \neq y$.

**Proposition Schema 5.1.2.** *For any classes $\mathbf{A}$ and $\mathbf{R}$, the following is a theorem:*

*If $\mathbf{R}$ is a partial order on $\mathbf{A}$ then so is $\mathbf{R}^{-1}$.*

Proof:
$\langle 1 \rangle 1$. $\mathbf{R}^{-1}$ is reflexive.
    Proof: Proposition 2.2.8.
$\langle 1 \rangle 2$. $\mathbf{R}^{-1}$ is antisymmetric.
    Proof: Proposition 2.2.12.
$\langle 1 \rangle 3$. $\mathbf{R}^{-1}$ is transitive.
    $\langle 2 \rangle 1$. Assume: $x\mathbf{R}^{-1}y$ and $y\mathbf{R}^{-1}z$
    $\langle 2 \rangle 2$. $y\mathbf{R}x$ and $z\mathbf{R}y$
    $\langle 2 \rangle 3$. $z\mathbf{R}x$
        Proof: Since $\mathbf{R}$ is transitive.
    $\langle 2 \rangle 4$. $x\mathbf{R}^{-1}z$
□

**Proposition Schema 5.1.3.** *For any classes $\mathbf{A}$, $\mathbf{B}$, $\mathbf{F}$ and $\mathbf{R}$, the following is a theorem:*

*Assume $\mathbf{R}$ is a partial order on $\mathbf{B}$ and $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ is injective. Define $\mathbf{S}$ on $\mathbf{A}$ by $x\mathbf{S}y$ iff $\mathbf{F}(x)\mathbf{R}\mathbf{F}(y)$. Then $\mathbf{S}$ is a partial order on $\mathbf{A}$.*

Proof:
$\langle 1 \rangle 1$. $\mathbf{S}$ is reflexive.
    Proof: For any $x \in \mathbf{A}$ we have $\mathbf{F}(x)\mathbf{R}\mathbf{F}(x)$.

⟨1⟩2. **S** is antisymmetric.
  ⟨2⟩1. LET: $x, y \in \mathbf{A}$
  ⟨2⟩2. ASSUME: $x\mathbf{S}y$ and $y\mathbf{S}x$
  ⟨2⟩3. $\mathbf{F}(x)\mathbf{RF}(y)$ and $\mathbf{F}(y)\mathbf{RF}(x)$
  ⟨2⟩4. $\mathbf{F}(x) = \mathbf{F}(y)$
    PROOF: **R** is antisymmetric.
  ⟨2⟩5. $x = y$
⟨1⟩3. **S** is transitive.
□

**Corollary Schema 5.1.3.1.** *For any classes* **A**, **B** *and* **R**, *the following is a theorem:*

  *Assume* **R** *be a partial order on* **A** *and* $\mathbf{B} \subseteq \mathbf{A}$. *Then* $\mathbf{R} \cap \mathbf{B}^2$ *is a partial order on* **B**.

**Definition 5.1.4** (Partially Ordered Set)**.** A *partially ordered set* or *poset* is a pair $(A, \leq)$ where $A$ is a set and $\leq$ is a partial ordering on $A$. We often write just $A$ for $(A, \leq)$.

  If $(A, \leq)$ is a poset and $B \subseteq A$ we write just $B$ for the poset $(B, \leq \cap B^2)$.

**Definition 5.1.5** (Strictly Monotone)**.** Let $(A, <_A)$ and $(B, <_B)$ be posets. A function $f : A \to B$ is *strictly monotone* iff, whenever $x <_A y$, then $f(x) <_B f(y)$.

**Definition 5.1.6** (Least)**.** Let $\leq$ be a partial order on **A**. An element $m \in \mathbf{A}$ is *least* iff for all $x \in \mathbf{A}$ we have $m \leq x$.

**Proposition 5.1.7.** *A partial order has at most one least element.*

PROOF: If $m$ and $m'$ are least then $m \leq m'$ and $m' \leq m$, so $m = m'$. □

**Definition 5.1.8** (Greatst)**.** Let $\leq$ be a partial order on **A**. An element $m \in \mathbf{A}$ is *greatest* iff for all $x \in A$ we have $x \leq m$.

**Proposition 5.1.9.** *A poset has at most one greatest element.*

PROOF: If $m$ and $m'$ are greatest then $m \leq m'$ and $m' \leq m$, so $m = m'$. □

**Definition 5.1.10** (Upper Bound)**.** Let $\leq$ be a partial ordering on **A** and $\mathbf{B} \subseteq \mathbf{A}$. Let $u \in \mathbf{A}$. Then $u$ is an *upper bound* for **B** iff $\forall x \in \mathbf{B}.x \leq u$.

**Definition 5.1.11** (Lower Bound)**.** Let $\leq$ be a partial ordering on **A** and $\mathbf{B} \subseteq \mathbf{A}$. Let $l \in \mathbf{A}$. Then $l$ is a *lower bound* for **B** iff $\forall x \in \mathbf{B}.l \leq x$.

**Definition 5.1.12** (Bounded Above)**.** Let $\leq$ be a partial ordering on **A** and $\mathbf{B} \subseteq \mathbf{A}$. Then **B** is *bounded above* iff it has an upper bound.

**Definition 5.1.13** (Bounded Below)**.** Let $\leq$ be a partial ordering on **A** and $\mathbf{B} \subseteq \mathbf{A}$. Then **B** is *bounded below* iff it has a lower bound.

**Definition 5.1.14** (Least Upper Bound)**.** Let $\leq$ be a partial ordering on **A** and **B** $\subseteq$ **A**. Let $s \in$ **A**. Then $s$ is the *least upper bound* or *supremum* of **B** iff $s$ is an upper bound for **B** and, for every upper bound $u$ for **B**, we have $s \leq u$.

**Definition 5.1.15** (Greatest Lower Bound)**.** Let $\leq$ be a partial ordering on **A** and **B** $\subseteq$ **A**. Let $i \in$ **A**. Then $i$ is the *greatest lower bound* or *infimum* of **B** iff $i$ is a lower bound for **B** and, for every lower bound $l$ for **B**, we have $i \leq l$.

**Definition 5.1.16** (Complete)**.** A partial order is *complete* iff every nonempty subset bounded above has a supremum, and every nonempty subset bounded below has an infimum.

**Definition 5.1.17** (Order Isomorphism)**.** Let $A$ and $B$ be posets. An *order isomorphism* between $A$ and $B$, $f : A \cong B$, is a bijection $f : A \approx B$ such that $f$ and $f^{-1}$ are monotone.

**Theorem 5.1.18** (Knaster Fixed-Point Theorem)**.** *Let $A$ be a complete poset with a greatest and least element. Let $\phi : A \to A$ be monotone. Then there exists $a \in A$ such that $\phi(a) = a$.*

PROOF:
$\langle 1 \rangle 1$. LET: $B = \{x \in A \mid x \leq \phi(x)\}$
$\langle 1 \rangle 2$. LET: $a = \sup B$
   PROOF: $B$ is nonempty because the least element of $A$ is in $B$, and it is
   bounded above by the greatest element of $A$.
$\langle 1 \rangle 3$. For all $b \in B$ we have $b \leq \phi(a)$
   $\langle 2 \rangle 1$. LET: $b \in B$
   $\langle 2 \rangle 2$. $b \leq \phi(b)$
   $\langle 2 \rangle 3$. $b \leq a$
   $\langle 2 \rangle 4$. $\phi(b) \leq \phi(a)$
   $\langle 2 \rangle 5$. $b \leq \phi(a)$
$\langle 1 \rangle 4$. $a \leq \phi(a)$
$\langle 1 \rangle 5$. $\phi(a) \leq \phi(\phi(a))$
$\langle 1 \rangle 6$. $\phi(a) \in B$
$\langle 1 \rangle 7$. $\phi(a) \leq a$
$\langle 1 \rangle 8$. $\phi(a) = a$
$\Box$

**Definition 5.1.19** (Dense)**.** Let $\leq$ be a partial order on **A** and **B** $\subseteq$ **A**. Then **B** is *dense* iff, for all $x, y \in$ **A**, if $x < y$ then there exists $z \in$ **B** such that $x < z < y$.

**Proposition 5.1.20.** *Let $A$ be a complete poset with no least element. Let $B \subseteq A$ be dense. Let $\theta : A \to A$ be a monotone map that is the identity on $B$. Then $\theta = \mathrm{id}_A$.*

PROOF:
$\langle 1 \rangle 1$. LET: $a \in A$
     PROVE: $\theta(a) = a$

$\langle 1 \rangle 2$. LET:  $S(a) = \{b \in B \mid b < a\}$

$\langle 1 \rangle 3$.  $S(a)$ is nonempty and bounded above.

    $\langle 2 \rangle 1$.  $S(a)$ is nonempty.

        $\langle 3 \rangle 1$. PICK $a_1 < a$

          PROOF: Since $a$ is not least.

        $\langle 3 \rangle 2$.  There exists $b \in B$ such that $a_1 < b < a$.

    $\langle 2 \rangle 2$.  $S(a)$ is bounded above by $a$.

$\langle 1 \rangle 4$.  $\sup S(a) \le a$

$\langle 1 \rangle 5$.  $\sup S(a) = a$

    $\langle 2 \rangle 1$. ASSUME:  for a contradiction $\sup S(a) < a$

    $\langle 2 \rangle 2$. PICK $b \in B$ such that $\sup S(a) < b < a$

    $\langle 2 \rangle 3$.  $b \in S(a)$

    $\langle 2 \rangle 4$.  Q.E.D.

      PROOF: This contradicts the fact that $\sup S(a) < b$.

$\langle 1 \rangle 6$.  For all $b \in S(a)$ we have $b \le \theta(a)$

    $\langle 2 \rangle 1$. LET:  $b \in S(a)$

    $\langle 2 \rangle 2$.  $b < a$

    $\langle 2 \rangle 3$.  $\theta(b) \le \theta(a)$

    $\langle 2 \rangle 4$.  $b \le \theta(a)$

      PROOF: $\theta(b) = b$

$\langle 1 \rangle 7$.  $a \le \theta(a)$

  PROOF: Since $a = \sup S(a)$ and $\theta(a)$ is an upper bound for $S(a)$.

$\langle 1 \rangle 8$.  $a \not< \theta(a)$

    $\langle 2 \rangle 1$. ASSUME:  for a contradiction $a < \theta(a)$.

    $\langle 2 \rangle 2$. PICK $b \in B$ such that $a < b < \theta(a)$

    $\langle 2 \rangle 3$.  $\theta(a) \le \theta(b) = b$

    $\langle 2 \rangle 4$.  Q.E.D.

      PROOF: This contradicts the fact that $b < \theta(a)$.

$\langle 1 \rangle 9$.  $\theta(a) = a$

$\Box$

**Theorem 5.1.21.** *Let $A$ and $P$ be complete posets with no least or greatest element. Let $B$ be dense in $A$ and $Q$ be dense in $P$. Every order isomorphism $\phi : B \cong Q$ extends uniquely to an order isomorphism $A \cong P$.*

PROOF:

$\langle 1 \rangle 1$.  For $a \in A$, let $S(a) = \{b \in B \mid b < a\}$.

$\langle 1 \rangle 2$.  Define $\overline{\phi} : A \to P$ by $\overline{\phi}(a) = \sup \phi(S(a))$.

    $\langle 2 \rangle 1$.  $\phi(S(a))$ is nonempty.

        $\langle 3 \rangle 1$. PICK $a_1 < a$

          PROOF: Since $a$ is not least.

        $\langle 3 \rangle 2$. PICK $b \in B$ such that $a_1 < b < a$.

        $\langle 3 \rangle 3$.  $\phi(b) \in \phi(S(a))$

    $\langle 2 \rangle 2$.  $\phi(S(a))$ is bounded above.

        $\langle 3 \rangle 1$. PICK $a_2 > a$

          PROOF: Since $a$ is not greatest.

        $\langle 3 \rangle 2$. PICK $b \in B$ such that $a < b < a_2$

⟨3⟩3. $\phi(b)$ is an upper bound for $\phi(S(a))$.

⟨1⟩3. $\overline{\phi}$ is monotone.

    PROOF: If $a \leq a'$ then $S(a) \subseteq S(a')$ and so $\overline{\phi}(a) \leq \overline{\phi}(a')$.

⟨1⟩4. $\overline{\phi}$ extends $\phi$.

  ⟨2⟩1. LET: $b \in B$

      PROVE: $\phi(b) = \sup \phi(S(b))$

  ⟨2⟩2. $\phi(b)$ is an upper bound for $\phi(S(b))$

  ⟨2⟩3. LET: $u$ be any upper bound for $\phi(S(b))$

      PROVE: $\phi(b) \leq u$

  ⟨2⟩4. ASSUME: for a contradiction $u < \phi(b)$

  ⟨2⟩5. PICK $q \in Q$ such that $u < q < \phi(b)$

  ⟨2⟩6. PICK $b' \in B$ such that $\phi(b') = q$

  ⟨2⟩7. $b' < b$

  ⟨2⟩8. $b' \in S(b)$

  ⟨2⟩9. $q = \phi(b') \leq u$

  ⟨2⟩10. Q.E.D.

    PROOF: This is a contradiction.

⟨1⟩5. LET: $\psi = \phi^{-1}$

⟨1⟩6. LET: $\overline{\psi} : P \to A$ be the function $\overline{\psi}(p) = \sup\{\psi(q) \mid q \in Q, q < p\}$

⟨1⟩7. $\overline{\psi}$ is monotone and extends $\psi$

  PROOF: Similar.

⟨1⟩8. $\overline{\psi} \circ \overline{\phi} : A \to A$ is monotone and the identity on $B$.

⟨1⟩9. $\overline{\psi} \circ \overline{\phi} = \mathrm{id}_A$

  PROOF: Proposition 5.1.20.

⟨1⟩10. $\overline{\phi} \circ \overline{\psi} = \mathrm{id}_B$

  PROOF: Proposition 5.1.20.

⟨1⟩11. If $\phi^* : A \cong P$ is any order isomorphism that extends $\phi$ then $\phi^* = \overline{\phi}$.

  ⟨2⟩1. LET: $a \in A$

      PROVE: $\phi^*(a) = \sup \phi(S(a))$

  ⟨2⟩2. $\phi^*(a)$ is an upper bound for $\phi(S(a))$

  ⟨2⟩3. LET: $u$ be any upper bound for $\phi(S(a))$

      PROVE: $\phi^*(a) \leq u$

  ⟨2⟩4. ASSUME: for a contradiction $u < \phi^*(a)$

  ⟨2⟩5. PICK $q \in Q$ such that $u < q < \phi^*(a)$

  ⟨2⟩6. PICK $b \in B$ such that $q = \phi(b)$

  ⟨2⟩7. $b < a$

  ⟨2⟩8. $b \in S(a)$

  ⟨2⟩9. $q = \phi(b) \leq u$

  ⟨2⟩10. Q.E.D.

    PROOF: This is a contradiction.

☐

**Definition 5.1.22** (Initial Segment). Let $\leq$ be a partial order on $\mathbf{A}$ and $t \in A$. The *initial segment* up to $t$ is the class

$$\mathrm{seg}\, t := \{x \in \mathbf{A} \mid x < t\}\ .$$

**Definition 5.1.23** (Lexicographic Ordering)**.** Let $\mathbf{R}$ be a partial order on $\mathbf{A}$ and $\mathbf{S}$ a partial order on $\mathbf{B}$. The *lexicographic ordering* $\leq$ on $\mathbf{A} \times \mathbf{B}$ is defined by:

$$(a, b) \leq (a', b') \Leftrightarrow (a\mathbf{R}a' \wedge a \neq a') \vee (a = a' \wedge b\mathbf{S}b') \ .$$

**Proposition Schema 5.1.24.** *For any classes* $\mathbf{A}$*,* $\mathbf{B}$*,* $\mathbf{R}$ *and* $\mathbf{S}$*, the following is a theorem:*

   *If* $\mathbf{R}$ *is a partial order on* $\mathbf{A}$ *and* $\mathbf{S}$ *is a partial order on* $\mathbf{B}$ *then the lexicographic ordering on* $\mathbf{A} \times \mathbf{B}$ *is a partial order.*

PROOF:
$\langle 1 \rangle 1.$  LET: $\leq$ be the lexicographic ordering on $\mathbf{A} \times \mathbf{B}$
$\langle 1 \rangle 2.$  $\leq$ is reflexive.
   PROOF: For any $a \in \mathbf{A}$ and $b \in \mathbf{B}$ we have $a = a$ and $b\mathbf{S}b$, so $(a, b) \leq (a, b)$.
$\langle 1 \rangle 3.$  $\leq$ is antisymmetric.
   $\langle 2 \rangle 1.$  ASSUME: $(a, b) \leq (a', b')$ and $(a', b') \leq (a, b)$
   $\langle 2 \rangle 2.$  $(a\mathbf{R}a' \wedge a \neq a') \vee (a = a' \wedge b\mathbf{S}b')$
   $\langle 2 \rangle 3.$  $(a'\mathbf{R}a \wedge a' \neq a) \vee (a' = a \wedge b\mathbf{S}b')$
   $\langle 2 \rangle 4.$  CASE: $a = a'$
      PROOF: Then $b\mathbf{S}b'$ and $b'\mathbf{S}b$ hence $b = b'$ and $(a, b) = (a', b')$.
   $\langle 2 \rangle 5.$  CASE: $a \neq a'$
      PROOF: Then $a\mathbf{R}a'$ and $a'\mathbf{R}a$ hence $a = a'$ which is a contradiction.
$\langle 1 \rangle 4.$  $\leq$ is transitive.
   $\langle 2 \rangle 1.$  ASSUME: $(a_1, b_1) \leq (a_2, b_2) \leq (a_3, b_3)$
   $\langle 2 \rangle 2.$  $(a_1\mathbf{R}a_2 \wedge a_1 \neq a_2) \vee (a_1 = a_2 \wedge b_1\mathbf{S}b_2)$
   $\langle 2 \rangle 3.$  $(a_2\mathbf{R}a_3 \wedge a_2 \neq a_3) \vee (a_2 = a_3 \wedge b_2\mathbf{S}b_3)$
   $\langle 2 \rangle 4.$  CASE: $a_1\mathbf{R}a_2, a_1 \neq a_2, a_2\mathbf{R}a_3, a_2 \neq a_3$
      $\langle 3 \rangle 1.$  $a_1\mathbf{R}a_3$
         PROOF: Since $\mathbf{R}$ is transitive.
      $\langle 3 \rangle 2.$  $a_1 \neq a_3$
         PROOF: If $a_1 = a_3$ then $a_1\mathbf{R}a_2$ and $a_2\mathbf{R}a_1$ so $a_1 = a_2$ which is a contradiction.
   $\langle 2 \rangle 5.$  CASE: $a_1\mathbf{R}a_2, a_1 \neq a_2, a_2 = a_3, b_2\mathbf{S}b_3$
      PROOF: Then $a_1\mathbf{R}a_3$ and $a_1 \neq a_3$.
   $\langle 2 \rangle 6.$  CASE: $a_1 = a_2, b_1\mathbf{S}b_2, a_2\mathbf{R}a_3, a_2 \neq a_3$
      PROOF: Then $a_1\mathbf{R}a_3$ and $a_1 \neq a_3$.
   $\langle 2 \rangle 7.$  CASE: $a_1 = a_2, b_1\mathbf{S}b_2, a_2 = a_3, b_2\mathbf{S}b_3$
      PROOF: Then $a_1 = a_3$ and $b_1\mathbf{S}b_3$.
□


## 5.2   Linear Orders

**Definition 5.2.1** (Linear Ordering)**.** Let $\mathbf{A}$ be a class. A *linear ordering* or *total ordering* on $\mathbf{A}$ is a partial ordering $\leq$ on $\mathbf{A}$ that is *total*, i.e.

$$\forall x, y \in \mathbf{A}.x \leq y \vee y \leq x$$

We often use the symbol $<$ for a linear ordering, and then write $x < y$ for $(x, y) \in <$.

**Proposition Schema 5.2.2** (Trichotomy). *For any classes $\mathbf{A}$ and $\leq$, the following is a theorem:*

*Assume $\leq$ be a linear ordering on $\mathbf{A}$. For any $x, y \in \mathbf{A}$, exactly one of $x < y$, $x = y$, $y < x$ holds.*

PROOF: Immediate from definitions. □

**Proposition Schema 5.2.3.** *For any classes $\mathbf{A}$ and $<$, the following is a theorem:*

*Let $<$ be a transitive relation on $\mathbf{A}$ that satisfies trichotomy. Define $\leq$ on $\mathbf{A}$ by $x \leq y$ iff $x < y$ or $x = y$. Then $\leq$ is a linear ordering on $\mathbf{A}$ and $x < y$ iff $x \leq y$ and $x \neq y$.*

PROOF:
$\langle 1 \rangle 1.$  $\leq$ is reflexive.
   PROOF: By definition we have $\forall x \in \mathbf{A}.x \leq x$.
$\langle 1 \rangle 2.$  $\leq$ is antisymmetric.
   $\langle 2 \rangle 1.$  ASSUME: $x \leq y$ and $y \leq x$
   $\langle 2 \rangle 2.$  $x < y$ or $x = y$
   $\langle 2 \rangle 3.$  $y < x$ or $y = x$
   $\langle 2 \rangle 4.$  We cannot have $x < y$ and $y < x$
      PROOF: Trichotomy.
   $\langle 2 \rangle 5.$  $x = y$
$\langle 1 \rangle 3.$  $\leq$ is transitive.
   $\langle 2 \rangle 1.$  ASSUME: $x \leq y$ and $y \leq z$
   $\langle 2 \rangle 2.$  $x < y$ or $x = y$
   $\langle 2 \rangle 3.$  $y < z$ or $y = z$
   $\langle 2 \rangle 4.$  CASE: $x < y$ and $y < z$
      PROOF: Then $x < z$ by transitivity, so $x \leq z$.
   $\langle 2 \rangle 5.$  CASE: $x = y$
      PROOF: Then we have $y \leq z$ and so $x \leq z$.
   $\langle 2 \rangle 6.$  CASE: $y = z$
      PROOF: Then we have $x \leq y$ and so $x \leq z$.
$\langle 1 \rangle 4.$  $\leq$ is total.
   PROOF: Immediate from trichotomy.
□

**Proposition Schema 5.2.4.** *For any classes $\mathbf{A}$ and $\mathbf{R}$, the following is a theorem:*

*If $\mathbf{R}$ is a linear ordering on $\mathbf{A}$ then $\mathbf{R}^{-1}$ is also a linear ordering on $\mathbf{A}$.*

PROOF:
$\langle 1 \rangle 1.$  $\mathbf{R}^{-1}$ is a partial order on $\mathbf{A}$.
   PROOF: Proposition 5.1.2.
$\langle 1 \rangle 2.$  $\mathbf{R}^{-1}$ is total.

$\langle 2 \rangle 1$.  LET:  $x, y \in \mathbf{A}$
$\langle 2 \rangle 2$.  $x\mathbf{R}y$ or $y\mathbf{R}x$.
$\langle 2 \rangle 3$.  $y\mathbf{R}^{-1}x$ or $x\mathbf{R}^{-1}y$.
□

**Proposition Schema 5.2.5.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{F}$, $\mathbf{R}$, $\mathbf{S}$, *the following is a theorem:*

*Assume* $\mathbf{R}$ *is a linear order on* $\mathbf{A}$, $\mathbf{S}$ *is a partial order on* $\mathbf{B}$, *and* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$. *If* $\mathbf{F}$ *is strictly monotone then it is injective.*

PROOF:
$\langle 1 \rangle 1$.  LET:  $x, y \in \mathbf{A}$
$\langle 1 \rangle 2$.  ASSUME:  $x \neq y$
       PROVE:    $\mathbf{F}(x) \neq \mathbf{F}(y)$
$\langle 1 \rangle 3$.  ASSUME: w.l.o.g. $x\mathbf{R}y$
   PROOF: $\mathbf{R}$ is total.
$\langle 1 \rangle 4$.  $\mathbf{F}(x)\mathbf{S}\mathbf{F}(y)$ and $\mathbf{F}(x) \neq \mathbf{F}(y)$
   PROOF: $\mathbf{F}$ is strictly monotone.
□

**Proposition Schema 5.2.6.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\leq$, $\preccurlyeq$ *and* $\mathbf{F}$, *the following is a theorem:*

*Assume* $\leq$ *is a linear order on* $\mathbf{A}$ *and* $\preccurlyeq$ *is a linear order on* $\mathbf{B}$. *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{F}$ *is strictly monotone. For all* $x, y \in \mathbf{A}$, *if* $\mathbf{F}(x) \prec \mathbf{F}(y)$ *then* $x < y$.

PROOF:
$\langle 1 \rangle 1$.  $\mathbf{F}(x) \neq \mathbf{F}(y)$ and $\mathbf{F}(y) \not\prec \mathbf{F}(x)$
   PROOF: Trichotomy.
$\langle 1 \rangle 2$.  $x \neq y$ and $y \not< x$
   PROOF: $\mathbf{F}$ is strictly monotone.
$\langle 1 \rangle 3$.  $x < y$
   PROOF: Trichotomy.
□

**Corollary Schema 5.2.6.1.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\leq$, $\preccurlyeq$ *and* $\mathbf{F}$, *the following is a theorem:*

*Assume* $\leq$ *is a linear order on* $\mathbf{A}$ *and* $\preccurlyeq$ *is a linear order on* $\mathbf{B}$. *Assume* $\mathbf{F} : \mathbf{A} \to \mathbf{B}$ *and* $\mathbf{F}$ *is strictly monotone. Then* $\mathbf{F}$ *is an order isomorphism.*

**Proposition Schema 5.2.7.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{F}$ *and* $\mathbf{S}$, *the following is a theorem:*

*Assume* $\mathbf{S}$ *is a linear order on* $\mathbf{B}$ *and* $\mathbf{F} : \mathbf{A} \rightarrowtail \mathbf{B}$. *Define* $\mathbf{R}$ *on* $\mathbf{A}$ *by* $x\mathbf{R}y$ *if and only if* $\mathbf{F}(x)\mathbf{S}\mathbf{F}(y)$. *Then* $\mathbf{R}$ *is a linear order on* $\mathbf{A}$.

PROOF:
$\langle 1 \rangle 1$.  $\mathbf{R}$ is a partial order on $\mathbf{A}$.
   PROOF: Proposition 5.1.3.

⟨1⟩2. **R** is total.
  PROOF: For all $x, y \in \mathbf{A}$ we have $\mathbf{F}(x)\mathbf{SF}(y)$ or $\mathbf{F}(y)\mathbf{SF}(x)$.
▯

**Corollary Schema 5.2.7.1.** *For any classes* **A**, **B** *and* **R**, *the following is a theorem:*
  *Assume* **R** *be a linear order on* **A** *and* $\mathbf{B} \subseteq \mathbf{A}$. *Then* $\mathbf{R} \cap \mathbf{B}^2$ *is a linear order on* **B**.

**Proposition Schema 5.2.8.** *For any classes* **A**, **B**, **R** *and* **S**, *the following is a theorem:*
  *Assume* **R** *is a linear order on* **A** *and* **S** *is a linear order on* **B**. *Then the lexicographic ordering is a linear order on* $\mathbf{A} \times \mathbf{B}$.

PROOF:
⟨1⟩1. LET: $\leq$ be the lexicographic order on $\mathbf{A} \times \mathbf{B}$
⟨1⟩2. $\leq$ is a partial order.
  PROOF: Proposition 5.1.24.
⟨1⟩3. $\leq$ is total.
  ⟨2⟩1. LET: $a, a' \in \mathbf{A}$ and $b, b' \in \mathbf{B}$
  ⟨2⟩2. CASE: $a\mathbf{R}a'$ and $a \neq a'$
    PROOF: Then $(a, b) \leq (a', b')$.
  ⟨2⟩3. CASE: $a = a'$
    PROOF: We have $b\mathbf{S}b'$ or $b'\mathbf{S}b$, so $(a, b) \leq (a', b')$ or $(a', b') \leq (a, b)$.
  ⟨2⟩4. CASE: $a'\mathbf{R}a$ and $a \neq a'$
    PROOF: Then $(a', b') \leq (a, b)$.
▯

## 5.3   Well Orderings

**Definition 5.3.1** (Well Ordering)**.** A *well ordering* on a class **A** is a well-founded linear ordering on **A**.

**Proposition Schema 5.3.2.** *For any classes* **A**, **B**, **F** *and* **S**, *the following is a theorem:*
  *Assume* **S** *well orders* **B** *and* $\mathbf{F} : \mathbf{A} \rightarrowtail \mathbf{B}$. *Define* **R** *on* **A** *by* $x\mathbf{R}y$ *if and only if* $\mathbf{F}(x)\mathbf{SF}(y)$. *Then* **R** *well orders* **A**.

PROOF:
⟨1⟩1. **R** linearly orders **A**.
  PROOF: Proposition 5.2.7.
⟨1⟩2. For all $t \in \mathbf{A}$ we have $\{x \in \mathbf{A} \mid x\mathbf{R}t \wedge x \neq t\}$ is a set.
  ⟨2⟩1. LET: $t \in \mathbf{A}$
  ⟨2⟩2. LET: $S = \{y \in \mathbf{B} \mid y\mathbf{SF}(t) \wedge y \neq \mathbf{F}(t)\}$
  ⟨2⟩3. LET: $P(x, y)$ be the property $\mathbf{F}(y) = x$
  ⟨2⟩4. For all $x \in S$ there exists at most one $y$ such that $P(x, y)$
    PROOF: **F** is injective.

⟨2⟩5. LET: $T = \{y \mid \exists x \in S.P(x,y)\}$
    PROOF: Axiom of Replacement.
⟨2⟩6. $T = \{x \in \mathbf{A} \mid x\mathbf{R}t \wedge x \neq t\}$
⟨1⟩3. Every nonempty subset of $\mathbf{A}$ has a least element.
  ⟨2⟩1. LET: $S$ be a nonempty subset of $\mathbf{A}$.
  ⟨2⟩2. LET: $y$ be the least element of $\mathbf{F}(S)$.
  ⟨2⟩3. PICK $x \in S$ such that $\mathbf{F}(x) = y$.
  ⟨2⟩4. $x$ is least in $S$.
□

**Corollary Schema 5.3.2.1.** *For any classes* $\mathbf{A}$, $\mathbf{B}$ *and* $\mathbf{R}$, *the following is a theorem:*
  *If* $\mathbf{R}$ *well orders* $\mathbf{B}$ *and* $\mathbf{A} \subseteq \mathbf{B}$ *then* $\mathbf{R} \cap \mathbf{A}^2$ *well orders* $\mathbf{A}$.

**Proposition 5.3.3.** *For any well ordered sets $A$ and $B$, the lexicographic order well orders $A \times B$.*

PROOF:
⟨1⟩1. $A \times B$ is linearly ordered.
  PROOF: Proposition 5.2.8.
⟨1⟩2. Every nonempty subset of $A \times B$ has a least element.
  ⟨2⟩1. LET: $S$ be a nonempty subset of $A \times B$.
  ⟨2⟩2. LET: $a$ be the least element of $\{x \in A \mid \exists y \in B.(x,y) \in S\}$.
  ⟨2⟩3. LET: $b$ be the least element of $\{y \in B \mid (a,y) \in S\}$.
  ⟨2⟩4. $(a,b)$ is least in $S$.
□

**Definition 5.3.4** (End Extension)**.** Let $A$ and $B$ be well ordered sets. Then $B$ is an *end extension* of $A$ iff $A \subseteq B$ and:

- Whenever $x,y \in A$ then $x \leq_A y$ iff $x \leq_B y$.

- Whenever $x \in A$ and $y \in B - A$ then $x < y$.

**Theorem 5.3.5.** *Let $\leq$ be a linear ordering on $A$. Assume that, for any $B \subseteq A$ such that $\forall t \in A. \operatorname{seg} t \subseteq B \Rightarrow t \in B$, we have $B = A$. Then $\leq$ is a well ordering on $A$.*

PROOF:
⟨1⟩1. LET: $C \subseteq A$ be nonempty.
⟨1⟩2. LET: $B = \{t \in A \mid \forall x \in C.t < x\}$
⟨1⟩3. $B \cap C = \emptyset$
⟨1⟩4. $B \neq A$
⟨1⟩5. PICK $t \in A$ such that $\operatorname{seg} t \subseteq B$ and $t \notin B$
⟨1⟩6. $t$ is least in $C$.
□

**Proposition Schema 5.3.6.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{F}$, $\mathbf{G}$, $\leq$ *and* $\preccurlyeq$, *the following is a theorem:*
  *Assume* $\leq$ *well orders* $\mathbf{A}$ *and* $\preccurlyeq$ *well orders* $\mathbf{B}$. *Assume* $\mathbf{F}$ *and* $\mathbf{G}$ *are order isomorphisms between* $\mathbf{A}$ *and* $\mathbf{B}$. *Then* $\mathbf{F} = \mathbf{G}$.

PROOF:

$\langle 1 \rangle 1$. For all $x \in \mathbf{A}$, if $\forall t < x.\mathbf{F}(t) = \mathbf{G}(t)$, then $\mathbf{F}(x) = \mathbf{G}(x)$

    $\langle 2 \rangle 1$. LET: $x \in \mathbf{A}$

    $\langle 2 \rangle 2$. ASSUME: $\forall t < x.\mathbf{F}(t) = \mathbf{G}(t)$

    $\langle 2 \rangle 3$. $\mathbf{F}(\text{seg } x) = \mathbf{G}(\text{seg } x)$

    $\langle 2 \rangle 4$. $\mathbf{F}(x)$ is the least element of $\mathbf{B} - \mathbf{F}(\text{seg } x)$

    $\langle 2 \rangle 5$. $\mathbf{G}(x)$ is the least element of $\mathbf{B} - \mathbf{G}(\text{seg } x)$

    $\langle 2 \rangle 6$. $\mathbf{F}(x) = \mathbf{G}(x)$

$\langle 1 \rangle 2$. $\forall x \in \mathbf{A}.\mathbf{F}(x) = \mathbf{G}(x)$

    PROOF: Transfinite induction.

□

**Theorem 5.3.7.** *Let A and B be well ordered sets. Then one of the following holds: $A \cong B$; there exists $b \in B$ such that $A \cong \text{seg } b$; there exists $a \in A$ such that $\text{seg } a \cong B$.*

PROOF:

$\langle 1 \rangle 1$. PICK $e$ that is not in $A$ or $B$.

$\langle 1 \rangle 2$. LET: $F : A \to B \cup \{e\}$ be the function defined by transfinite recursion thus:

$$F(t) = \begin{cases} \text{the least element of } B - F(\text{seg } t) & \text{if } B - F(\text{seg } t) \neq \emptyset \\ e & \text{if } B - F(\text{seg } t) = \emptyset \end{cases}$$

$\langle 1 \rangle 3$. CASE: $e \in \text{ran } F$

    $\langle 2 \rangle 1$. LET: $t$ be least such that $F(t) = e$

    $\langle 2 \rangle 2$. $F \upharpoonright \text{seg } t : \text{seg } t \cong B$

$\langle 1 \rangle 4$. CASE: $\text{ran } F = B$

    PROOF: We have $F : A \cong B$

$\langle 1 \rangle 5$. CASE: $\text{ran } F \subsetneq B$

    $\langle 2 \rangle 1$. LET: $b$ be the least element of $B - \text{ran } F$

    $\langle 2 \rangle 2$. $F : A \cong \text{seg } b$

□

# Chapter 6

# Ordinal Numbers

## 6.1 Ordinals

**Definition 6.1.1** (Ordinal Number). An *ordinal (number)* is a transitive set $\alpha$ that is *well-ordered by* $\in$; that is, such that $\{(x,y) \in \alpha^2 \mid x \in y \vee x = y\}$ well orders $\alpha$.

Given $x, y \in \alpha$, we write $x < y$ iff $x \in y$, and $x \leq y$ iff $x \in y$ or $x = y$.

Let **On** be the class of ordinal numbers. For $\alpha, \beta \in$ **On**, we write $\alpha < \beta$ iff $\alpha \in \beta$, and $\alpha \leq \beta$ iff $\alpha < \beta$ or $\alpha = \beta$.

**Proposition 6.1.2.** *For any ordinal numbers $\alpha$ and $\beta$, if $\alpha \cong \beta$ then $\alpha = \beta$.*

PROOF:
$\langle 1 \rangle 1$. LET: $f : \alpha \cong \beta$
$\langle 1 \rangle 2$. For all $x \in \alpha$, if $\forall t < x.f(t) = t$ then $f(x) = x$
  $\langle 2 \rangle 1$. $f(x) \subseteq x$
    $\langle 3 \rangle 1$. LET: $y \in f(x)$
    $\langle 3 \rangle 2$. $y \in \beta$
    $\langle 3 \rangle 3$. PICK $t \in \alpha$ such that $f(t) = y$
      PROOF: $f$ is surjective.
    $\langle 3 \rangle 4$. $f(t) \in f(x)$
    $\langle 3 \rangle 5$. $t \in x$
      PROOF: Since $f$ is an order isomorphism.
    $\langle 3 \rangle 6$. $f(t) = t$
      PROOF: Induction hypothesis.
    $\langle 3 \rangle 7$. $y = t$
    $\langle 3 \rangle 8$. $y \in x$
  $\langle 2 \rangle 2$. $x \subseteq f(x)$
    $\langle 3 \rangle 1$. LET: $t \in x$
    $\langle 3 \rangle 2$. $f(t) \in f(x)$
    $\langle 3 \rangle 3$. $f(t) = t$
    $\langle 3 \rangle 4$. $t \in f(x)$

$\langle 1 \rangle 3.$  $\forall x \in \alpha . f(x) = x$
  Proof: Transfinite induction.
$\langle 1 \rangle 4.$  $\alpha = \beta$
  Proof: Since $\beta = \{f(t) \mid t \in \alpha\} = \{t \mid t \in \alpha\} = \alpha$.
▯

**Theorem 6.1.3.** *Every well-ordered set is isomorphic to a unique ordinal.*

Proof:
$\langle 1 \rangle 1.$  For any well-ordered set $A$, there exists an ordinal $\alpha$ such that $A \cong \alpha$.
  $\langle 2 \rangle 1.$  Let:  $A$ be a well-ordered set.
  $\langle 2 \rangle 2.$  Define the function $E$ on $A$ by transfinite recursion thus:
$$E(t) = \{E(x) \mid x < t\} \qquad (t \in A) \ .$$
  $\langle 2 \rangle 3.$  Let:  $\alpha = \{E(x) \mid x \in A\}$
  $\langle 2 \rangle 4.$  $\alpha$ is an ordinal.
    $\langle 3 \rangle 1.$  $\alpha$ is a transitive set.
      $\langle 4 \rangle 1.$  Let:  $x \in y \in \alpha$
      $\langle 4 \rangle 2.$  Pick $t \in A$ such that $y = E(t)$
      $\langle 4 \rangle 3.$  $x \in E(t) = \{E(s) \mid s < t\}$
      $\langle 4 \rangle 4.$  Pick $s < t$ such that $x = E(s)$
      $\langle 4 \rangle 5.$  $x \in \alpha$
    $\langle 3 \rangle 2.$  $\alpha$ is well-ordered by $\in$.
      $\langle 4 \rangle 1.$  Let:  $<= \{(x, y) \in \alpha \mid x \in y\}$
      $\langle 4 \rangle 2.$  $<$ is transitive.
        $\langle 5 \rangle 1.$  Let:  $x, y, z \in \alpha$ with $x \in y \in z$
        $\langle 5 \rangle 2.$  Pick $t \in A$ such that $z = E(t)$
        $\langle 5 \rangle 3.$  Pick $s \in A$ such that $s < t$ and $y = E(s)$
        $\langle 5 \rangle 4.$  Pick $r \in A$ such that $r < s$ and $x = E(r)$
        $\langle 5 \rangle 5.$  $r < t$
        $\langle 5 \rangle 6.$  $x \in z$
      $\langle 4 \rangle 3.$  $<$ satisfies trichotomy.
        $\langle 5 \rangle 1.$  Let:  $x, y \in \alpha$
        $\langle 5 \rangle 2.$  Pick $s, t \in A$ such that $E(s) = x$ and $E(t) = y$
        $\langle 5 \rangle 3.$  Exactly one of $s < t$, $s = t$, $t < s$ holds.
        $\langle 5 \rangle 4.$  Case:  $s < t$
          $\langle 6 \rangle 1.$  $x \in y$
          $\langle 6 \rangle 2.$  $x \neq y$ and $y \notin x$
            Proof: Axiom of Regularity.
        $\langle 5 \rangle 5.$  Case:  $s = t$
          $\langle 6 \rangle 1.$  $x = y$
          $\langle 6 \rangle 2.$  $x \notin y$ and $y \notin x$
            Proof: Axiom of Regularity.
        $\langle 5 \rangle 6.$  Case:  $t < s$
          Proof: Similar to $\langle 5 \rangle 4$.
      $\langle 4 \rangle 4.$  $\leq$ is a linear order on $\alpha$.
        Proof: Proposition 5.2.3.
      $\langle 4 \rangle 5.$  Every nonempty subset of $\alpha$ has a least element.

$\langle 5 \rangle 1$. Let: $S$ be a nonempty subset of $\alpha$
$\langle 5 \rangle 2$. Let: $T = \{x \in A \mid E(x) \in S\}$
$\langle 5 \rangle 3$. Let: $t$ be the least element of $T$.
  Prove: $E(t)$ is least in $S$
$\langle 5 \rangle 4$. Let: $y \in S$
$\langle 5 \rangle 5$. Pick $s \in T$ such that $E(s) = y$
$\langle 5 \rangle 6$. $t \leq s$
$\langle 5 \rangle 7$. $x \leq y$
$\langle 2 \rangle 5$. $E$ is surjective.
 Proof: By definition of $\alpha$.
$\langle 2 \rangle 6$. $E$ is strictly monotone.
 Proof: If $s < t$ then $E(s) \in E(t)$ by definition of $E(t)$.
$\langle 2 \rangle 7$. Q.E.D.
 Proof: Corollary 5.2.6.1.
$\langle 1 \rangle 2$. For any ordinals $\alpha$ and $\beta$, if $\alpha \cong \beta$ then $\alpha = \beta$.
 Proof: Proposition 6.1.2.
$\square$

**Proposition 6.1.4.** *The class* **On** *is a transitive class. That is, every element of an ordinal is an ordinal.*

Proof:
$\langle 1 \rangle 1$. Let: $\alpha$ be an ordinal.
$\langle 1 \rangle 2$. Let: $\beta \in \alpha$
$\langle 1 \rangle 3$. $\beta$ is a transitive set.
 $\langle 2 \rangle 1$. Let: $x \in y \in \beta$
 $\langle 2 \rangle 2$. $y \in \alpha$
  Proof: $\alpha$ is transitive.
 $\langle 2 \rangle 3$. $x \in \alpha$
  Proof: $\alpha$ is transitive.
 $\langle 2 \rangle 4$. $x \in \beta$
  Proof: Since $\{(x, y) \in \alpha^2 \mid x \in y\}$ is transitive.
$\langle 1 \rangle 4$. $\beta$ is well ordered by $\in$.
 Proof: By Corollary 5.3.2.1.
$\square$

**Proposition 6.1.5.** *Given two ordinal numbers* $\alpha$, $\beta$, *exactly one of* $\alpha \in \beta$, $\alpha = \beta$, $\beta \in \alpha$ *holds.*

Proof:
$\langle 1 \rangle 1$. At most one holds.
 Proof: Since every ordinal is a transitive set and we never have $\alpha \in \alpha$.
$\langle 1 \rangle 2$. At least one holds.
 $\langle 2 \rangle 1$. Either $\alpha \cong \beta$ or $\exists t \in \beta. \alpha \cong \operatorname{seg} t$ or $\exists t \in \alpha. \operatorname{seg} t \cong \beta$.
 $\langle 2 \rangle 2$. Case: $\alpha \cong \beta$
  Proof: Then $\alpha = \beta$ by Proposition 6.1.2.
 $\langle 2 \rangle 3$. Case: There exists $t \in \beta$ such that $\alpha \cong \operatorname{seg} t$

$\langle 3 \rangle 1.$  $t$ is an ordinal number.
  PROOF: Proposition 6.1.4.
$\langle 3 \rangle 2.$  $t = \text{seg}\, t$
  $\langle 4 \rangle 1.$  $t \subseteq \text{seg}\, t$
    $\langle 5 \rangle 1.$  LET:  $s \in t$
    $\langle 5 \rangle 2.$  $s \in \beta$
      PROOF: $\beta$ is a transitive set.
    $\langle 5 \rangle 3.$  $s \in \text{seg}\, t$
  $\langle 4 \rangle 2.$  $\text{seg}\, t \subseteq t$
    PROOF: Immediate from definitions.
$\langle 3 \rangle 3.$  $\alpha = t$
  PROOF: Proposition 6.1.2.
$\langle 3 \rangle 4.$  $\alpha \in \beta$
$\langle 2 \rangle 4.$  CASE:  There exists $t \in \alpha$ such that $\text{seg}\, t \cong \beta$
  PROOF: $\beta \in \alpha$ similarly.

☐

**Proposition 6.1.6.** *Any nonempty set $S$ of ordinal numbers has a least element.*

PROOF:
$\langle 1 \rangle 1.$  PICK $\beta \in S$
$\langle 1 \rangle 2.$  CASE:  $\beta \cap S = \emptyset$
  PROOF: Then $\beta$ is least in $S$.
$\langle 1 \rangle 3.$  CASE:  $\beta \cap S \neq \emptyset$
  PROOF: The least element of $\beta \cap S$ is least in $S$.

☐

**Theorem 6.1.7.** *The class **On** is well ordered by $\in$.*

PROOF:
$\langle 1 \rangle 1.$  LET:  $\mathbf{E} = \{(x, y) \in \mathbf{On}^2 \mid x \in y\}$
$\langle 1 \rangle 2.$  $\mathbf{E}$ is transitive.
  PROOF: If $\alpha \in \beta \in \gamma$ then $\alpha \in \gamma$ because every ordinal is a transitive set.
$\langle 1 \rangle 3.$  $\mathbf{E}$ satisfies trichotomy.
  PROOF: Proposition 6.1.5.
$\langle 1 \rangle 4.$  $\mathbf{E}$ linearly orders $\mathbf{On}$.
  PROOF: Proposition 5.2.3.
$\langle 1 \rangle 5.$  For any $\alpha \in \mathbf{On}$, the class $\{\beta \in \mathbf{On} \mid \beta \mathbf{E} \alpha\}$ is a set.
  PROOF: It is equal to $\alpha$.
$\langle 1 \rangle 6.$  Every nonempty subset of $\mathbf{On}$ has an $\mathbf{E}$-least element.
  PROOF: Proposition 6.1.6.

☐

**Corollary 6.1.7.1** (Burali-Forti Paradox)**.** *The class **On** is a proper class.*

PROOF: If it were a set, it would be a transitive set well-ordered by $\in$, and hence a member of itself, contradicting the Axiom of Regularity.

**Proposition 6.1.8.** *Any transitive set of ordinal numbers is an ordinal number.*

PROOF: It is well-ordered by $\in$ by Corollary 5.3.2.1 and Theorem 6.1.7. $\square$

**Proposition 6.1.9.** $\emptyset$ *is an ordinal number.*

PROOF: Vacuously, it is a transitive set well-ordered by $\in$.

**Definition 6.1.10.** We define $0 = \emptyset$.

**Proposition 6.1.11.** *If $A$ is a set of ordinal numbers then $\bigcup A$ is an ordinal number.*

PROOF:
$\langle 1 \rangle 1$. $\bigcup A$ is a transitive set.
    PROOF: Proposition 1.5.3.
$\langle 1 \rangle 2$. $\bigcup A$ is a set of ordinals.
    PROOF: Proposition 6.1.4.
$\square$

**Corollary 6.1.11.1.** *The poset **On** is complete.*

PROOF: For any nonempty set $A$ of ordinals, $\bigcup A$ is its supremum. $\square$

**Proposition 6.1.12.** *Let $\alpha$ be an ordinal and $S \subseteq \alpha$. Then $S$ is well-ordered by $\in$ and the ordinal of $(S, \in)$ is $\leq \alpha$.*

PROOF:
$\langle 1 \rangle 1$. $S$ is well ordered by $\in$.
$\langle 1 \rangle 2$. LET: $\beta$ be the ordinal of $(S, \in)$
$\langle 1 \rangle 3$. LET: $E : S \approx \beta$ be the unique isomorphism.
$\langle 1 \rangle 4$. $\forall \gamma \in S.E(\gamma) \leq \gamma$
    $\langle 2 \rangle 1$. LET: $\gamma \in S$
    $\langle 2 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall \delta < \gamma.E(\delta) \leq \delta$
    $\langle 2 \rangle 3$. $E(\gamma)$ is the least element of $\beta$ that is greater than $E(\delta)$ for all $\delta < \gamma$
    $\langle 2 \rangle 4$. $\gamma$ is greater than $E(\delta)$ for all $\delta < \gamma$
    $\langle 2 \rangle 5$. $E(\gamma) \leq \gamma$
$\langle 1 \rangle 5$. $\beta \leq \alpha$
    $\langle 2 \rangle 1$. $\forall \gamma < \beta.\gamma < \alpha$
        $\langle 3 \rangle 1$. LET: $\gamma < \beta$
        $\langle 3 \rangle 2$. PICK $\delta \in S$ such that $E(\delta) = \gamma$
        $\langle 3 \rangle 3$. $\gamma = E(\delta) \leq \delta < \alpha$
$\square$

**Proposition 6.1.13.** *Let $\alpha$ be a set. Then the following are equivalent.*

1. *$\alpha$ is an ordinal.*

2. *$\alpha$ is a transitive set and, for all $x, y \in \alpha$, either $x = y$ or $x \in y$ or $y \in x$.*

3. *$\alpha$ is a transitive set of transitive sets.*

PROOF:

⟨1⟩1.  $1 \Rightarrow 2$
   PROOF: Immediate from definitions.

⟨1⟩2.  $2 \Rightarrow 3$
   ⟨2⟩1.  ASSUME:  $\alpha$ is a transitive set and, for all $x, y \in \alpha$, either $x = y$ or $x \in y$
                or $y \in x$
   ⟨2⟩2.  LET:  $z \in \alpha$
         PROVE:   $z$ is transitive.
   ⟨2⟩3.  LET:  $x \in y \in z$
   ⟨2⟩4.  $y \in \alpha$
   ⟨2⟩5.  $x \in \alpha$
   ⟨2⟩6.  Either $x = z$ or $x \in z$ or $z \in x$
   ⟨2⟩7.  $x \neq z$
         PROOF: We cannot have $x \in y \in x$ by the Axiom of Regularity.
   ⟨2⟩8.  $z \notin x$
         PROOF: We cannot have $x \in y \in z \in x$ by the Axiom of Regularity.

⟨1⟩3.  $3 \Rightarrow 1$
   ⟨2⟩1.  LET:  $x$ be a transitive set of transitive sets.
   ⟨2⟩2.  ASSUME:  as $\in$-induction hypothesis that, for all $y \in x$, if $y$ is a transitive
                set of transitive sets then $y$ is a transitive set of ordinals.
   ⟨2⟩3.  Every element of $x$ is an ordinal.
      ⟨3⟩1.  LET:  $y \in x$
      ⟨3⟩2.  $y$ is transitive.
      ⟨3⟩3.  Every element of $y$ is transitive.
         PROOF: Since every element of $y$ is an element of $x$, because $x$ is transitive.
      ⟨3⟩4.  $y$ is an ordinal.
         PROOF: ⟨2⟩2
   ⟨2⟩4.  Q.E.D.
         PROOF: Proposition 6.1.8.
▯

**Lemma 6.1.14.** *Let A and B be well-ordered sets. If B is an end extension of A then the ordinal of A is $\leq$ the ordinal of B.*

PROOF:

⟨1⟩1.  LET:  $\alpha$ be the ordinal of $A$ and $\beta$ the ordinal of $B$.
⟨1⟩2.  LET:  $E_A : A \cong \alpha$ and $E_B : B \cong \beta$ be the canonical isomorphisms.
⟨1⟩3.  $\forall a \in A. E_A(a) = E_B(a)$
   ⟨2⟩1.  LET:  $a \in A$
   ⟨2⟩2.  ASSUME:  as transfinite induction hypothesis $\forall x < a. E_A(x) = E_B(x)$
   ⟨2⟩3.  $E_A(a)$ is the least ordinal that is greater than $E_A(x)$ for all $x < a$
   ⟨2⟩4.  $E_B(a)$ is the least ordinal that is greater than $E_B(x)$ for all $x < b$
   ⟨2⟩5.  $\{x \in A \mid x <_A a\} = \{x \in B \mid x <_B a\}$
   ⟨2⟩6.  $E_A(a) = E_B(a)$
⟨1⟩4.  $\alpha \subseteq \beta$
⟨1⟩5.  $\alpha \leq \beta$

☐

**Lemma 6.1.15.** *Let $\mathcal{C}$ be a set of well ordered sets such that, for any $A, B \in \mathcal{C}$, we have that one of $A$ and $B$ is an end extension of the other. Let $W = \bigcup \mathcal{C}$ under $x \leq y$ iff there exists $A \in W$ such that $x, y \in A$ and $x \leq y$. Then $W$ is a well ordered set whose ordinal is the supremum of the ordinals of the members of $\mathcal{C}$.*

PROOF:

$\langle 1 \rangle 1$. $\leq$ is reflexive on $W$.

$\quad \langle 2 \rangle 1$. LET: $x \in W$

$\quad \langle 2 \rangle 2$. PICK $A \in W$ such that $x \in A$.

$\quad \langle 2 \rangle 3$. $x \leq x$

$\langle 1 \rangle 2$. $\leq$ is antisymmetric on $W$.

$\quad \langle 2 \rangle 1$. LET: $x, y \in W$

$\quad \langle 2 \rangle 2$. ASSUME: $x \leq y$ and $y \leq x$

$\quad \langle 2 \rangle 3$. PICK $A \in W$ such that $x, y \in A$ and $x \leq_A y$, and $B \in W$ such that $x, y \in B$ and $y \leq_B x$

$\quad \langle 2 \rangle 4$. ASSUME: w.l.o.g. $B$ is an end extension of $A$

$\quad \langle 2 \rangle 5$. $x \leq_B y$ and $y \leq_B x$

$\quad \langle 2 \rangle 6$. $x = y$

$\langle 1 \rangle 3$. $\leq$ is transitive on $W$.

$\quad \langle 2 \rangle 1$. ASSUME: $x \leq y \leq z$

$\quad \langle 2 \rangle 2$. PICK $A, B \in W$ such that $x \leq_A y$ and $y \leq_B z$

$\quad \langle 2 \rangle 3$. CASE: $A$ is an end extension of $B$.

$\quad \quad \langle 3 \rangle 1$. $x \leq_A y$ and $y \leq_A z$

$\quad \quad \langle 3 \rangle 2$. $x \leq_A z$

$\quad \quad \langle 3 \rangle 3$. $x \leq z$

$\quad \langle 2 \rangle 4$. CASE: $B$ is an end extension of $A$.

$\quad \quad$ PROOF: Similar.

$\langle 1 \rangle 4$. $\leq$ is total on $W$.

$\quad \langle 2 \rangle 1$. LET: $x, y \in W$

$\quad \langle 2 \rangle 2$. PICK $A, B \in \mathcal{C}$ such that $x \in A$ and $y \in B$

$\quad \langle 2 \rangle 3$. ASSUME: w.l.o.g. $B$ is an end extension of $A$

$\quad \langle 2 \rangle 4$. $x \leq_B y$ or $y \leq_B x$

$\quad \langle 2 \rangle 5$. $x \leq_W y$ or $y \leq_W x$

$\langle 1 \rangle 5$. Every nonempty subset of $W$ has a least element.

$\quad \langle 2 \rangle 1$. LET: $S$ be a nonempty subset of $W$

$\quad \langle 2 \rangle 2$. PICK $s \in S$

$\quad \langle 2 \rangle 3$. PICK $A \in \mathcal{C}$ such that $s \in A$

$\quad \langle 2 \rangle 4$. LET: $a$ be the $\leq_A$-least element of $S \cap A$

$\quad \quad$ PROVE: $a$ is least in $S$

$\quad \langle 2 \rangle 5$. LET: $x \in S$

$\quad \quad$ PROVE: $a \leq x$

$\quad \langle 2 \rangle 6$. PICK $B \in \mathcal{C}$ such that $x \in B$

$\quad \langle 2 \rangle 7$. CASE: $A$ is an end extension of $B$

$\quad \quad \langle 3 \rangle 1$. $a \leq_A x$

⟨3⟩2. $a \leq x$

⟨2⟩8. CASE: $B$ is an end extension of $A$

  ⟨3⟩1. CASE: $x \in A$

    ⟨4⟩1. $a \leq_A x$

    ⟨4⟩2. $a \leq x$

  ⟨3⟩2. CASE: $x \in B - A$

    ⟨4⟩1. $a \leq_B x$

    ⟨4⟩2. $a \leq x$

⟨1⟩6. For all $A \in \mathcal{C}$, $W$ is an end extension of $A$.

  ⟨2⟩1. For all $x, y \in A$, we have $x \leq_A y$ if and only if $x \leq_W y$

    ⟨3⟩1. LET: $x, y \in A$

    ⟨3⟩2. If $x \leq_A y$ then $x \leq_W y$

    PROOF: Immediate from definitions.

    ⟨3⟩3. If $x \leq_W y$ then $x \leq_A y$

      ⟨4⟩1. ASSUME: $x \leq_W y$

      ⟨4⟩2. PICK $B \in \mathcal{C}$ such that $x \leq_B y$

      ⟨4⟩3. CASE: $A$ is an end extension of $B$

        PROOF: Then $x \leq_A y$.

      ⟨4⟩4. CASE: $B$ is an end extension of $A$

        PROOF: Then $x \leq_A y$.

  ⟨2⟩2. For all $x \in A$ and $y \in W - A$ we have $x < y$

    ⟨3⟩1. LET: $x \in A$ and $y \in W - A$

    ⟨3⟩2. PICK $B \in \mathcal{C}$ such that $y \in B$

    ⟨3⟩3. $B$ is an end extension of $A$

    ⟨3⟩4. $x <_B y$

    ⟨3⟩5. $x <_W y$

⟨1⟩7. For all $A \in \mathcal{C}$, the ordinal of $A$ is $\leq$ the ordinal of $W$.

  PROOF: Lemma 6.1.14.

⟨1⟩8. For any ordinal $\alpha$, if for all $A \in \mathcal{C}$ the ordinal of $A$ is $\leq \alpha$, then the ordinal of $W$ is $\leq \alpha$.

  ⟨2⟩1. LET: $\alpha$ be an ordinal.

  ⟨2⟩2. ASSUME: for all $A \in \mathcal{C}$, the ordinal of $A$ is $\leq \alpha$

  ⟨2⟩3. LET: $\beta$ be the ordinal of $W$

  ⟨2⟩4. LET: $E : W \approx \beta$ be the canonical isomorphism.

  ⟨2⟩5. ASSUME: for a contradiction $\alpha < \beta$

  ⟨2⟩6. LET: $a \in W$ be the element with $E(a) = \alpha$

  ⟨2⟩7. PICK $A \in \mathcal{C}$ such that $a \in A$

  ⟨2⟩8. LET: $\gamma$ be the ordinal of $A$ and $E_A : A \cong \gamma$ be the canonical isomorphism.

  ⟨2⟩9. For all $x \in A$ we have $E_A(x) = E(x)$

  PROOF: Transfinite induction on $x$.

  ⟨2⟩10. $E_A(a) = \alpha$

  ⟨2⟩11. $\alpha < \gamma$

  ⟨2⟩12. Q.E.D.

  PROOF: This contradicts ⟨2⟩2.

∎

## 6.2 Successors

**Definition 6.2.1** (Successor)**.** The *successor* of a set $a$ is the set $a^+ := a \cup \{a\}$.

**Proposition 6.2.2.** *A set $a$ is a transitive set if and only if*

$$\bigcup(a^+) = a \ .$$

Proof:
$\langle 1 \rangle 1$. If $a$ is a transitive set then $\bigcup(a^+) = a$.
   $\langle 2 \rangle 1$. Assume: $a$ is a transitive set.
   $\langle 2 \rangle 2$. $\bigcup(a^+) \subseteq a$
      $\langle 3 \rangle 1$. Let: $x \in \bigcup(a^+)$
            Prove: $\quad x \in a$
      $\langle 3 \rangle 2$. Pick $y \in a^+$ such that $x \in y$.
      $\langle 3 \rangle 3$. $y \in a$ or $y = a$.
      $\langle 3 \rangle 4$. Case: $y \in a$
        Proof: Then $x \in a$ because $a$ is a transitive set.
      $\langle 3 \rangle 5$. Case: $y = a$
        Proof: Then $x \in a$ immediately.
   $\langle 2 \rangle 3$. $a \subseteq \bigcup(a^+)$
     Proof: Since $a \in a^+$.
$\langle 1 \rangle 2$. If $\bigcup(a^+) = a$ then $a$ is a transitive set.
   $\langle 2 \rangle 1$. Assume: $\bigcup(a^+) = a$
   $\langle 2 \rangle 2$. $\bigcup a \subseteq a$
     Proof:

$$\bigcup a \subseteq \bigcup(a^+) \qquad\qquad \text{(Proposition 1.4.8)}$$
$$= a \qquad\qquad\qquad\qquad (\langle 2 \rangle 1)$$

   $\langle 2 \rangle 3$. $a$ is a transitive set.
     Proof: Proposition 1.5.2.
☐

**Proposition 6.2.3.** *For any set $a$, we have $a$ is a transitive set if and only if $a^+$ is a transitive set.*

Proof:
$\langle 1 \rangle 1$. If $a$ is a transitive set then $a^+$ is a transitiveset.
   Proof: If $a$ is a transitive set then $\bigcup(a^+) = a \subseteq a^+$ by Proposition 6.2.2 and
   so $a^+$ is a transitive set.
$\langle 1 \rangle 2$. If $a^+$ is a transitive set then $a$ is a transitive set.
   $\langle 2 \rangle 1$. Assume: $a^+$ is a transitive set.
   $\langle 2 \rangle 2$. Let: $x \in y \in a$
   $\langle 2 \rangle 3$. $x \in y \in a^+$
   $\langle 2 \rangle 4$. $x \in a^+$
     Proof: $\langle 2 \rangle 1$
   $\langle 2 \rangle 5$. $x \neq a$
     Proof: From $\langle 2 \rangle 2$ and the Axiom of Regularity.

$\langle 2 \rangle 6.$  $x \in a$

□

**Definition 6.2.4.** We write $0$ for $\emptyset$, $1$ for $\emptyset^+$, $2$ for $\emptyset^{++}$, etc.

**Proposition 6.2.5.** *For any set $A$ we have $\mathcal{P}A \approx 2^A$.*

PROOF: The function $H : \mathcal{P}A \to 2^A$ defined by $H(S)(a) = \{\emptyset\}$ if $a \in S$ and $\emptyset$ if $a \notin S$ is a bijection. □

**Proposition 6.2.6.** *For any ordinal number $\alpha$ we have $\alpha^+$ is an ordinal number.*

PROOF:
$\langle 1 \rangle 1.$  $\alpha^+$ is a transitive set.
 PROOF: Proposition 6.2.3.
$\langle 1 \rangle 2.$  $\alpha^+$ is well-ordered by $\in$.
  $\langle 2 \rangle 1.$  For all $x, y, z \in \alpha^+$, if $x \in y \in z$ then $x \in z$
   $\langle 3 \rangle 1.$  CASE: $z = \alpha$
   PROOF: Then $x \in \alpha$ since $\alpha$ is a transitive set.
   $\langle 3 \rangle 2.$  CASE: $z \in \alpha$
   PROOF: Then $x \in z$ since $\alpha$ is well-ordered by $\in$.
  $\langle 2 \rangle 2.$  For all $x, y \in \alpha^+$ we have $x \in y$ or $x = y$ or $y \in x$
   $\langle 3 \rangle 1.$  CASE: $x, y \in \alpha$
   PROOF: The result follows because $\alpha$ is well-ordered by $\in$.
   $\langle 3 \rangle 2.$  CASE: $x \in \alpha$, $y = \alpha$
   PROOF: Then $x \in y$.
   $\langle 3 \rangle 3.$  CASE: $x = \alpha$, $y \in \alpha$
   PROOF: Then $y \in x$.
   $\langle 3 \rangle 4.$  CASE: $x = \alpha$, $y = \alpha$
   PROOF: Then $x = y$.
  $\langle 2 \rangle 3.$  Every nonempty subset of $\alpha^+$ has an $\in$-least element.
   $\langle 3 \rangle 1.$  LET: $S \subseteq \alpha^+$ be nonempty
   $\langle 3 \rangle 2.$  CASE: $S = \{\alpha\}$
   PROOF: $\alpha$ is least in $S$.
   $\langle 3 \rangle 3.$  CASE: $S \neq \{\alpha\}$
    $\langle 4 \rangle 1.$  $S - \{\alpha\}$ is a nonempty subset of $\alpha$
    $\langle 4 \rangle 2.$  LET: $\beta$ be least in $S - \{\alpha\}$
    $\langle 4 \rangle 3.$  $\beta$ is least in $S$.
□

**Proposition 6.2.7.** *For ordinals $\alpha$ and $\beta$, if $\alpha^+ = \beta^+$ then $\alpha = \beta$.*

PROOF: If $\alpha^+ = \beta^+$ then
$$\alpha = \bigcup (\alpha^+) \qquad \text{(Proposition 6.2.2)}$$
$$= \bigcup (\beta^+)$$
$$= \beta \qquad \text{(Proposition 6.2.2)}$$

**Proposition 6.2.8.** *For ordinals $\alpha$ and $\beta$, we have $\alpha < \beta$ if and only if $\alpha^+ < \beta^+$.*

PROOF:

$$\alpha < \beta \Leftrightarrow \alpha^+ \leq \beta$$
$$\Leftrightarrow \alpha^+ < \beta^+ \qquad\qquad □$$

**Definition 6.2.9** (Successor Ordinal)**.** An ordinal $\alpha$ is a *successor ordinal* iff $\alpha = \beta^+$ for some $\beta$.

**Definition 6.2.10** (Limit Ordinal)**.** A *limit ordinal* is an ordinal that is neither 0 nor a successor ordinal.

**Proposition 6.2.11.** *If $\lambda$ is a limit ordinal and $\beta < \lambda$ then $\beta^+ < \lambda$.*

PROOF: Since $\beta^+ \leq \lambda$ and $\beta^+ \neq \lambda$. □

# 6.3   The Well-Ordering Theorem and Zorn's Lemma

**Theorem 6.3.1** (Hartogs)**.** *For any set A, there exists an ordinal not dominated by A.*

PROOF:
⟨1⟩1. LET: $\alpha$ be the class of all ordinals $\beta$ such that $\beta \preccurlyeq A$
    PROVE:   $\alpha$ is a set.
⟨1⟩2. LET: $W = \{(B, R) \mid B \subseteq A, R \text{ is a well ordering on } B\}$
⟨1⟩3. $\alpha$ is the class of the ordinals of the elements of $W$.
  ⟨2⟩1. For all $(B, R) \in W$, the ordinal of $(B, R)$ is in $\alpha$.
    ⟨3⟩1. LET: $(B, R) \in W$
    ⟨3⟩2. LET: $\beta$ be the ordinal of $(B, R)$
    ⟨3⟩3. LET: $E : B \cong \beta$ be the canonical isomorphism.
    ⟨3⟩4. LET: $i : B \hookrightarrow A$ be the inclusion
    ⟨3⟩5. $i \circ E^{-1}$ is an injection $\beta \to A$
    ⟨3⟩6. $\beta \in \alpha$
  ⟨2⟩2. For all $\beta \in \alpha$, there exists $(B, R) \in W$ such that $\beta$ is the ordinal number of $(B, R)$.
    ⟨3⟩1. LET: $\beta \in \alpha$
    ⟨3⟩2. PICK an injection $f : \beta \to A$
    ⟨3⟩3. Define $\leq$ on ran $f$ by $f(x) \leq f(y)$ iff $x \leq y$
    ⟨3⟩4. $(\text{ran } f, \leq) \in W$
    ⟨3⟩5. $\beta$ is the ordinal number of $(\text{ran } f, \leq)$
⟨1⟩4. $\alpha$ is a set.
  PROOF: By an Axiom of Replacement.
⟨1⟩5. $\alpha$ is an ordinal.
  PROOF: It is a transitive set of ordinals.
⟨1⟩6. $\alpha \not\preccurlyeq A$
  PROOF: Since $\alpha \notin \alpha$.

□

**Theorem 6.3.2** (Numeration Theorem). *Every set is equinumerous with some ordinal.*

PROOF:
⟨1⟩1. LET:  $A$  be any set.
⟨1⟩2. PICK an ordinal  $\alpha$  not dominated by  $A$ .
⟨1⟩3. PICK a choice function  $G$  for  $A$ .
⟨1⟩4. PICK  $e \notin A$ 
⟨1⟩5. LET:  $F : \alpha \to A \cup \{e\}$  by transfinite recursion:
$$F(\gamma) = \begin{cases} G(A - F(\{\delta \mid \delta < \gamma\})) & \text{if } A - F(\{\delta \mid \delta < \gamma\}) \neq \emptyset \\ e & \text{if } A - F(\{\delta \mid \delta < \gamma\}) = \emptyset \end{cases}$$
⟨1⟩6.  $e \in \operatorname{ran} F$ 
   ⟨2⟩1. ASSUME: for a contradiction  $e \notin \operatorname{ran} F$ 
   ⟨2⟩2.  $F$  is an injection  $\alpha \to A$ .
      ⟨3⟩1. LET:  $\beta, \gamma \in \alpha$  with  $\beta \neq \gamma$ 
          PROVE:   $F(\beta) \neq F(\gamma)$ 
      ⟨3⟩2. ASSUME: w.l.o.g.  $\beta < \gamma$ 
      ⟨3⟩3.  $F(\gamma) \in A - F(\{\delta \mid \delta < \gamma\})$ 
      ⟨3⟩4.  $F(\gamma) \notin F(\{\delta \mid \delta < \gamma\})$ 
      ⟨3⟩5.  $F(\gamma) \neq F(\beta)$ 
   ⟨2⟩3. Q.E.D.
      PROOF: This contradicts ⟨1⟩2.
⟨1⟩7. LET:  $\delta$  be least such that  $F(\delta) = e$ 
⟨1⟩8.  $F \upharpoonright \delta : \delta \approx A$ 

**Theorem 6.3.3** (Well-Ordering Theorem). *Any set can be well ordered.*

PROOF:
⟨1⟩1. PICK an ordinal  $\delta$  and a bijection  $F : A \approx \delta$ 
⟨1⟩2. Define  $\leq$  on  $A$  by  $F(x) \leq F(y)$  iff  $x \leq y$  for  $x, y \in \delta$ 
⟨1⟩3.  $\leq$  is a well ordering on  $A$ .
□

**Theorem 6.3.4** (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. PICK a well ordering  $<$  on  $\mathcal{A}$ .
⟨1⟩2. LET:  $F : \mathcal{A} \to 2$  be the function defined by transfinite recursion by:
$$F(A) = \begin{cases} 1 & \text{if } A \text{ includes every set } B < A \text{ for which } F(B) = 1 \\ 0 & \text{otherwise} \end{cases}$$
⟨1⟩3. LET:  $\mathcal{C} = \{A \in \mathcal{A} \mid F(A) = 1\}$ 
   PROVE:   $\bigcup \mathcal{C}$  is a maximal element of  $\mathcal{A}$ 
⟨1⟩4. For all  $A \in \mathcal{A}$ , we have  $A \in \mathcal{C}$  iff  $\forall B < A.B \in \mathcal{C} \Rightarrow B \subseteq A$ 
⟨1⟩5.  $\mathcal{C}$  is a chain.

     $\langle 2 \rangle$1. LET: $A, A' \in \mathcal{C}$
     $\langle 2 \rangle$2. ASSUME: w.l.o.g. $A \leq A'$
     $\langle 2 \rangle$3. $A \subseteq A'$
       PROOF: By $\langle 1 \rangle$4
$\langle 1 \rangle$6. $\bigcup \mathcal{C} \in \mathcal{A}$
$\langle 1 \rangle$7. $\bigcup \mathcal{C}$ is maximal in $\mathcal{A}$.
     $\langle 2 \rangle$1. LET: $A \in \mathcal{A}$ and $\bigcup \mathcal{C} \subseteq A$
     $\langle 2 \rangle$2. $A \in \mathcal{C}$
       PROOF: By $\langle 1 \rangle$4 since $\forall B \in \mathcal{C}.B \subseteq A$.
     $\langle 2 \rangle$3. $A \subseteq \bigcup \mathcal{C}$
     $\langle 2 \rangle$4. $A = \bigcup \mathcal{C}$
☐

**Proposition 6.3.5** (Teichmüller-Tukey Lemma). *Let $\mathcal{A}$ be a nonempty set such that, for every $B$, we have $B \in \mathcal{A}$ if and only if every finite subset of $B$ is a member of $\mathcal{A}$. Then $\mathcal{A}$ has a maximal element.*

PROOF:
$\langle 1 \rangle$1. For every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$
     $\langle 2 \rangle$1. LET: $\mathcal{B} \subseteq \mathcal{A}$ be a chain.
     $\langle 2 \rangle$2. Every finite subset of $\bigcup \mathcal{B}$ is a member of $\mathcal{A}$.
       $\langle 3 \rangle$1. LET: $C$ be a finite subset of $\bigcup \mathcal{B}$.
       $\langle 3 \rangle$2. PICK $B \in \mathcal{B}$ such that $C \subseteq B$.
       $\langle 3 \rangle$3. $B \in \mathcal{A}$
       $\langle 3 \rangle$4. Every finite subset of $B$ is in $\mathcal{A}$.
       $\langle 3 \rangle$5. $C \in \mathcal{A}$
     $\langle 2 \rangle$3. $\bigcup \mathcal{B} \in \mathcal{A}$.
$\langle 1 \rangle$2. Q.E.D.
     PROOF: Zorn's lemma.
☐

**Theorem Schema 6.3.6.** *For any class $\mathbf{A}$, there exists a class $\mathbf{F}$ such that the following is a theorem:*
     *If $\mathbf{A}$ is a proper class of ordinals, then $\mathbf{F} : \mathbf{On} \to \mathbf{A}$ is an order isomorphism.*

PROOF:
$\langle 1 \rangle$1. Define $\mathbf{F} : \mathbf{On} \to \mathbf{A}$ by transfinite recursion as follows: $\mathbf{F}(\alpha)$ is the least element of $\mathbf{A}$ that is different from $\mathbf{F}(\beta)$ for all $\beta < \alpha$.
$\langle 1 \rangle$2. For all $\alpha, \beta \in \mathbf{On}$, if $\alpha < \beta$ then $\mathbf{F}(\alpha) < \mathbf{F}(\beta)$
     PROOF: We have $\mathbf{F}(\alpha) \neq \mathbf{F}(\beta)$ by the definition of $\mathbf{F}(\beta)$, and $\mathbf{F}(\beta) \not< \mathbf{F}(\alpha)$ by the leastness of $\mathbf{F}(\alpha)$.
$\langle 1 \rangle$3. $\mathbf{F}$ is surjective.
     $\langle 2 \rangle$1. LET: $\alpha \in \mathbf{A}$
     $\langle 2 \rangle$2. ASSUME: as transfinite induction hypothesis $\forall \beta \in \mathbf{A}$, if $\beta < \alpha$ then there exists $\gamma$ such that $\beta = \mathbf{F}(\gamma)$.
     $\langle 2 \rangle$3. LET: $\gamma = \{\delta \in \mathbf{On} \mid \mathbf{F}(\delta) < \alpha\}$
     $\langle 2 \rangle$4. $\gamma$ is a set.

PROOF: Axiom of Replacement applied to $\alpha$.

$\langle 2 \rangle 5$.  $\gamma$ is a transitive set.

PROOF: If $\mathbf{F}(\delta) < \alpha$ and $\epsilon < \delta$ then $\mathbf{F}(\epsilon) < \alpha$ by $\langle 1 \rangle 2$.

$\langle 2 \rangle 6$.  $\gamma$ is an ordinal.

PROOF: Proposition 6.1.8.

$\langle 2 \rangle 7$.  $\mathbf{F}(\gamma) = \alpha$

$\langle 3 \rangle 1$.  $\mathbf{F}(\gamma)$ is the least element of $\mathbf{A}$ different from $\mathbf{F}(\delta)$ for all $\delta < \gamma$

$\langle 3 \rangle 2$.  $\mathbf{F}(\gamma)$ is the least element of $\mathbf{A}$ different from $x$ for all $x \in \mathbf{A}$ with $x < \alpha$

$\langle 3 \rangle 3$.  $\mathbf{F}(\gamma) = \alpha$

☐

## 6.4   Ordinal Operations

**Definition 6.4.1** (Ordinal Operation)**.** An *ordinal operation* is a function $\mathbf{On} \to \mathbf{On}$.

**Definition 6.4.2** (Continuous)**.** An ordinal operation $\mathbf{T} : \mathbf{On} \to \mathbf{On}$ is *continuous* iff, for every limit ordinal $\lambda$, we have $\mathbf{T}(\lambda) = \bigcup_{\alpha < \lambda} \mathbf{T}(\alpha)$.

**Definition 6.4.3** (Normal)**.** An ordinal operation is *normal* iff it is continuous and strictly monotone.

**Proposition Schema 6.4.4.** *For any class* $\mathbf{T}$*, the following is a theorem.*

*If* $\mathbf{T}$ *is a continuous ordinal operation and* $\forall \gamma. \mathbf{T}(\gamma) < \mathbf{T}(\gamma^+)$*, then* $\mathbf{T}$ *is normal.*

PROOF:

$\langle 1 \rangle 1$.  LET:  $P[\beta]$ be the property $\forall \gamma < \beta. \mathbf{T}(\gamma) < \mathbf{T}(\beta)$

$\langle 1 \rangle 2$.  $P[0]$

PROOF: Vacuous.

$\langle 1 \rangle 3$.  For any ordinal $\gamma$, if $P[\gamma]$ then $P[\gamma^+]$

$\langle 2 \rangle 1$.  ASSUME:  $P[\gamma]$

$\langle 2 \rangle 2$.  LET:  $\delta < \gamma^+$

$\langle 2 \rangle 3$.  CASE:  $\delta < \gamma$

PROOF: Then $\mathbf{T}(\delta) < \mathbf{T}(\gamma) < \mathbf{T}(\gamma^+)$.

$\langle 2 \rangle 4$.  CASE:  $\delta = \gamma$

PROOF: Then $\mathbf{T}(\delta) = \mathbf{T}(\gamma) < \mathbf{T}(\gamma^+)$.

$\langle 1 \rangle 4$.  For any limit ordinal $\lambda$, if $\forall \gamma < \lambda. P[\gamma]$ then $P[\lambda]$.

$\langle 2 \rangle 1$.  ASSUME:  $\forall \gamma < \lambda. P[\gamma]$

$\langle 2 \rangle 2$.  LET:  $\delta < \lambda$

$\langle 2 \rangle 3$.  $\mathbf{T}(\delta) < \mathbf{T}(\lambda)$

PROOF:

$$
\begin{aligned}
\mathbf{T}(\delta) &< \mathbf{T}(\delta^+) \\
&\leq \bigcup_{\epsilon < \lambda} \mathbf{T}(\epsilon) \\
&= \mathbf{T}(\lambda)
\end{aligned}
$$

☐

**Proposition Schema 6.4.5.** *For any class* **T***, the following is a theorem:*

*Assume* **T** *is a normal ordinal operation.  For every ordinal $\alpha$, we have $\alpha \leq \mathbf{T}(\alpha)$.*

PROOF:
⟨1⟩1. LET: $\gamma$ be an ordinal.
⟨1⟩2. ASSUME: as induction hypothesis $\forall \delta < \gamma.\mathbf{T}(\delta) \geq \delta$
⟨1⟩3. For all $\delta < \gamma$ we have $\delta < \mathbf{T}(\gamma)$
    PROOF: **T** is strictly monotone.
⟨1⟩4. $\gamma \leq \mathbf{T}(\gamma)$
☐

**Proposition Schema 6.4.6.** *For any class* **T***, the following is a theorem:*

*Assume* **T** *is a normal ordinal operation.  For any ordinal $\beta \geq \mathbf{T}(0)$, there exists a greatest ordinal $\gamma$ such that $\mathbf{T}(\gamma) \leq \beta$.*

PROOF:
⟨1⟩1. There exists $\gamma$ such that $\mathbf{T}(\gamma) > \beta$
    ⟨2⟩1. For all $\gamma$ we have $\mathbf{T}(\gamma) \geq \gamma$
        PROOF: Proposition 6.4.5.
    ⟨2⟩2. $\mathbf{T}(\beta^+) > \beta$
⟨1⟩2. LET: $\delta$ be least such that $\mathbf{T}(\delta) > \beta$
⟨1⟩3. $\delta$ is a successor ordinal.
    ⟨2⟩1. $\delta \neq 0$
        PROOF: Since $\mathbf{T}(0) \leq \beta$.
    ⟨2⟩2. $\delta$ is not a limit ordinal.
        ⟨3⟩1. ASSUME: for a contradiction $\delta$ is a limit ordinal.
        ⟨3⟩2. $\beta < \bigcup_{\epsilon < \delta} \mathbf{T}(\epsilon)$
            PROOF: **T** is continuous.
        ⟨3⟩3. There exists $\epsilon < \delta$ such that $\beta < \mathbf{T}(\epsilon)$
        ⟨3⟩4. Q.E.D.
            PROOF: This contradicts the minimality of $\delta$.
⟨1⟩4. LET: $\delta = \gamma^+$
⟨1⟩5. $\gamma$ is greatest such that $\mathbf{T}(\gamma) \leq \beta$
☐

**Theorem Schema 6.4.7.** *For any class* **T***, the following is a theorem:*

*Assume that* **T** *is a normal ordinal operation.  For any nonempty set of ordinals S, we have*

$$\mathbf{T}(\sup S) = \sup_{\alpha \in S} \mathbf{T}(\alpha) \ .$$

PROOF:
⟨1⟩1. $\forall \alpha \in S.\mathbf{T}(\alpha) \leq \mathbf{T}(\sup S)$
    PROOF: Since **T** is monotone.
⟨1⟩2. For any ordinal $\beta$, if $\forall \alpha \in S.\mathbf{T}(\alpha) \leq \beta$, then $\mathbf{T}(\sup S) \leq \beta$

⟨2⟩1. LET:  $\beta$ be an ordinal.
⟨2⟩2. LET:  $\gamma = \sup S$
⟨2⟩3. ASSUME:  $\forall \alpha \in S.\mathbf{T}(\alpha) \leq \beta$
⟨2⟩4. CASE:  $\gamma$ is 0 or a successor ordinal
  PROOF: Then we must have $\gamma \in S$ so $\mathbf{T}(\gamma) \leq \beta$ from ⟨2⟩3.
⟨2⟩5. CASE:  $\gamma$ is a limit ordinal
  ⟨3⟩1.  $\mathbf{T}(\gamma) = \sup_{\alpha < \gamma} \mathbf{T}(\alpha)$
    PROOF: $\mathbf{T}$ is continuous.
  ⟨3⟩2. ASSUME:  for a contradiction $\beta < \mathbf{T}(\gamma)$
  ⟨3⟩3. PICK $\alpha < \gamma$ such that $\beta < \mathbf{T}(\alpha)$
    PROOF: ⟨3⟩1, ⟨3⟩2
  ⟨3⟩4. PICK $\alpha' \in S$ such that $\alpha < \alpha'$
    PROOF: ⟨2⟩2, ⟨3⟩3
  ⟨3⟩5.  $\beta < \mathbf{T}(\alpha') \leq \beta$
    PROOF: $\mathbf{T}$ is strictly monotone, ⟨3⟩3, ⟨3⟩4, ⟨2⟩3.
  ⟨3⟩6. Q.E.D.
    PROOF: This is a contradiction.

☐

**Proposition 6.4.8.**  *For any classes $\mathbf{A}$ and $\mathbf{T}$, the following is a theorem:*

  *Assume $\mathbf{A}$ is a proper class of ordinals such that, for every set $S \subseteq \mathbf{A}$, we have $\bigcup S \in \mathbf{A}$. Assume $\mathbf{T}$ is the unique order isomorphism $\mathbf{On} \cong \mathbf{A}$. Then $\mathbf{T}$ is normal.*

PROOF:
⟨1⟩1.  $\mathbf{T}$ is strictly monotone.
  PROOF: Since it is an order isomorphism.
⟨1⟩2.  $\mathbf{T}$ is continuous.
  ⟨2⟩1. LET:  $\lambda$ be a limit ordinal.
  ⟨2⟩2.  $\mathbf{T}'(\lambda)$ is the least member of $\mathbf{A}$ that is greater than $\mathbf{T}'(\alpha)$ for all $\alpha < \lambda$
  ⟨2⟩3.  $\mathbf{T}'(\lambda) = \sup_{\alpha < \lambda} \mathbf{T}'(\alpha)$

☐

**Proposition Schema 6.4.9.**  *For any class $\mathbf{T}$, the following is a theorem:*

  *If $\mathbf{T}$ is a normal ordinal operation, then for any limit ordinal $\lambda$, we have $\mathbf{T}(\lambda)$ is a limit ordinal.*

PROOF:
⟨1⟩1.  $\mathbf{T}(\lambda) \neq 0$
  PROOF: Since $0 \leq \mathbf{T}(0) < \mathbf{T}(\lambda)$.
⟨1⟩2.  $\mathbf{T}(\lambda)$ is not a successor ordinal.
  ⟨2⟩1. ASSUME:  for a contradiction $\mathbf{T}(\lambda) = \alpha^+$
  ⟨2⟩2.  $\alpha < \mathbf{T}(\lambda) = \sup_{\beta < \lambda} \mathbf{T}(\beta)$
  ⟨2⟩3. PICK $\beta < \lambda$ such that $\alpha < \mathbf{T}(\beta)$
  ⟨2⟩4.  $\alpha^+ \leq \mathbf{T}(\beta) < \mathbf{T}(\lambda)$
  ⟨2⟩5. Q.E.D.
    PROOF: This is a contradiction.

☐

## 6.5 Ordinal Arithmetic

### 6.5.1 Addition

**Definition 6.5.1.** Let $A$ and $B$ be disjoint well-ordered sets. The *concatenation* of $A$ and $B$ is the set $A \cup B$ under the relation:

- if $a, a' \in A$ then $a \leq a'$ iff $a \leq a'$ in $A$

- if $b, b' \in B$ then $b \leq b'$ iff $b \leq b'$ in $B$

- if $a \in A$ and $b \in B$ then $a \leq b$ and $b \not\leq a$.

**Proposition 6.5.2.** *If $A$ and $B$ are disjoint well-ordered sets, then their concatenation is well-ordered.*

PROOF:
$\langle 1 \rangle 1.$ $\leq$ is reflexive.
   PROOF: For all $a \in A$ we have $a \leq a$, and for all $b \in B$ we have $b \leq b$.
$\langle 1 \rangle 2.$ $\leq$ is antisymmetric.
   $\langle 2 \rangle 1.$ ASSUME: $x \leq y \leq x$
   $\langle 2 \rangle 2.$ CASE: $x, y \in A$
     PROOF: Then $x = y$ since the order on $A$ is antisymmetric.
   $\langle 2 \rangle 3.$ CASE: $x \in A$ and $y \in B$
     PROOF: This is impossible as it would imply $y \not\leq x$.
   $\langle 2 \rangle 4.$ CASE: $x \in B$ and $y \in A$
     PROOF: This is impossible as it would imply $x \not\leq y$.
   $\langle 2 \rangle 5.$ CASE: $x, y \in B$
     PROOF: Then $x = y$ since the order on $B$ is antisymmetric.
$\langle 1 \rangle 3.$ $\leq$ is transitive.
   $\langle 2 \rangle 1.$ ASSUME: $x \leq y \leq z$
   $\langle 2 \rangle 2.$ CASE: $x, z \in A$
     PROOF: In this case $y \in A$ since $y \leq z$, and so $x \leq z$ since the order on $A$ is transitive.
   $\langle 2 \rangle 3.$ CASE: $x \in A$ and $z \in B$
     PROOF: Then $x \leq z$ immediately.
   $\langle 2 \rangle 4.$ CASE: $x \in B$ and $z \in A$
     PROOF: This is impossible because we have $y \notin A$ since $x \leq y$ and $y \notin B$ since $y \leq z$.
   $\langle 2 \rangle 5.$ CASE: $x, z \in B$
     PROOF: In this case $y \in B$ since $x \leq y$, and so $x \leq z$ since the order on $B$ is transitive.
$\langle 1 \rangle 4.$ $\leq$ is total.
   $\langle 2 \rangle 1.$ LET: $x, y \in A \cup B$
   $\langle 2 \rangle 2.$ CASE: $x, y \in A$
     PROOF: Then $x \leq y$ or $y \leq x$ because the order on $A$ is total.
   $\langle 2 \rangle 3.$ CASE: $x \in A$ and $y \in B$
     PROOF: Then $x \leq y$.

$\langle 2 \rangle 4$. CASE: $x \in B$ and $y \in A$
    PROOF: Then $y \leq x$.
$\langle 2 \rangle 5$. CASE: $x, y \in B$
    PROOF: Then $x \leq y$ or $y \leq x$ because the order on $B$ is total.
$\langle 1 \rangle 5$. Every nonempty subset of $A \cup B$ has a least element.
  $\langle 2 \rangle 1$. LET: $S$ be a nonempty subset of $A \cup B$
  $\langle 2 \rangle 2$. CASE: $S \cap A = \emptyset$
    PROOF: Then $S \subseteq B$ and so $S$ has a least element.
  $\langle 2 \rangle 3$. CASE: $S \cap A \neq \emptyset$
    PROOF: The least element of $S \cap A$ is the least element of $S$.

$\square$

**Definition 6.5.3** (Ordinal Addition)**.** Let $\alpha$ and $\beta$ be ordinal numbers. Then $\alpha + \beta$ is the ordinal number of the concatenation of $A$ and $B$, where $A$ is any well ordered set with ordinal $\alpha$ and $B$ is any well ordered set with ordinal $\beta$.

**Theorem 6.5.4** (Associative Law for Addition)**.** *For any ordinals $\rho$, $\sigma$ and $\tau$, we have*

$$\rho + (\sigma + \tau) = (\rho + \sigma) + \tau \ .$$

PROOF: Given disjoint well ordered sets $A$, $B$ and $C$, the concatenation of $A$ with (the concatenation of $B$ and $C$) is the same as the concatenation of (the concatenation of $A$ and $B$) and $C$. $\square$

**Theorem 6.5.5.** *For any ordinal $\rho$ we have*

$$\rho + 0 = 0 + \rho = \rho \ .$$

PROOF: For any well ordered set $A$, the concatenation of $A$ with $\emptyset$ is $A$, and the concatenation of $\emptyset$ with $A$ is $A$. $\square$

**Theorem 6.5.6.** *For any ordinal $\alpha$ we have $\alpha + 1 = \alpha^+$.*

PROOF: Since $\alpha^+$ is the concatenation of $\alpha$ and $\{\alpha\}$. $\square$

**Theorem 6.5.7.** *For any ordinal $\alpha$, the operation that maps $\beta$ to $\alpha + \beta$ is normal.*

PROOF:
$\langle 1 \rangle 1$. For any limit ordinal $\lambda$, we have $\alpha + \lambda = \sup_{\beta < \lambda} (\alpha + \beta)$.
  $\langle 2 \rangle 1$. LET: $\lambda$ be a limit ordinal.
  $\langle 2 \rangle 2$. $(\{0\} \times \alpha) \cup (\{1\} \times \lambda) = \bigcup_{\beta \in \lambda} ((\{0\} \times \alpha) \cup (\{1\} \times \beta))$, where the order on the right hand side is as in Lemma 6.1.15.
    PROOF:

$$(\{0\} \times \alpha) \cup (\{1\} \times \lambda) = (\{0\} \times \alpha) \cup (\{1\} \times \bigcup_{\beta < \lambda} \beta)$$

$$= (\{0\} \times \alpha) \cup \bigcup_{\beta < \lambda} (\{1\} \times \beta)$$

$$= \bigcup_{\beta < \lambda} ((\{0\} \times \alpha) \cup (\{1\} \times \beta))$$

$\langle 1 \rangle 2$. For any ordinal $\beta$ we have $\alpha + \beta < \alpha + \beta^+$
  PROOF: Since $\alpha + \beta^+ = \alpha + \beta + 1 = (\alpha + \beta)^+$.
☐

**Corollary 6.5.7.1.** *For any ordinals $\alpha$, $\beta$, $\gamma$, we have $\beta < \gamma$ if and only if $\alpha + \beta < \alpha + \gamma$.*

**Corollary 6.5.7.2** (Left Cancellation for Addition)**.** *For any ordinals $\alpha$, $\beta$ and $\gamma$, if $\alpha + \beta = \alpha + \gamma$ then $\beta = \gamma$.*

**Theorem 6.5.8.** *For any ordinals $\alpha$, $\beta$, $\gamma$, if $\beta \leq \gamma$ then $\beta + \alpha \leq \gamma + \alpha$.*

PROOF: Transfinite induction on $\alpha$. ☐

**Theorem 6.5.9** (Subtraction Theorem)**.** *Let $\alpha$ and $\beta$ be ordinals with $\alpha \leq \beta$. Then there exists a unique ordinal $\delta$ such that $\alpha + \delta = \beta$.*

PROOF:
$\langle 1 \rangle 1$. For all ordinals $\alpha$ and $\beta$ with $\alpha \leq \beta$, there exists $\delta$ such that $\alpha + \delta = \beta$
  $\langle 2 \rangle 1$. LET: $\alpha$ and $\beta$ be ordinals with $\alpha \leq \beta$
  $\langle 2 \rangle 2$. LET: $\delta$ be the greatest ordinal such that $\alpha + \delta \leq \beta$
    PROOF: Proposition 6.4.6.
  $\langle 2 \rangle 3$. $\alpha + \delta = \beta$
    PROOF: If $\alpha + \delta < \beta$ then $\alpha + \delta + 1 \leq \beta$ contradicting the greatestness of $\delta$.
$\langle 1 \rangle 2$. Q.E.D.
  PROOF: Uniqueness follows from the Left Cancellation Law.
☐

## 6.5.2   Multiplication

**Definition 6.5.10** (Ordinal Multiplication)**.** Let $\alpha$ and $\beta$ be ordinal numbers. Then $\alpha\beta$ is the ordinal number of $A \times B$ under the lexicographic order, where $A$ is any well ordered set with ordinal $\alpha$ and $B$ is any well ordered set with ordinal $\beta$.

  This is well defined by Proposition 5.3.3.

**Theorem 6.5.11** (Associative Law)**.** *For any ordinals $\rho$, $\sigma$ and $\tau$, we have*

$$\rho(\sigma\tau) = (\rho\sigma)\tau \ .$$

PROOF: Let $A$, $B$ and $C$ be well ordered sets with ordinals $\rho$, $\sigma$ and $\tau$. Then both $\rho(\sigma\tau)$ and $(\rho\sigma)\tau$ are the ordinal of $A \times B \times C$ under
$(a, b, c) \leq (a', b', c') \Leftrightarrow a \leq a' \lor (a = a' \land b \leq b') \lor (a = a' \land b = b' \land c \leq c') \ .$    ☐

**Theorem 6.5.12** (Left Distributive Law)**.** *For any ordinals $\rho$, $\sigma$ and $\tau$, we have*

$$\rho(\sigma + \tau) = \rho\sigma + \rho\tau$$

PROOF: Let $A$, $B$ and $C$ be well ordered sets with ordinals $\rho$, $\sigma$ and $\tau$ and with $B \cap C = \emptyset$. Then both $\rho(\sigma + \tau)$ and $\rho\sigma + \rho\tau$ are the ordinal of $A \times (B \cup C)$ under the lexicographic ordering. $\square$

**Theorem 6.5.13.** *For any ordinal $\rho$ we have $\rho 0 = 0\rho = 0$.*

PROOF: For any well ordered set $A$ we have $A \times \emptyset = \emptyset \times A = \emptyset$. $\square$

**Theorem 6.5.14.** *For any ordinal $\rho$ we have $\rho 1 = 1\rho = \rho$.*

PROOF: Easy. $\square$

**Theorem 6.5.15.** *For any ordinals $\rho$ and $\sigma$, if $\rho\sigma = 0$ then $\rho = 0$ or $\sigma = 0$.*

PROOF: If $A \times B = \emptyset$ then $A = \emptyset$ or $B = \emptyset$. $\square$

**Theorem 6.5.16.** *For any non-zero ordinal $\alpha$, the operation that maps $\beta$ to $\alpha\beta$ is normal.*

PROOF:
$\langle 1 \rangle 1$. For any limit ordinal $\lambda$, we have $\alpha\lambda = \bigcup_{\beta < \lambda} \alpha\beta$
    $\langle 2 \rangle 1$. LET: $\lambda$ be a limit ordinal
    $\langle 2 \rangle 2$. $\alpha \times \lambda = \bigcup_{\beta < \lambda} (\alpha \times \beta)$ as well-ordered sets
$\langle 1 \rangle 2$. For any ordinal $\beta$ we have $\alpha\beta < \alpha\beta^+$
    PROOF: $\alpha\beta^+ = \alpha\beta + \alpha > \alpha\beta$
$\square$

**Corollary 6.5.16.1.** *For any ordinals $\alpha$, $\beta$, $\gamma$, if $\alpha \neq 0$ then $\beta < \gamma$ if and only if $\alpha\beta < \alpha\gamma$.*

**Corollary 6.5.16.2** (Left Cancellation for Multiplication)**.** *For any ordinals $\alpha$, $\beta$, $\gamma$, if $\alpha \neq 0$ and $\alpha\beta = \alpha\gamma$ then $\beta = \gamma$.*

**Theorem 6.5.17.** *For any ordinals $\alpha$, $\beta$ and $\gamma$, if $\beta \leq \gamma$ then $\beta\alpha \leq \gamma\alpha$.*

PROOF: Transfinite induction on $\alpha$. $\square$

**Theorem 6.5.18** (Division Theorem)**.** *Let $\alpha$ and $\delta$ be ordinal numbers with $\delta \neq 0$. Then there exist unique ordinals $\beta$ and $\gamma$ with $\gamma < \delta$ and*

$$\alpha = \delta\beta + \gamma \ .$$

PROOF:
$\langle 1 \rangle 1$. For any ordinal numbers $\alpha$ and $\delta$ with $\delta \neq 0$, there exist ordinals $\beta$ and $\gamma$ such that $\gamma < \delta$ and $\alpha = \delta\beta + \gamma$
    $\langle 2 \rangle 1$. LET: $\alpha$ and $\delta$ be ordinals with $\delta \neq 0$
    $\langle 2 \rangle 2$. LET: $\beta$ be the greatest ordinal such that $\delta\beta \leq \alpha$
        PROOF: Proposition 6.4.6.
    $\langle 2 \rangle 3$. There exists an ordinal $\gamma$ such that $\alpha = \delta\beta + \gamma$
        PROOF: Subtraction Theorem

⟨1⟩2. For any ordinals $\delta$, $\beta$, $\beta'$, $\gamma$, $\gamma'$, if $\delta\beta+\gamma = \delta\beta'+\gamma'$ and $\delta \neq 0$ and $\gamma, \gamma' < \delta$ then $\beta = \beta'$ and $\gamma = \gamma'$

  ⟨2⟩1. LET: $\delta$, $\beta$, $\beta'$, $\gamma$, $\gamma'$ be ordinals.

  ⟨2⟩2. ASSUME: $\delta \neq 0$ and $\delta\beta + \gamma = \delta\beta' + \gamma'$

  ⟨2⟩3. $\beta = \beta'$

    ⟨3⟩1. $\beta \not< \beta'$

      PROOF: If $\beta < \beta'$ then

$$\begin{aligned}
\delta\beta' + \gamma' &\geq \delta\beta' \\
&\geq \delta(\beta + 1) \\
&= \delta\beta + \delta \\
&> \delta\beta + \gamma
\end{aligned}$$

    ⟨3⟩2. $\beta' \not< \beta$

      PROOF: Similar.

  ⟨2⟩4. $\gamma = \gamma'$

    PROOF: By Cancellation.

☐

## 6.5.3 Exponentiation

**Definition 6.5.19.** Given ordinals $\alpha$ and $\beta$, define the ordinal $\alpha^\beta$ as follows:

$$\begin{aligned}
0^\alpha &:= 0 & (\alpha > 0) \\
\alpha^0 &:= 1 & \\
\alpha^{\beta^+} &:= \alpha^\beta \alpha & (\alpha > 0) \\
\alpha^\lambda &:= \sup_{\beta<\lambda} \alpha^\beta & (\alpha > 0, \lambda \text{ a limit ordinal})
\end{aligned}$$

**Theorem 6.5.20.** *Let $\alpha$ be an ordinal $\geq 2$. The operation that maps $\beta$ to $\alpha^\beta$ is normal.*

PROOF:

⟨1⟩1. For $\lambda$ a limit ordinal we have $\alpha^\lambda = \sup_{\beta<\lambda} \alpha^\beta$

  PROOF: By definition.

⟨1⟩2. For any ordinal $\beta$ we have $\alpha^\beta < \alpha^{\beta^+}$

  PROOF: We have $\alpha^{\beta^+} = \alpha^\beta \alpha > \alpha^\beta$ by Theorem 6.5.16 since $\alpha > 1$ and $\alpha^\beta \neq 0$.

☐

**Corollary 6.5.20.1.** *For any ordinals $\alpha$, $\beta$, $\gamma$, if $\alpha \geq 2$ then $\beta < \gamma$ if and only if $\alpha^\beta < \alpha^\gamma$.*

**Corollary 6.5.20.2** (Cancellation for Exponentiation)**.** *For any ordinals $\alpha$, $\beta$, $\gamma$, if $\alpha \geq 2$ and $\alpha^\beta = \alpha^\gamma$ then $\beta = \gamma$.*

**Theorem 6.5.21.** *For any ordinals $\alpha$, $\beta$ and $\gamma$, if $\beta \leq \gamma$ then $\beta^\alpha \leq \gamma^\alpha$.*

PROOF: Transfinite induction on $\alpha$.

**Theorem 6.5.22** (Logarithm Theorem)**.** *Let $\alpha$ and $\beta$ be ordinal numbers with $\alpha \neq 0$ and $\beta > 1$. Then there exist unique ordinals $\gamma$, $\delta$ and $\rho$ such that*

$$\alpha = \beta^\gamma \delta + \rho, \qquad 0 \neq \delta < \beta, \qquad \rho < \beta^\gamma \ .$$

PROOF:

⟨1⟩1. For any ordinals $\alpha$ and $\beta$ with $\alpha \neq 0$ and $\beta > 1$, there exist ordinals $\gamma$, $\delta$, $\rho$ such that

$$\alpha = \beta^\gamma \delta + \rho, \qquad 0 \neq \delta < \beta, \qquad \rho < \beta^\gamma \ .$$

  ⟨2⟩1. LET: $\alpha$ and $\beta$ be ordinals with $\alpha \neq 0$ and $\beta > 1$.

  ⟨2⟩2. LET: $\gamma$ be the greatest ordinal such that $\beta^\gamma \leq \alpha$.

    PROOF: Proposition 6.4.6.

  ⟨2⟩3. LET: $\delta$ and $\rho$ be the unique ordinals with $\rho < \beta^\gamma$ such that $\alpha = \beta^\gamma \delta + \rho$.

    PROOF: By the Division Theorem.

  ⟨2⟩4. $\delta \neq 0$

    PROOF: If $\delta = 0$ then $\alpha = \beta^\gamma 0 + \rho = \rho < \beta^\gamma \leq \alpha$ which is a contradiction.

  ⟨2⟩5. $\delta < \beta$

    PROOF: If $\beta \leq \delta$ then $\alpha \geq \beta^\gamma \delta \geq \beta^\gamma \beta = \beta^{\gamma+1}$, contradicting the greatestness of $\gamma$.

⟨1⟩2. If $\beta^\gamma \delta + \rho = \beta^{\gamma'} \delta' + \rho'$ with $\beta > 1$, $0 \neq \delta < \beta$, $0 \neq \delta' < \beta$, $\rho < \beta^\gamma$ and $\rho' < \beta^{\gamma'}$, then $\gamma = \gamma'$, $\delta = \delta'$ and $\rho = \rho'$.

  ⟨2⟩1. LET: $\alpha = \beta^\gamma \delta + \rho = \beta^{\gamma'} \delta' + \rho'$

  ⟨2⟩2. $\beta^\gamma \leq \alpha < \beta^{\gamma+1}$

  ⟨2⟩3. $\beta^{\gamma'} \leq \alpha < \beta^{\gamma'+1}$

  ⟨2⟩4. $\beta^\gamma < \beta^{\gamma'+1}$ and $\beta^{\gamma'} < \beta^{\gamma+1}$

  ⟨2⟩5. $\gamma < \gamma' + 1$ and $\gamma' < \gamma + 1$

  ⟨2⟩6. $\gamma = \gamma'$

  ⟨2⟩7. $\delta = \delta'$ and $\rho = \rho'$

    PROOF: By the Division Theorem.

☐

**Theorem 6.5.23.** *For any ordinal numbers $\alpha$, $\beta$, $\gamma$, we have*

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

PROOF:

⟨1⟩1. LET: $P[\gamma]$ be the property: for any ordinals $\alpha$ and $\beta$ we have $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$

⟨1⟩2. $P[0]$

  PROOF:

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

⟨1⟩3. For all $\gamma$, if $P[\gamma]$ then $P[\gamma + 1]$

  PROOF:

$$\begin{aligned}
\alpha^{\beta+\gamma+1} &= \alpha^{\beta+\gamma} \alpha \\
&= \alpha^\beta \alpha^\gamma \alpha && \text{(induction hypothesis)} \\
&= \alpha^\beta \alpha^{\gamma+1}
\end{aligned}$$

⟨1⟩4.  For any limit ordinal $\lambda$, if $\forall \gamma < \lambda.P[\gamma]$ then $P[\lambda]$.

   ⟨2⟩1.  LET:  $\lambda$ be a limit ordinal

   ⟨2⟩2.  ASSUME:  $\forall \gamma < \lambda.P[\gamma]$

   ⟨2⟩3.  LET:  $\alpha$ and $\beta$ be any ordinals.

   ⟨2⟩4.  CASE:  $\alpha = 0$

     PROOF: We have $\alpha^{\beta+\lambda} = \alpha^{\beta}\alpha^{\lambda} = 0$.

   ⟨2⟩5.  CASE:  $\alpha = 1$

     PROOF: We have $\alpha^{\beta+\lambda} = \alpha^{\beta}\alpha^{\lambda} = 1$.

   ⟨2⟩6.  CASE:  $\alpha > 1$

     PROOF:

$$\alpha^{\beta+\lambda} = \alpha^{\sup_{\gamma<\lambda}(\beta+\gamma)}$$

$$= \sup_{\gamma<\lambda} \alpha^{\beta+\gamma} \qquad\qquad \text{(Theorem 6.4.7)}$$

$$= \sup_{\gamma<\lambda} \alpha^{\beta}\alpha^{\gamma} \qquad\qquad (\langle 2\rangle 2)$$

$$= \alpha^{\beta}\sup_{\gamma<\lambda} \alpha^{\gamma} \qquad\qquad \text{(Theorem 6.4.7)}$$

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

☐

**Theorem 6.5.24.** *For any ordinal numbers $\alpha$, $\beta$ and $\gamma$, we have*

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

PROOF:

⟨1⟩1.  LET:  $P[\gamma]$ be the property: For any ordinals $\alpha$ and $\beta$, we have $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\gamma}$

⟨1⟩2.  $P[0]$

   PROOF:

$$(\alpha^{\beta})^{0} = 1$$

$$= \alpha^{\beta 0}$$

⟨1⟩3.  $\forall \gamma \in \mathbf{On}.P[\gamma] \Rightarrow P[\gamma+1]$

   PROOF:

$$(\alpha^{\beta})^{\gamma+1} = (\alpha^{\beta})^{\gamma}\alpha^{\beta}$$

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

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

$$= \alpha^{\beta(\gamma+1)}$$

⟨1⟩4.  For any limit ordinal $\lambda$, if $\forall \gamma < \lambda.P[\gamma]$ then $P[\lambda]$.

   ⟨2⟩1.  LET:  $\lambda$ be a limit ordinal.

   ⟨2⟩2.  ASSUME:  $\forall \gamma < \lambda.P[\gamma]$

   ⟨2⟩3.  LET:  $\alpha$ and $\beta$ be any ordinals.

   ⟨2⟩4.  CASE:  $\alpha = 0$ and $\beta = 0$

Proof:

$$
\begin{aligned}
(0^\beta)^\lambda &= 1^\lambda \\
&= 1 \\
&= 0^0 \\
&= 0^{0\lambda}
\end{aligned}
$$

⟨2⟩5.  CASE:  $\alpha = 0$ and $\beta \neq 0$
   PROOF: $(0^\beta)^\lambda = 0^{\beta\lambda} = 0$.
⟨2⟩6.  CASE:  $\alpha = 1$
   PROOF: $(1^\beta)^\lambda = 1^{\beta\lambda} = 1$
⟨2⟩7.  CASE:  $\alpha > 1$
   PROOF:

$$
\begin{aligned}
(\alpha^\beta)^\lambda &= \sup_{\gamma < \lambda}(\alpha^\beta)^\gamma \\
&= \sup_{\gamma < \lambda}\alpha^{\beta\gamma} \\
&= \alpha^{\sup_{\gamma < \lambda}\beta\gamma} \\
&= \alpha^{\beta\lambda}
\end{aligned}
$$

∎

# Chapter 7

# Cardinal Numbers

## 7.1 Cardinal Numbers

**Definition 7.1.1** (Cardinality)**.** For any set $A$, the *cardinality* or *cardinal number* $|A|$ of $A$ is the least ordinal equinumerous with $A$.

Let **Card** be the class of all cardinal numbers.

**Proposition 7.1.2.** *For any sets $A$ and $B$, we have $A \approx B$ iff $|A| = |B|$.*

Proof: Easy. □

**Definition 7.1.3** (Addition)**.** Given cardinal numbers $\kappa$ and $\lambda$, we define $\kappa + \lambda$ to be $|A \cup B|$ where $A$ and $B$ are disjoint sets of cardinality $\kappa$ and $\lambda$ respectively.

We prove this is well-defined.

Proof:
⟨1⟩1. Assume: $A \approx A'$, $B \approx B'$, and $A \cap B = A' \cap B' = \emptyset$
⟨1⟩2. Pick bijections $f : A \approx A'$ and $g : B \approx B'$
⟨1⟩3. The function $A \cup B \to A' \cup B'$ that maps $a \in A$ to $f(a)$ and $b \in B$ to $g(b)$ is a bijection.
□

**Proposition 7.1.4.** *For any cardinal number $\kappa$, we have $\kappa + 0 = \kappa$.*

Proof: Let $A$ and $B$ be disjoint sets of cardinality $\kappa$ and 0. Then $B = \emptyset$ so $A \cup B = A$ and so $|A \cup B| = \kappa$. □

**Theorem 7.1.5** (Associative Law for Addition)**.** *For any cardinal numbers $\kappa$, $\lambda$, $\mu$ we have $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$.*

Proof: Since $A \cup (B \cup C) = (A \cup B) \cup C$. □

**Proposition 7.1.6.** *For any cardinal numbers $\kappa$ and $\lambda$ we have $\kappa + \lambda = \lambda + \kappa$.*

Proof: Since $A \cup B = B \cup A$. □

**Definition 7.1.7** (Multiplication)**.** For $\kappa$ and $\lambda$ cardinal numbers, we define $\kappa\lambda$ to be the cardinal number of $A \times B$, where $|A| = \kappa$ and $|B| = \lambda$.

We prove this is well-defined.

PROOF: If $f : A \approx A'$ and $g : B \approx B'$ then the function that maps $(a, b)$ to $(f(a), g(b))$ is a bijection $A \times B \approx A' \times B'$. $\square$

**Proposition 7.1.8.** *For any cardinal number $\kappa$ we have $\kappa \cdot 0 = 0$.*

PROOF: Since $A \times \emptyset = \emptyset$. $\square$

**Proposition 7.1.9.** *For any cardinal number $\kappa$ we have $\kappa \cdot 1 = \kappa$.*

PROOF: The function that maps $(a, e)$ to $a$ is a bijection $A \times \{e\} \approx A$. $\square$

**Theorem 7.1.10** (Distributive Law)**.** *For any cardinal numbers $\kappa$, $\lambda$ and $\mu$, we have $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$.*

PROOF: Since $A \times (B \cup C) = (A \times B) \cup (A \times C)$. $\square$

**Theorem 7.1.11** (Associative Law for Multiplication)**.** *For any cardinal numbers $\kappa$, $\lambda$ and $\mu$, we have $\kappa(\lambda\mu) = (\kappa\lambda)\mu$.*

PROOF: Since $A \times (B \times C) \approx (A \times B) \times C$. $\square$

**Theorem 7.1.12** (Commutative Law for Multiplication)**.** *For any cardinal numbers $\kappa$ and $\lambda$, we have $\kappa\lambda = \lambda\kappa$.*

PROOF: Since $A \times B \approx B \times A$. $\square$

**Theorem 7.1.13.** *For any cardinal numbers $\kappa$ and $\lambda$, if $\kappa\lambda = 0$ then $\kappa = 0$ or $\lambda = 0$.*

PROOF: if $A \times B = \emptyset$ then $A = \emptyset$ or $B = \emptyset$. $\square$

**Definition 7.1.14** (Exponentiation)**.** Given cardinal numbers $\kappa$ and $\lambda$, we define $\kappa^\lambda$ to be $|A^B|$, where $|A| = \kappa$ and $|B| = \lambda$.

We prove this is well-defined.

PROOF:If $f : A \approx A'$ and $g : B \approx B'$, then the function that maps $h : B \to A$ to $f \circ h \circ g^{-1}$ is a bijection $A^B \approx A'^{B'}$. $\square$

**Proposition 7.1.15.** *For any cardinal numbers $\kappa$, $\lambda$ and $\mu$,*

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

PROOF: The function that maps $f : A \times B \to C$ to $\lambda a \in A.\lambda b \in B.f(a, b)$ is a bijection $A^{B \times C} \approx (A^B)^C$. $\square$

**Proposition 7.1.16.** *For any cardinal numbers $\kappa$, $\lambda$ and $\mu$,*

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

PROOF: The function $f : A^C \times B^C \to (A \times B)^C$ with $f(g,h)(c) = (g(c), h(c))$ is a bijection. $\square$

**Proposition 7.1.17.** *For any cardinal numbers $\kappa$, $\lambda$ and $\mu$, we have*

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

PROOF: If $B \cap C = \emptyset$, then $f : A^B \times A^C \to A^{B \cup C}$ given by $f(g,h)(b) = g(b)$ and $f(g,h)(c) = h(c)$ is a bijection. $\square$

**Proposition 7.1.18.** *For any cardinal number $\kappa$, we have $\kappa^0 = 1$.*

PROOF: For any set $A$, we have $A^\emptyset = \{\emptyset\}$. $\square$

**Proposition 7.1.19.** *For any cardinal number $\kappa$, we have $\kappa^1 = \kappa$.*

PROOF: For any sets $A$ and $B$, if $B = \{b\}$ then the function $f : A \to A^B$ with $f(a)(b) = a$ is a bijection. $\square$

**Proposition 7.1.20.** *For any non-zero cardinal number $\kappa$ we have $0^\kappa = 0$.*

PROOF: If $A$ is nonempty then there is no function $A \to \emptyset$. $\square$

**Proposition 7.1.21.** *For any set $A$ we have $|\mathcal{P}A| = 2^{|A|}$.*

PROOF: The function $f : \mathcal{P}A \to 2^A$ where $f(X)(a) = 0$ if $a \notin X$ and $f(X)(a) = 1$ if $a \in X$. $\square$

**Corollary 7.1.21.1.** *For any cardinal number $\kappa$ we have $\kappa < 2^\kappa$.*

PROOF: By Cantor's Theorem. $\square$

## 7.2   Ordering on Cardinal Numbers

**Definition 7.2.1.** Given cardinal numbers $\kappa$ and $\lambda$, we have $\kappa \leq \lambda$ iff $A \preccurlyeq B$, where $|A| = \kappa$ and $|B| = \lambda$.

PROOF:
$\langle 1 \rangle 1.$ LET: $|A| = \kappa$ and $|B| = \lambda$
$\langle 1 \rangle 2.$ PICK bijections $f : A \approx \kappa$ and $g : B \approx \lambda$
$\langle 1 \rangle 3.$ If $\kappa \leq \lambda$ then $A \preccurlyeq B$
    PROOF: Let $i : \kappa \hookrightarrow \lambda$ be the inclusion. Then $g^{-1} \circ i \circ f$ is an injection $A \to B$.
$\langle 1 \rangle 4.$ If $A \preccurlyeq B$ then $\kappa \leq \lambda$
    $\langle 2 \rangle 1.$ ASSUME: $A \preccurlyeq B$
    $\langle 2 \rangle 2.$ PICK an injection $h : A \rightarrowtail B$
    $\langle 2 \rangle 3.$ $g(h(A)) \subseteq B$ is well-ordered by $\in$
    $\langle 2 \rangle 4.$ LET: $\gamma$ be the ordinal number of $(g(h(A)), \in)$
    $\langle 2 \rangle 5.$ $\gamma \leq \lambda$
        PROOF: Proposition 6.1.12.
    $\langle 2 \rangle 6.$ $\kappa \leq \gamma$

PROOF: By the leastness of $\kappa$, since $A$ is equinumerous with $\gamma$.
   $\langle 2 \rangle 7.$ $\kappa \leq \lambda$
☐

**Corollary 7.2.1.1.** *There is no largest cardinal number.*

**Proposition 7.2.2.** *For any cardinal numbers $\kappa$, $\lambda$, $\mu$, if $\kappa \leq \lambda$ then $\kappa + \mu \leq \lambda + \mu$.*

PROOF: If $f : A \to B$ is injective, and $A \cap C = B \cap C = \emptyset$, then the function $A \cup C \to B \cup C$ that maps $a$ to $f(a)$ and maps $c$ to $c$ is an injection. ☐

**Proposition 7.2.3.** *For any cardinal numbers $\kappa$, $\lambda$, $\mu$, if $\kappa \leq \lambda$ then $\kappa\mu \leq \lambda\mu$.*

PROOF: If $f : A \to B$ is injective, then the function $A \times C \to B \times C$ that maps $(a, c)$ to $(f(a), c)$ is injective. ☐

**Proposition 7.2.4.** *For any cardinal numbers $\kappa$, $\lambda$, $\mu$, if $\kappa \leq \lambda$ then $\kappa^\mu \leq \lambda^\mu$.*

PROOF: Given an injection $f : A \to B$, the function that maps $A^C \to B^C$ that maps $g$ to $f \circ g$ is an injection. ☐

**Proposition 7.2.5.** *For any cardinal numbers $\kappa$, $\lambda$, $\mu$, if $\kappa \leq \lambda$ and $\mu$ and $\kappa$ are not both 0, then $\mu^\kappa \leq \mu^\lambda$.*

PROOF:
$\langle 1 \rangle 1.$ LET: $A$, $B$ and $C$ be sets with $A$ and $C$ not both empty.
$\langle 1 \rangle 2.$ LET: $f : A \to B$ be an injection.
    PROVE:  $C^A \preccurlyeq C^B$
$\langle 1 \rangle 3.$ CASE: $C = \emptyset$
  PROOF: Then $A \neq \emptyset$ so $C^A = \emptyset \preccurlyeq C^B$.
$\langle 1 \rangle 4.$ CASE: $C \neq \emptyset$
   $\langle 2 \rangle 1.$ PICK $c \in C$
   $\langle 2 \rangle 2.$ LET: $g : C^A \to C^B$ be the function $g(h)(f(a)) = h(a)$, $g(h)(b) = c$ if
         $b \notin f(A)$
   $\langle 2 \rangle 3.$ $g$ is an injection.
☐

**Proposition 7.2.6.** *Let $\mathcal{A}$ be a set such that $\forall X \in \mathcal{A}.|X| \leq \kappa$. Then*

$$\left| \bigcup \mathcal{A} \right| \leq |\mathcal{A}|\kappa \ .$$

PROOF:
$\langle 1 \rangle 1.$ For $X \in \mathcal{A}$, choose a surjection $f_X : \kappa \to X$.
$\langle 1 \rangle 2.$ Define $g : \mathcal{A} \times \kappa \to \bigcup \mathcal{A}$ by $g(X, \alpha) = f_X(\alpha)$
$\langle 1 \rangle 3.$ $g$ is surjective.
☐

**Lemma 7.2.7.** *The union of a set of cardinal numbers is a cardinal number.*

PROOF:

⟨1⟩1. LET: $A$ be a set of cardinal numbers.
    PROVE: $\bigcup A$ is the smallest ordinal equinumerous with $\bigcup A$
⟨1⟩2. LET: $\alpha < \bigcup A$
    PROVE: $\alpha \not\approx \bigcup A$
⟨1⟩3. PICK $\kappa \in A$ such that $\alpha < \kappa$
⟨1⟩4. $\alpha \prec \kappa$
⟨1⟩5. $\alpha \prec \bigcup A$
∎

# Chapter 8

# Natural Numbers

## 8.1 Inductive Sets

**Definition 8.1.1** (Inductive). A set $I$ is *inductive* iff $0 \in I$ and $\forall x \in I.x^+ \in I$.

**Definition 8.1.2** (Natural Number). A *natural number* is a set that belongs to every inductive set.

**Theorem 8.1.3.** *The class $\mathbb{N}$ of natural numbers is a set.*

PROOF:
$\langle 1 \rangle 1$. PICK an inductive set $I$.
  PROOF: Axiom of Infinity.
$\langle 1 \rangle 2$. $\mathbb{N} \subseteq I$
☐

**Theorem 8.1.4.** $\mathbb{N}$ *is inductive, and is a subset of every other inductive set.*

PROOF:
$\langle 1 \rangle 1$. $\mathbb{N}$ is inductive.
  $\langle 2 \rangle 1$. $0 \in \mathbb{N}$
    PROOF: Since 0 is a member of every inductive set.
  $\langle 2 \rangle 2$. $\forall n \in \mathbb{N}.n^+ \in \mathbb{N}$
    $\langle 3 \rangle 1$. LET: $n \in \mathbb{N}$
    $\langle 3 \rangle 2$. LET: $I$ be any inductive set.
        PROVE: $n^+ \in I$
    $\langle 3 \rangle 3$. $n \in I$
      PROOF: $\langle 3 \rangle 1$, $\langle 3 \rangle 2$
    $\langle 3 \rangle 4$. $n^+ \in I$
      PROOF: $\langle 3 \rangle 2$, $\langle 3 \rangle 3$
$\langle 1 \rangle 2$. $\mathbb{N}$ is a subset of every inductive set.
  PROOF: Immediate from definitions.
☐

**Corollary 8.1.4.1** (Induction Principle for $\mathbb{N}$). *Any inductive subset of $\mathbb{N}$ coincides with $\mathbb{N}$.*

**Theorem 8.1.5.** *Every natural number except 0 is the successor of some natural number.*

PROOF: Trivially by induction. □

**Proposition 8.1.6.** *Every natural number is an ordinal.*

PROOF: By induction. □

**Proposition 8.1.7.** $\mathbb{N}$ *is a transitive set.*

PROOF:
⟨1⟩1. $0 \subseteq \mathbb{N}$
⟨1⟩2. $\forall n \in \mathbb{N}.n \subseteq \mathbb{N} \Rightarrow n^+ \subseteq \mathbb{N}$
⟨1⟩3. $\forall n \in \mathbb{N}.n \subseteq \mathbb{N}$
   PROOF: From ⟨1⟩1 and ⟨1⟩2 by induction.
□

**Corollary 8.1.7.1.** $\mathbb{N}$ *is an ordinal.*

**Definition 8.1.8.** We define $\omega = \mathbb{N}$.

**Proposition 8.1.9** (Dependent Choice). *Let $A$ be a nonempty set and $R$ a relation on $A$ such that $\forall x \in A.\exists y \in A.(y, x) \in R$. Then there exists a function $f : \mathbb{N} \to A$ such that $\forall n \in \mathbb{N}.(f(n + 1), f(n)) \in R$.*

PROOF:
⟨1⟩1. PICK a choice function $F$ for $A$.
⟨1⟩2. PICK $a \in A$
⟨1⟩3. Define $f : \mathbb{N} \to A$ by $f(0) = a$ and $f(n + 1) = F(\{y \in A \mid (y, f(n)) \in R\})$.
□

**Theorem Schema 8.1.10.** *For any classes $\mathbf{A}$ and $\mathbf{R}$, the following is a theorem:*

*Assume $\mathbf{R}$ is a relation on $\mathbf{A}$ and, for all $a \in \mathbf{A}$, the class $\{x \in \mathbf{A} \mid x\mathbf{R}a\}$ is a set. Then $\mathbf{R}$ is well founded if and only if there does not exist a function $f : \mathbb{N} \to \mathbf{A}$ such that $\forall n \in \mathbb{N}.f(n + 1)\mathbf{R}f(n)$.*

PROOF:
⟨1⟩1. If there exists a function $f : \mathbb{N} \to \mathbf{A}$ such that $\forall n \in \mathbb{N}.f(n+1)\mathbf{R}f(n)$ then $\mathbf{R}$ is not well founded.
   PROOF: $f(\mathbb{N})$ is a nonempty subset of $\mathbf{A}$ with no $\mathbf{R}$-minimal element.
⟨1⟩2. If $\mathbf{R}$ is not well founded then there exists a function $f : \mathbb{N} \to \mathbf{A}$ such that $\forall n \in \mathbb{N}.f(n + 1)\mathbf{R}f(n)$.
   ⟨2⟩1. ASSUME: $\mathbf{R}$ is not well founded.
   ⟨2⟩2. PICK a nonempty subset $B \subseteq \mathbf{A}$ that has no $\mathbf{R}$-minimal element.
   ⟨2⟩3. $\forall x \in B.\exists y \in B.y\mathbf{R}x$

$\langle 2 \rangle 4$. Choose a function $g : B \to B$ such that $\forall x \in B.g(x)\mathbf{R}x$
$\langle 2 \rangle 5$. PICK $b \in B$
$\langle 2 \rangle 6$. Define $f : \mathbb{N} \to \mathbf{A}$ recursively by $f(0) = b$ and $\forall n \in \mathbb{N}.f(n+1) = g(f(n))$
$\langle 2 \rangle 7$. $\forall n \in \mathbb{N}.f(n + 1)\mathbf{R}f(n)$

$\square$

## 8.2 Cardinality

**Definition 8.2.1** (Finite)**.** A set is *finite* iff it is equinumerous to some natural number; otherwise it is *infinite*.

**Theorem 8.2.2** (Pigeonhole Principle)**.** *No natural number is equinumerous to a proper subset of itself.*

PROOF:
$\langle 1 \rangle 1$. LET: $P(n)$ be the property: any one-to-one function $n \to n$ is surjective.
$\langle 1 \rangle 2$. $P(0)$
   PROOF: The only function $0 \to 0$ is injective.
$\langle 1 \rangle 3$. For every natural number $n$, if $P(n)$ then $P(n + 1)$.
  $\langle 2 \rangle 1$. ASSUME: $P(n)$
  $\langle 2 \rangle 2$. LET: $f$ be a one-to-one function $n + 1 \to n + 1$
  $\langle 2 \rangle 3$. $f \restriction n$ is a one-to-one function $n \to n + 1$
  $\langle 2 \rangle 4$. CASE: $n \notin ran f$
    $\langle 3 \rangle 1$. $f \restriction n : n \to n$
    $\langle 3 \rangle 2$. $\mathrm{ran}(f \restriction n) = n$
    $\langle 3 \rangle 3$. $f(n) = n$
      PROOF: $\langle 2 \rangle 1$.
    $\langle 3 \rangle 4$. $\mathrm{ran}\, f = n + 1$
  $\langle 2 \rangle 5$. CASE: $n \in \mathrm{ran}\, f$
    $\langle 3 \rangle 1$. PICK $p \in n$ such that $f(p) = n$
    $\langle 3 \rangle 2$. LET: $\hat{f} : n \to n$ be the function
$$\hat{f}(p) = f(n)$$
$$\hat{f}(x) = f(x) \qquad\qquad (x \neq p)$$
    $\langle 3 \rangle 3$. $\hat{f}$ is one-to-one
    $\langle 3 \rangle 4$. $\mathrm{ran}\, \hat{f} = n$
      PROOF: $\langle 2 \rangle 1$
    $\langle 3 \rangle 5$. $\mathrm{ran}\, f = n + 1$
$\langle 1 \rangle 4$. For every natural number $n$, $P(n)$.

$\square$

**Corollary 8.2.2.1.** *No finite set is equinumerous to a proper subset of itself.*

**Corollary 8.2.2.2.** *Every natural number is a cardinal number.*

PROOF: For any natural number $n$, we have that $n$ is the least ordinal such that $n \approx n$. $\square$

**Corollary 8.2.2.3.** $\mathbb{N}$ *is a cardinal number.*

**Corollary 8.2.2.4.** $\mathbb{N}$ *is infinite.*

PROOF: The function that maps $n$ to $n+1$ is a bijection between $\mathbb{N}$ and $\mathbb{N} - \{0\}$. $\square$

**Corollary 8.2.2.5.** *If $C$ is a proper subset of a natural number $n$, then there exists $m < n$ such that $C \approx m$.*

PROOF: By Proposition 6.1.12. $\square$

**Corollary 8.2.2.6.** *Any subset of a finite set is finite.*

**Proposition 8.2.3.** *For any natural numbers $m$ and $n$ we have $m+n$ (cardinal addition) is a natural number.*

PROOF: Induction on $n$. $\square$

**Corollary 8.2.3.1.** *The union of two finite sets is finite.*

**Corollary 8.2.3.2.** *The union of a finite set of finite sets is finite.*

PROOF: By induction on the number of elements. $\square$

**Proposition 8.2.4.** *For natural numbers $m$ and $n$, the cardinal sum $m + n$ is equal to the ordinal sum $m + n$.*

PROOF: Induction on $n$. $\square$

**Proposition 8.2.5.** *For any natural numbers $m$ and $n$, we have $mn$ (cardinal multiplication) is a natural number.*

**Corollary 8.2.5.1.** *If $A$ and $B$ are finite sets then $A \times B$ is finite.*

**Proposition 8.2.6.** *For natural numbers $m$ and $n$, the cardinal product $mn$ is equal to the ordinal product $mn$.*

PROOF: Induction on $n$. $\square$

**Proposition 8.2.7.** *For any natural numbers $m$ and $n$ we have $m^n$ (cardinal exponentiation) is a natural number.*

PROOF: Induction on $n$.

**Corollary 8.2.7.1.** *If $A$ and $B$ are finite sets then $A^B$ are finite.*

**Proposition 8.2.8.** *For natural numbers $m$ and $n$, the cardinal exponentiation $m^n$ and the ordinal exponentiation $m^n$ agree.*

PROOF: Induction on $n$. $\square$

**Proposition 8.2.9.** $\mathbb{N}^2 \approx \mathbb{N}$

PROOF: The function $J : \mathbb{N}^2 \to \mathbb{N}$ defined by $J(m, n) = ((m + n)^2 + 3m + n)/2$ is a bijection. $\square$

**Proposition 8.2.10.** *For any infinite cardinal $\kappa$ we have $\aleph_0 \leq \kappa$.*

PROOF:
$\langle 1 \rangle 1$. LET: $A$ be an infinite set.
  PROVE: $\mathbb{N} \preccurlyeq A$
$\langle 1 \rangle 2$. PICK a choice function $F$ for $A$.
$\langle 1 \rangle 3$. Define $h : \mathbb{N} \to \{ X \in \mathcal{P}A \mid X \text{ is finite} \}$ by
$$h(0) = \emptyset$$
$$h(n + 1) = h(n) \cup \{ F(A - \{ h(m) \mid m < n \}) \}$$
$\langle 1 \rangle 4$. Define $g : \mathbb{N} \to A$ by $g(n) = F(A - \{ h(m) \mid m < n \})$
$\langle 1 \rangle 5$. $g$ is injective.
 PROOF: If $m < n$ then $g(m) \neq g(n)$.
$\square$

**Theorem Schema 8.2.11** (König's Lemma)**.** *For any classes $\mathbf{A}$ and $\mathbf{R}$, the following is a theorem:*
 *Assume $\mathbf{R}$ is a well founded relation on $\mathbf{A}$ such that, for all $y \in \mathbf{A}$, the class $\{ x \in \mathbf{A} \mid x\mathbf{R}y \}$ is a finite set. Let $\mathbf{R}^t$ be the transitive closure of $\mathbf{R}$. Then, for all $y \in \mathbf{A}$, the class $\{ x \in \mathbf{A} \mid x\mathbf{R}^t y \}$ is a finite set.*

PROOF:
$\langle 1 \rangle 1$. LET: $y \in \mathbf{A}$
$\langle 1 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall x\mathbf{R}y . \{ z \in \mathbf{A} \mid z\mathbf{R}^t x \}$ is a
     finite set.
$\langle 1 \rangle 3$. $\{ x \mid x\mathbf{R}^t y \} = \bigcup_{x\mathbf{R}y} (\{ x \} \cup \{ z \mid z\mathbf{R}^t x \})$
$\langle 1 \rangle 4$. $\{ x \mid x\mathbf{R}^t y \}$ is finite.
 PROOF: Corollary 8.2.3.2.
$\square$

## 8.3 Countable Sets

**Definition 8.3.1** (Countable)**.** A set $A$ is *countable* iff $|A| \leq \aleph_0$.

**Theorem 8.3.2.** *The union of a countable set of countable sets is countable.*

PROOF: Proposition 7.2.6. $\square$

## 8.4 Arithmetic

**Definition 8.4.1** (Even)**.** A natural number $n$ is *even* iff there exists $m \in \mathbb{N}$ such that $n = 2m$.

**Definition 8.4.2** (Odd)**.** A natural number $n$ is *odd* iff there exists $p \in \mathbb{N}$ such that $n = 2p + 1$.

**Proposition 8.4.3.** *Every natural number is either even or odd.*

PROOF:

$\langle 1 \rangle 1$.  0 is even.
   PROOF: $0 = 2 \times 0$.
$\langle 1 \rangle 2$.  For any natural number $n$, if $n$ is either even or odd then $n^+$ is either even
      or odd.
   PROOF:
   $\langle 2 \rangle 1$.  LET: $n \in \mathbb{N}$
   $\langle 2 \rangle 2$.  If $n$ is even then $n^+$ is odd.
      PROOF: If $n = 2p$ then $n^+ = 2p + 1$.
   $\langle 2 \rangle 3$.  If $n$ is odd then $n^+$ is even.
      PROOF: If $n = 2p + 1$ then $n^+ = 2(p + 1)$.
⬚

**Proposition 8.4.4.** *No natural number is both even and odd.*

PROOF:

$\langle 1 \rangle 1$.  0 is not odd.
   PROOF: For any $p$ we have $2p + 1 = (2p)^+ \neq 0$.
$\langle 1 \rangle 2$.  For any natural number $n$, if $n$ is not both even and odd, then $n^+$ is not
      both even and odd.
   $\langle 2 \rangle 1$.  LET: $n$ be a natural number.
   $\langle 2 \rangle 2$.  If $n^+$ is even then $n$ is odd.
      $\langle 3 \rangle 1$.  ASSUME: $n^+$ is even.
      $\langle 3 \rangle 2$.  PICK $p$ such that $n^+ = 2p$
      $\langle 3 \rangle 3$.  $p \neq 0$
         PROOF: Since $n^+ \neq 0$.
      $\langle 3 \rangle 4$.  PICK $q$ such that $p = q^+$
         PROOF: Theorem 8.1.5.
      $\langle 3 \rangle 5$.  $n^+ = 2q + 2$
         PROOF: $\langle 3 \rangle 2$, $\langle 3 \rangle 4$.
      $\langle 3 \rangle 6$.  $n = 2q + 1$
         PROOF: Proposition 6.2.7, $\langle 3 \rangle 5$
      $\langle 3 \rangle 7$.  $n$ is odd.
   $\langle 2 \rangle 3$.  If $n^+$ is odd then $n$ is even.
      $\langle 3 \rangle 1$.  ASSUME: $n^+$ is odd.
      $\langle 3 \rangle 2$.  PICK $p$ such that $n^+ = 2p + 1$
      $\langle 3 \rangle 3$.  $n = 2p$
         PROOF: Proposition 6.2.7, $\langle 3 \rangle 2$
      $\langle 3 \rangle 4$.  $n$ is even.
⬚

**Proposition 8.4.5.** *Let $m$, $n$, $p$, $q$ be natural numbres. Assume $m + n = p + q$.*
*Then $m < p$ if and only if $q < n$.*

PROOF:

$\langle 1 \rangle 1$.  If $m < p$ then $q < n$.

PROOF: If $m < p$ and $n \leq q$ then $m + n < p + q$.
⟨1⟩2. If $q < n$ then $m < p$.
   PROOF: Similar.
□

**Proposition 8.4.6.** *Let $m$, $n$, $p$ and $q$ be natural numbers. Assume $n < m$ and $q < p$. Then*
$$mq + np < mp + nq \ .$$

PROOF:
⟨1⟩1. PICK positive natural numbers $a$ and $b$ such that $m = n+a$ and $p = q+b$.
⟨1⟩2. $mp + nq > mq + np$
   PROOF:
$$mp + nq = (n + a)(q + b) + nq$$
$$= 2nq + nb + aq + ab$$
$$mq + np = (n + a)q + n(q + b)$$
$$= 2nq + aq + nb$$
$$\therefore mp + nq = mq + np + ab$$
$$> mq + np$$

□

## 8.5   Sequences

**Definition 8.5.1** (Sequence)**.** Let $A$ be a set. A *finite sequence* in $A$ is a function $a : n \to A$ for some natural number $n$; we write it as $(a(0), a(1), \ldots, a(n-1))$. An *(infinite) sequence* in $A$ is a function $\mathbb{N} \to A$.
   We write $A^*$ for the set of all finite sequences in $A$.

**Proposition 8.5.2.** *If $A$ is countable then $A^*$ is countable.*

PROOF: For any $n$, the set $A^n$ is countable, and $A^*$ is equinumerous with $\bigcup_n A^n$.
□

## 8.6   Transitive Closure of a Set

**Proposition 8.6.1.** *For any set $A$, there exists a unique transitive set $C$ such that:*

- $A \subseteq C$

- *For any transitive set $X$, if $A \subseteq X$ then $C \subseteq X$*

PROOF:
⟨1⟩1. Define a function $F : \mathbb{N} \to \mathbf{V}$ by
$$F(0) = A$$
$$F(n + 1) = A \cup \bigcup(F(0) \cup \cdots \cup F(n))$$

$\langle 1 \rangle 2$. For all $n \in \mathbb{N}$ and $a \in F(n)$ we have $a \subseteq F(n+1)$
    PROOF: $a \in F(0) \cup \cdots \cup F(n)$ so $a \subseteq \bigcup(F(0) \cup \cdots \cup F(n)) \subseteq F(n+1)$.
$\langle 1 \rangle 3$. LET: $C = \bigcup_{n \in \mathbb{N}} F(n)$
$\langle 1 \rangle 4$. $C$ is transitive.
    $\langle 2 \rangle 1$. LET: $x \in y \in C$
    $\langle 2 \rangle 2$. PICK $n \in \mathbb{N}$ such that $y \in F(n)$
    $\langle 2 \rangle 3$. $y \subseteq F(n+1)$
        PROOF: $\langle 1 \rangle 2$
    $\langle 2 \rangle 4$. $x \in F(n+1)$
    $\langle 2 \rangle 5$. $x \in C$
$\langle 1 \rangle 5$. $A \subseteq C$
    PROOF: Since $F(0) = A$.
$\langle 1 \rangle 6$. For any transitive set $X$, if $A \subseteq X$ then $C \subseteq X$
    $\langle 2 \rangle 1$. LET: $X$ be a transitive set
    $\langle 2 \rangle 2$. ASSUME: $A \subseteq X$
    $\langle 2 \rangle 3$. For all $n \in \mathbb{N}$ we have $F(n) \subseteq X$.
        $\langle 3 \rangle 1$. $F(0) \subseteq X$
            PROOF: $\langle 2 \rangle 2$
        $\langle 3 \rangle 2$. For all $n \in \mathbb{N}$, if $F(n) \subseteq X$, then $F(n+1) \subseteq X$.
            $\langle 4 \rangle 1$. LET: $n \in \mathbb{N}$
            $\langle 4 \rangle 2$. ASSUME: $\forall m < n . F(m) \subseteq X$
            $\langle 4 \rangle 3$. $F(0) \cup \cdots \cup F(n) \subseteq X$
            $\langle 4 \rangle 4$. $\bigcup(F(0) \cup \cdots \cup F(n)) \subseteq X$
                PROOF: Since $X$ is transitive.
            $\langle 4 \rangle 5$. $F(n+1) \subseteq X$
    $\langle 2 \rangle 4$. $C \subseteq X$
$\langle 1 \rangle 7$. Let $D$ be a transitive set such that $A \subseteq D$ and, for any transitive set $X$,
        if $A \subseteq X$ then $D \subseteq X$. Then $D = C$.
    PROOF: We have $C \subseteq D$ and $D \subseteq C$.
$\Box$


## 8.7   The Veblen Fixed Point Theorem

**Theorem Schema 8.7.1** (Veblen Fixed Point Theorem)**.** *For any class* $\mathbf{T}$*, the following is a theorem:*

*Assume* $\mathbf{T}$ *is a normal ordinal operation. For every ordinal* $\beta$*, there exists* $\gamma \geq \beta$ *such that* $\mathbf{T}(\gamma) = \gamma$.

PROOF:
$\langle 1 \rangle 1$. LET: $\beta$ be an ordinal.
$\langle 1 \rangle 2$. ASSUME: w.l.o.g. $\beta < \mathbf{T}(\beta)$
    PROOF: We have $\beta \leq \mathbf{T}(\beta)$ by Proposition 6.4.5, and if $\beta = \mathbf{T}(\beta)$ we take
    $\gamma := \beta$.

$\langle 1 \rangle 3$. Define $f : \mathbb{N} \to \mathbf{On}$ by recursion thus:

$$f(0) = \beta$$
$$f(n^+) = \mathbf{T}(f(n))$$

$\langle 1 \rangle 4$.  LET:  $\gamma = \sup_{n \in \mathbb{N}} f(n)$

$\langle 1 \rangle 5$.  $\beta \leq \gamma$

  PROOF: Since $\beta = f(0)$.

$\langle 1 \rangle 6$.  $\mathbf{T}(\gamma) = \gamma$

  $\langle 2 \rangle 1$.  $\mathbf{T}(\gamma) \leq \gamma$

    PROOF:

$$
\begin{aligned}
\mathbf{T}(\gamma) &= \sup_{n \in \mathbb{N}} \mathbf{T}(f(n)) && \text{(Theorem 6.4.7)} \\
&= \sup_{n \in \mathbb{N}} f(n^+) && (\langle 1 \rangle 3) \\
&\leq \sup_{n \in \mathbb{N}} f(n) \\
&= \gamma
\end{aligned}
$$

  $\langle 2 \rangle 2$.  $\gamma \leq \mathbf{T}(\gamma)$

    PROOF:Proposition 6.4.5.

□

**Definition 8.7.2** (Derived Operation)**.** Let $\mathbf{T}$ be a normal ordinal operation. The *derived* operation $\mathbf{T}' : \mathbf{On} \to \mathbf{V}$ is the unique order isomorphism between $\mathbf{On}$ and the fixed points of $\mathbf{T}$.

**Proposition Schema 8.7.3.** *For any class* $\mathbf{T}$*, the following is a theorem:*
   *If* $\mathbf{T}$ *is a normal ordinal operation, then the derived operation is normal.*

PROOF:

$\langle 1 \rangle 1$. For any set $S$ of fixed points of $\mathbf{T}$, we have $\bigcup S$ is a fixed point of $\mathbf{T}$

  $\langle 2 \rangle 1$.  LET:  $S$ be a set of fixed points of $\mathbf{T}$.

  $\langle 2 \rangle 2$.  $\mathbf{T}(\sup S) = \sup S$

    PROOF:

$$
\begin{aligned}
\mathbf{T}(\sup S) &= \sup_{\alpha \in S} \mathbf{T}(\alpha) && \text{(Theorem 6.4.7)} \\
&= \sup_{\alpha \in S} \alpha && (\langle 2 \rangle 1) \\
&= \sup S
\end{aligned}
$$

$\langle 1 \rangle 2$.  Q.E.D.

  PROOF: Proposition 6.4.8.

□

## 8.8   Cantor Normal Form

**Theorem 8.8.1.** *For any ordinal* $\alpha$*, there exist a unique sequence of nonzero natural numbers* $(n_1, \dots, n_k)$ *and sequence of ordinals* $(\gamma_1, \dots, \gamma_k)$ *such that*

$$\gamma_k < \gamma_{k-1} < \cdots < \gamma_1$$

*and*

$$\alpha = \omega^{\gamma_1} n_1 + \omega^{\gamma_2} n_2 + \cdots + \omega^{\gamma_k} n_k \ .$$

PROOF:

⟨1⟩1. For any ordinal $\alpha$, there exist a sequence of nonzero natural numbers $(n_1, \ldots, n_k)$ and sequence of ordinals $(\gamma_1, \ldots, \gamma_k)$ such that

$$\gamma_k < \gamma_{k-1} < \cdots < \gamma_1$$

and

$$\alpha = \omega^{\gamma_1} n_1 + \omega^{\gamma_2} n_2 + \cdots + \omega^{\gamma_k} n_k \ .$$

⟨2⟩1. LET: $\alpha$ be an ordinal

⟨2⟩2. ASSUME: as an induction hypothesis that, for all $\beta < \alpha$, the theorem holds.

⟨2⟩3. ASSUME: w.l.o.g. $\alpha \neq 0$

⟨2⟩4. LET: $\gamma_1, n_1, \rho_1$ be the unique ordinals such that $0 \neq n_1 < \omega$, $\rho_1 < \omega^{\gamma_1}$, and $\alpha = \omega^{\gamma_1} n_1 + \rho_1$

⟨2⟩5. LET: $(\gamma_2, \ldots, \gamma_k)$ and $(n_2, \ldots, n_k)$ be sequences such that $\gamma_k < \gamma_{k-1} < \cdots < \gamma_2$ and $\rho_1 = \omega^{\gamma_2} n_2 + \cdots + \omega^{\gamma_k} n_k$

⟨2⟩6. $\gamma_2 < \gamma_1$

PROOF: Since $\omega^{\gamma_2} \leq \rho_1 < \omega^{\gamma_1}$

⟨1⟩2. If

$$\gamma_k < \gamma_{k-1} < \cdots < \gamma_1$$
$$\gamma_k' < \gamma_{k-1}' < \cdots < \gamma_1'$$

and

$$\omega^{\gamma_1} n_1 + \omega^{\gamma_2} n_2 + \cdots + \omega^{\gamma_k} n_k = \omega^{\gamma_1'} n_1' + \omega^{\gamma_2'} n_2' + \cdots + \omega^{\gamma_k'} n_k'$$

then $\gamma_i = \gamma_i'$ for all $i$ and $n_i = n_i'$ for all $i$

PROOF: Prove by induction on $i$ using the Logarithm Theorem.

☐

**Definition 8.8.2** (Cantor Normal Form)**.** For any ordinal $\alpha$, the *Cantor normal form* of $\alpha$ is the expression $\alpha = \omega^{\gamma_1} n_1 + \cdots + \omega^{\gamma_k} n_k$ such that $n_1, \ldots, n_k$ are nonzero natural numbers and $\gamma_k < \gamma_{k-1} < \cdots < \gamma_1$.

# Chapter 9

# Infinite Cardinals

## 9.1 Alephs

**Definition 9.1.1** (Aleph)**.** Let $\aleph$ be the unique order isomorphism between **On** and the class of infinite cardinals.

**Proposition 9.1.2.** *The operation $\aleph$ is normal.*

PROOF: Proposition 6.4.8 and Lemma 7.2.7. $\square$

**Definition 9.1.3** (Continuum Hypothesis)**.** The *continuum hypothesis* is the statement that $\aleph_1 = 2^{\aleph_0}$.

**Definition 9.1.4** (Generalised Continuum Hypothesis)**.** The *generalised continuum hypothesis* is the statement that, for all $\alpha$, $\aleph_{\alpha^+} = 2^{\aleph_\alpha}$.

## 9.2 Beths

**Definition 9.2.1** (Beth)**.** Define the operation $\beth \colon \mathbf{On} \to \mathbf{Card}$ by transfinite recursion as follows:

$$\beth_0 := \aleph_0$$
$$\beth_{\alpha^+} := 2^{\beth_\alpha}$$
$$\beth_\lambda := \bigcup_{\alpha < \lambda} \beth_\alpha \qquad\qquad (\lambda \text{ a limit ordinal})$$

**Proposition 9.2.2.** $\beth$ *is a normal operation.*

PROOF: It is continuous by definition, and $\beth_\alpha < \beth_{\alpha^+}$ by Cantor's Theorem. $\square$

**Proposition 9.2.3.** *The continuum hypothesis is equivalent to the statement* $\beth_1 = \aleph_1$.

  *The generalised continuum hypothesis is equivalent to the statement* $\beth = \alpha$.

PROOF: Immediate from definitions. $\square$

# Chapter 10

# The Cumulative Hierarchy

**Definition 10.0.1** (Cumulative Hierarchy)**.** Define the function $V : \mathbf{On} \to \mathbf{V}$
by transfinite recursion thus:

$$V_\alpha = \bigcup_{\beta < \alpha} \mathcal{P} V_\beta$$

**Proposition 10.0.2.** *For all* $\alpha \in \mathbf{On}$, $V_\alpha$ *is a transitive set.*

PROOF:
$\langle 1 \rangle 1.$ LET: $\alpha \in \mathbf{On}$
$\langle 1 \rangle 2.$ ASSUME: as transfinite induction hypothesis $\forall \beta < \alpha. V_\beta$ is a transitive set.
$\langle 1 \rangle 3.$ For all $\beta < \alpha$, $\mathcal{P} V_\beta$ is a transitive set.
    PROOF: Proposition 1.5.4.
$\langle 1 \rangle 4.$ $V_\alpha$ is a transitive set.
    PROOF: Proposition 1.5.3.
□

**Proposition 10.0.3.** *For any ordinals* $\alpha$ *and* $\beta$, *if* $\beta < \alpha$ *then* $V_\beta \subseteq V_\alpha$.

PROOF: Since $V_\beta \in \mathcal{P} V_\beta \subseteq V_\alpha$ and $V_\alpha$ is a transitive set. □

**Theorem 10.0.4.**

1. $V_0 = \emptyset$

2. $\forall \alpha \in \mathbf{On}. V_{\alpha^+} = \mathcal{P} V_\alpha$

3. *For any limit ordinal* $\lambda$, $V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha$.

PROOF:
$\langle 1 \rangle 1.$ $V_0 = \emptyset$
    PROOF: Immediate from definition.
$\langle 1 \rangle 2.$ $\forall \alpha \in \mathbf{On}. V_{\alpha^+} = \mathcal{P} V_\alpha$
    PROOF:

87

$\langle 2 \rangle 1$. LET: $\alpha \in \mathbf{On}$

$\langle 2 \rangle 2$. For all $\beta < \alpha$ we have $\mathcal{P}V_\beta \subseteq \mathcal{P}V_\alpha$

   PROOF: Propositions 1.4.7 and 10.0.3.

$\langle 2 \rangle 3$. $V_{\alpha^+} = \mathcal{P}V_\alpha$

$$
\begin{aligned}
V_{\alpha^+} &= \bigcup_{\beta < \alpha^+} \mathcal{P}V_\beta \\
&= \bigcup_{\beta < \alpha} \mathcal{P}V_\beta \cup \mathcal{P}V_\alpha \\
&\quad \mathcal{P}V_\alpha
\end{aligned}
$$

$\square$

$\langle 1 \rangle 3$. For any limit ordinal $\lambda$, $V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha$

   PROOF:

$\langle 2 \rangle 1$. $V_\lambda \subseteq \bigcup_{\alpha < \lambda} V_\alpha$

   PROOF:

$$
\begin{aligned}
V_\lambda &= \bigcup_{\alpha < \lambda} \mathcal{P}V_\alpha \\
&= \bigcup_{\alpha < \lambda} V_{\alpha^+} \qquad\qquad (\langle 1 \rangle 2) \\
&\subseteq \bigcup_{\alpha < \lambda} V_\alpha
\end{aligned}
$$

$\langle 2 \rangle 2$. $\bigcup_{\alpha < \lambda} V_\alpha \subseteq V_\lambda$

   PROOF: Proposition 10.0.3.

$\square$

**Proposition 10.0.5.** *For every set $A$, there exists an ordinal $\alpha$ such that $A \in V_\alpha$.*

PROOF:

$\langle 1 \rangle 1$. Let us say a set $A$ is *grounded* iff there exists an ordinal $\alpha$ such that $A \in V_\alpha$.

$\langle 1 \rangle 2$. For any set $A$, if every element of $A$ is grounded, then $A$ is grounded.

   $\langle 2 \rangle 1$. LET: $A$ be a set.

   $\langle 2 \rangle 2$. $S = \{\alpha \mid \exists a \in A.\alpha \text{ is the least ordinal such that } a \in V_\alpha\}$

      PROOF: $S$ is a set by an Axiom of Replacement.

   $\langle 2 \rangle 3$. LET: $\beta = \sup S$

   $\langle 2 \rangle 4$. $A \subseteq V_\beta$

      $\langle 3 \rangle 1$. LET: $a \in A$

      $\langle 3 \rangle 2$. LET: $\alpha$ be the least ordinal such that $a \in V_\beta$

      $\langle 3 \rangle 3$. $\alpha \in S$

      $\langle 3 \rangle 4$. $\alpha \leq \beta$

      $\langle 3 \rangle 5$. $a \in V_\beta$

   $\langle 2 \rangle 5$. $A \in V_{\beta^+}$

$\langle 1 \rangle 3$. ASSUME: for a contradiction there exists an ungrounded set.

$\langle 1 \rangle 4$. PICK a transitive set $B$ that has an ungrounded member.

   PROOF: Pick a transitive set $c$, and take $B$ to be the transitive closure of $\{c\}$.

$\langle 1 \rangle 5$. LET:  $A = \{x \in B \mid x \text{ is ungrounded}\}$
$\langle 1 \rangle 6$. PICK $m \in A$ such that $m \cap A = \emptyset$
  PROOF: Axiom of Regularity.
$\langle 1 \rangle 7$. Every member of $m$ is grounded.
  $\langle 2 \rangle 1$. ASSUME: for a contradiction $x \in m$ is ungrounded.
  $\langle 2 \rangle 2$. $x \in B$
    PROOF: Since $B$ is transitive ($\langle 1 \rangle 4$).
  $\langle 2 \rangle 3$. $x \in A$
    PROOF: $\langle 1 \rangle 5$
  $\langle 2 \rangle 4$. Q.E.D.
    PROOF: This contradicts $\langle 1 \rangle 6$.
$\langle 1 \rangle 8$. $m$ is grounded.
  PROOF: $\langle 1 \rangle 2$
$\langle 1 \rangle 9$. Q.E.D.
  PROOF: This contradicts $\langle 1 \rangle 6$.
□

**Definition 10.0.6** (Rank). The *rank* of a set $A$ is the least ordinal $\alpha$ such that $A \in V_{\alpha^+}$.

**Proposition 10.0.7.** *For any set $A$ we have*

$$\operatorname{rank} A = \bigcup_{a \in A} (\operatorname{rank} a)^+$$

PROOF:
$\langle 1 \rangle 1$. LET: $\alpha = \bigcup_{a \in A} (\operatorname{rank} a)^+$
$\langle 1 \rangle 2$. $A \subseteq V_\alpha$
  $\langle 2 \rangle 1$. LET: $a \in A$
  $\langle 2 \rangle 2$. $a \in V_{(\operatorname{rank} a)^+}$
  $\langle 2 \rangle 3$. $a \in V_\alpha$
$\langle 1 \rangle 3$. $A \in V_{\alpha^+}$
$\langle 1 \rangle 4$. If $A \subseteq V_\beta$ then $\alpha \leq \beta$
  $\langle 2 \rangle 1$. ASSUME: $A \subseteq V_\beta$
  $\langle 2 \rangle 2$. For all $a \in A$ we have $(\operatorname{rank} a)^+ \leq \beta$
    PROOF: Since $a \in V_\beta$.
  $\langle 2 \rangle 3$. $\alpha \leq \beta$
□

**Corollary 10.0.7.1.** *For any sets $a$ and $b$, if $a \in b$ then $\operatorname{rank} a < \operatorname{rank} b$.*

**Proposition 10.0.8.** *For any ordinal number $\alpha$ we have $\operatorname{rank} \alpha = \alpha$.*

PROOF:
$\langle 1 \rangle 1$. LET: $\alpha$ be an ordinal.
$\langle 1 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall \beta < \alpha . \operatorname{rank} \beta = \beta$
$\langle 1 \rangle 3$. $\operatorname{rank} \alpha = \bigcup_{\beta < \alpha} \beta^+$

Proof:

$$\operatorname{rank}\alpha = \bigcup_{\beta<\alpha}(\operatorname{rank}\beta)^+$$

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

$\langle 1\rangle 4.$  $\bigcup_{\beta<\alpha}\beta^+ \leq \alpha$

Proof: Since for all $\beta < \alpha$ we have $\beta^+ \leq \alpha$.

$\langle 1\rangle 5.$  $\alpha \leq \bigcup_{\beta<\alpha}\beta^+$

   $\langle 2\rangle 1.$  Let:  $\gamma = \bigcup_{\beta<\alpha}\beta^+$

   $\langle 2\rangle 2.$  Assume:  for a contradiction $\gamma < \alpha$

   $\langle 2\rangle 3.$  $\gamma^+ \leq \bigcup_{\beta<\alpha}\beta^+ = \gamma$

   $\langle 2\rangle 4.$  Q.E.D.

      Proof: This is a contradiction.

∎

# Chapter 11

# Models of Set Theory

**Definition 11.0.1** (Relativization). Let $\sigma$ be a sentence in the language of set theory and $\mathbf{M}$ a class. The *relativization* of $\sigma$ to $\mathbf{M}$ is the sentence $\sigma^{\mathbf{M}}$ formed by replacing every quantifier $\forall x$ with $\forall x \in \mathbf{M}$, and $\exists x$ with $\exists x \in \mathbf{M}$.

We write '$\mathbf{M}$ is a model of $\sigma$' for the sentence $\sigma^{\mathbf{M}}$.

**Theorem Schema 11.0.2.** *For any class $\mathbf{M}$, the following is a theorem:*
   *If $\mathbf{M}$ is a transitive class, then $\mathbf{M}$ is a model of the Axiom of Extensionality.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: $\mathbf{M}$ is a transitive class.
   PROVE:   $\forall x, y \in \mathbf{M}(\forall z \in \mathbf{M}(z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$
$\langle 1 \rangle 2.$ LET: $x, y \in \mathbf{M}$
$\langle 1 \rangle 3.$ ASSUME: $\forall z \in \mathbf{M}(z \in x \Leftrightarrow z \in y)$
$\langle 1 \rangle 4.$ $\forall z(z \in x \Leftrightarrow z \in y)$
   PROOF: Since $z \in x \Rightarrow z \in \mathbf{M}$ and $z \in y \Rightarrow z \in \mathbf{M}$ by $\langle 1 \rangle 1$.
$\langle 1 \rangle 5.$ $x = y$
□

**Theorem 11.0.3.** *If $\alpha$ is a non-zero ordinal then $V_\alpha$ is a model of the statement: The empty class is a set.*

PROOF:
$\langle 1 \rangle 1.$ LET: $\alpha \neq 0$
   PROVE:   $\exists x \in V_\alpha . \forall y \in V_\alpha . y \notin x$
$\langle 1 \rangle 2.$ $\emptyset \in V_\alpha$
$\langle 1 \rangle 3.$ $\forall y \in V_\alpha . y \notin \emptyset$
□

**Theorem 11.0.4.** *For any limit ordinal $\lambda$, we have $V_\lambda$ is a model of the statement: for any sets $a$ and $b$, the class $\{a, b\}$ is a set.*

PROOF:
$\langle 1 \rangle 1.$ LET: $\lambda$ be a limit ordinal.

PROVE:    $\forall a, b \in V_\lambda . \exists c \in V_\lambda . \forall x \in V_\lambda (x \in c \Leftrightarrow x = a \vee x = b)$

⟨1⟩2. LET:  $a, b \in V_\lambda$

⟨1⟩3. PICK $\alpha, \beta < \lambda$ such that $a \in V_\alpha$ and $b \in V_\beta$

⟨1⟩4. ASSUME:  w.l.o.g. $\alpha \leq \beta$

⟨1⟩5. $a, b \in V_\beta$

⟨1⟩6. $\{a, b\} \in V_{\beta+1}$

⟨1⟩7. $\{a, b\} \in V_\lambda$

⟨1⟩8. $\forall x \in V_\lambda (x \in \{a, b\} \Leftrightarrow x = a \vee x = b)$

☐

**Theorem 11.0.5.** *For any ordinal $\alpha$, we have $V_\alpha$ is a model of the Union Axiom.*

PROOF:

⟨1⟩1. LET:  $\alpha$ be an ordinal.

PROVE:    $\forall a \in V_\alpha . \exists b \in V_\alpha . \forall x \in V_\alpha (x \in b \Leftrightarrow \exists y \in V_\alpha (x \in y \wedge y \in a))$

⟨1⟩2. LET:  $a \in V_\alpha$

⟨1⟩3. PICK $\beta < \alpha$ such that $a \subseteq V_\beta$

⟨1⟩4. $\bigcup a \subseteq V_\beta$

PROOF: $V_\beta$ is a transitive set.

⟨1⟩5. $\bigcup a \in V_\alpha$

⟨1⟩6. $\forall x \in V_\alpha (x \in \bigcup a \Leftrightarrow \exists y \in V_\alpha (x \in y \wedge y \in a))$

PROOF: $V_\alpha$ is a transitive set.

☐

**Theorem 11.0.6.** *For any limit ordinal $\lambda$, we have $V_\lambda$ is a model of the Power Set Axiom.*

PROOF:

⟨1⟩1. LET:  $\lambda$ be a limit ordinal.

PROVE:    $\forall a \in V_\lambda . \exists b \in V_\lambda . \forall x \in V_\lambda (x \in b \Leftrightarrow \forall y \in V_\lambda (y \in x \Rightarrow y \in a))$

⟨1⟩2. LET:  $a \in V_\lambda$

⟨1⟩3. PICK $\alpha < \lambda$ such that $a \in V_\alpha$

⟨1⟩4. $\mathcal{P}a \in V_{\alpha+1}$

⟨1⟩5. $\mathcal{P}a \in V_\lambda$

⟨1⟩6. $\forall x \in V_\lambda (x \in \mathcal{P}a \Leftrightarrow \forall y \in V_\lambda (y \in x \Rightarrow y \in a))$

☐

# Chapter 12

# Group Theory

## 12.1 Groups

**Definition 12.1.1** (Group). A *group* $G$ consists of a set $G$ and a function $\cdot : G^2 \to G$ such that:

1. $\cdot$ is associative

2. There exists $e \in G$ such that $\forall x \in G. xe = x$ and $\forall x \in G. \exists y \in G. xy = e$.

**Proposition 12.1.2.** *The inverse of an element in a group is unique.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: $b$ and $b'$ are inverses of $a$.
$\langle 1 \rangle 2.$ $b = b'$
   PROOF:
$$b = be$$
$$= bab'$$
$$= eb'$$
$$= b'$$

☐

**Definition 12.1.3.** We write $x^{-1}$ for the inverse of $x$.

**Proposition 12.1.4.** *In any group, if $ab = ac$ then $b = c$.*

PROOF:
$$b = eb$$
$$= a^{-1}ab$$
$$= a^{-1}ac$$
$$= ec$$
$$= c \qquad\qquad\qquad ☐$$

## 12.2   Abelian Groups

**Definition 12.2.1** (Abelian group)**.** An *Abelian group* is a group whose multiplication is commutative.

We may say we are writing an Abelian group *additively*, meaning we write $a + b$ for $ab$, 0 for $e$ and $-a$ for $a^{-1}$. In this case we write $a - b$ for $ab^{-1}$.

# Chapter 13

# Ring Theory

## 13.1 Rings

**Definition 13.1.1** (Commutative Ring). A *commutative ring* consists of a set $R$ and two binary operations $+, \cdot$ on $R$ such that:

- $D$ is an Abelian group under $+$. Let us write $0$ for its identity element.

- $\cdot$ is commutative and associative, and distributes over $+$.

- $\cdot$ has an identity element $1$ that is different from $0$.

**Proposition 13.1.2.** *In any commutative ring, $0x = 0$.*

PROOF:

$$(0 + 0)x = 0x$$
$$\therefore 0x + 0x = 0x + 0$$
$$\therefore 0x = 0 \qquad \qquad \text{(Proposition 12.1.4)} \square$$

**Proposition 13.1.3.** *In any commutative ring, $(-a)b = -(ab)$.*

PROOF:

$$ab + (-a)b = (a + (-a))b$$
$$= 0b$$
$$= 0 \qquad \qquad \text{(Proposition 13.1.2)} \square$$

## 13.2 Ordered Rings

**Definition 13.2.1** (Ordered Commutative Ring). An *ordered commutative ring* consists of a commutative ring $R$ with a linear order $<$ on $R$ such that:

- for all $x, y, z \in R$, we have $x < y$ if and only if $x + z < y + z$.

- for all $x, y, z \in R$, if $0 < z$ then we have $x < y$ if and only if $xz < yz$.

**Proposition 13.2.2.** *In any ordered commutative ring, $0 < 1$.*

PROOF: If $1 < 0$ then we have $0 < -1$ and so $0 < (-1)(-1) = 1$, which is a contradiction. □

**Proposition 13.2.3.** *The ordering on an ordered commutative ring is dense; that is, if $x < y$ then there exists $z$ such that $x < z < y$.*

PROOF: Take $z = (x + y)/2$. □

## 13.3    Integral Domains

**Definition 13.3.1** (Integral Domain). An *integral domain* is a commutative ring such that, for all $a, b \in D$, if $ab = 0$ then $a = 0$ or $b = 0$.

**Proposition 13.3.2.** *In any integral domain, if $ab = ac$ and $a \neq 0$ then $b = c$.*

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

**Definition 13.3.3** (Ordered Integral Domain). An *ordered integral domain* is an ordered commutative ring that is an integral domain.

# Chapter 14

# Field Theory

## 14.1 Fields

**Definition 14.1.1** (Field). A *field* $F$ is a commutative ring such that $0 \neq 1$ and, for all $x \in F$, if $x \neq 0$ then there exists $y \in F$ such that $xy = 1$.

**Proposition 14.1.2.** *Every field is an integral domain.*

PROOF: If $ab = 0$ and $a \neq 0$ then $b = a^{-1}ab = 0$. □

**Proposition 14.1.3.** *In any field $F$, we have $F - \{0\}$ is an Abelian group under multiplication.*

PROOF: Immediate from the definition. □

**Definition 14.1.4** (Field of Fractions). Let $D$ be an integral domain. The *field of fractions* of $D$ is the quotient set $F = (D \times (D - \{0\}))/\sim$ where

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

under

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$
$$[(a, b)][(c, d)] = [(ac, bd)]$$

We prove this is a field.

PROOF:
$\langle 1 \rangle 1.$ $\sim$ is an equivalence relation on $D \times (D - \{0\})$.
  PROOF:
   $\langle 2 \rangle 1.$ $\sim$ is reflexive.
    PROOF: We always have $ab = ba$.
   $\langle 2 \rangle 2.$ $\sim$ is symmetric.
    PROOF: If $ad = bc$ then $cb = da$.

⟨2⟩3. ∼ is transitive.

  ⟨3⟩1. ASSUME: $(a, b) \sim (c, d) \sim (e, f)$

  ⟨3⟩2. $ad = bc$ and $cf = de$

  ⟨3⟩3. $adf = bde$

    PROOF: $adf = bcf = bde$

  ⟨3⟩4. $af = be$

    PROOF: Proposition 13.3.2.

□

⟨1⟩2. Addition is well-defined.

  PROOF:

  ⟨2⟩1. If $b \neq 0$ and $d \neq 0$ then $bd \neq 0$.

    PROOF: Since $D$ is an integral domain.

  ⟨2⟩2. If $ab' = a'b$ and $cd' = c'd$ then $(ad + bc)b'd' = (a'd' + b'c')bd$.

    PROOF:

$$(ad + bc)b'd' = ab'dd' + bb'cd'$$
$$= a'bdd' + bb'c'd$$
$$= (a'd' + b'c')bd$$

□

⟨1⟩3. Multiplication is well-defined.

  PROOF:

  ⟨2⟩1. If $b \neq 0$ and $d \neq 0$ then $bd \neq 0$.

    PROOF: Since $D$ is an integral domain.

  ⟨2⟩2. If $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$ then $[(ac, bd)] = [(a'c', b'd')]$.

    PROOF: If $ab' = a'b$ and $cd' = c'd$ then $acb'd' = a'c'bd$.

□

⟨1⟩4. Addition is commutative.

  PROOF: $[(a, b)] + [(c, d)] = [(ad + bc, bd)] = [(cb + da, db)] = [(c, d)] + [(a, b)]$ □

⟨1⟩5. Addition is associative.

  PROOF:

$$[(a, b)] + ([(c, d)] + [(e, f)]) = [(a, b)] + [(cf + de, df)]$$
$$= [(adf + bcf + bde, bdf)]$$
$$= [(ad + bc, bd)] + [(e, f)]$$
$$= ([(a, b)] + [(c, d)]) + [(e, f)] \qquad □$$

⟨1⟩6. For any $x \in F$ we have $x + [(0, 1)] = x$

  PROOF: $[(a, b)] + [(0, 1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a, b)]$ □

⟨1⟩7. For any $x \in F$, there exists $y \in F$ such that $x + y = [(0, 1)]$.

  PROOF: $[(a, b)] + [(-a, b)] = [(ab - ab, b^2)] = [(0, b^2)] = [(0, 1)]$ □

⟨1⟩8. Multiplication is commutative.

  PROOF: $[(a, b)][(c, d)] = [(c, d)][(a, b)] = [(ac, bd)]$. □

⟨1⟩9. Multiplication is assocative.

  PROOF: $[(a, b)]([(c, d)][(e, f)]) = ([(a, b)][(c, d)])[(e, f)] = [(ace, bdf)]$. □

⟨1⟩10. For any $x \in F$ we have $x[(1, 1)] = x$

  PROOF: $[(a, b)][(1, 1)] = [(a, b)]$ □

⟨1⟩11. For any non-zero $x \in F$, there exists $y \in F$ such that $xy = [(1, 1)]$.

PROOF:
⟨2⟩1. LET: $[(a, b)] \in \mathbb{Q}$
⟨2⟩2. ASSUME: $[(a, b)] \neq [(0, 1)]$
⟨2⟩3. $a \neq 0$
⟨2⟩4. $[(a, b)][(b, a)] = [(1, 1)]$
$\square$

$\square$

**Definition 14.1.5.** For any field $F$, let $N(F)$ be the intersection of all the subsets $S \subseteq F$ such that $1 \in S$ and $\forall x \in S.x + 1 \in S$.

**Definition 14.1.6** (Characteristic Zero)**.** A field $F$ has *characteristic 0* iff $0 \notin N(F)$.

**Proposition 14.1.7.** *In a field $F$ with characteristic 0, the function $n : \mathbb{N} \to N(F)$ defined by*

$$n(0) = 1$$
$$n(x + 1) = n(x) + 1$$

*is a bijection.*

PROOF:
⟨1⟩1. $n$ is injective.
    ⟨2⟩1. ASSUME: for a contradiction $n(i) = n(j)$ with $i \neq j$
    ⟨2⟩2. ASSUME: w.l.o.g. $i < j$
    ⟨2⟩3. $n(j - i) = 0$
    ⟨2⟩4. Q.E.D.
        PROOF: This contradicts the fact that $F$ has characteristic 0.
⟨1⟩2. $n$ is surjective.
    PROOF: Since ran $n$ is a subset of $F$ that includes 1 and is closed under $+1$.
$\square$

**Definition 14.1.8.** In any field $F$, let

$$I(F) = N(F) \cup \{0\} \cup \{-x \mid x \in N(F)\}$$

**Definition 14.1.9.** In any field $F$, let

$$Q(F) = \{x/y \mid x, y \in I(F), y \neq 0\}$$

**Proposition 14.1.10.** $Q(F)$ *is the smallest subfield of $F$.*

PROOF: $Q(F)$ is closed under $+$ and $\cdot$, and any subset of $F$ closed under $+$ and $\cdot$ that contains 0 and 1 must include $Q(F)$. $\square$

**Theorem 14.1.11.** *Let $F$ and $G$ be fields of characteristic 0. Then there exists a unique field isomorphism between $Q(F)$ and $Q(G)$.*

PROOF:

⟨1⟩1. LET: $\phi : N(F) \to N(G)$ be the unique function such that $\phi(1) = 1$ and
        $\forall x \in N(F).\phi(x + 1) = \phi(x) + 1$.

⟨1⟩2. $\phi$ is a bijection.
    PROOF: Similar to Proposition 14.1.7.

⟨1⟩3. $\forall x, y \in N(F).\phi(x + y) = \phi(x) + \phi(y)$
    PROOF: Induction on $y$.

⟨1⟩4. $\forall x, y \in N(F).\phi(xy) = \phi(x)\phi(y)$
    PROOF: Induction on $y$.

⟨1⟩5. Extend $\phi$ to a bijection $I(F) \cong I(G)$ such that $\forall x, y \in I(F).\phi(x + y) =$
        $\phi(x) + \phi(y)$ and $\forall x, y \in I(F).\phi(xy) = \phi(x)\phi(y)$

  ⟨2⟩1. Define $\phi(0) = 0$ and $\phi(-x) = -\phi(x)$ for $x \in N(F)$

    ⟨3⟩1. $0 \notin N(F)$

    ⟨3⟩2. For all $x \in N(F)$ we have $-x \notin N(F)$
        PROOF: Then we would have $x + -x = 0 \in N(F)$.

    ⟨3⟩3. For all $x \in N(F)$ we have $-x \neq 0$

  ⟨2⟩2. For all $x, y \in I(F)$ we have $\phi(x + y) = \phi(x) + \phi(y)$
        PROOF: Case analysis on $x$ and $y$.

  ⟨2⟩3. For all $x, y \in I(F)$ we have $\phi(xy) = \phi(x)\phi(y)$
        PROOF: Case analysis on $x$ and $y$.

⟨1⟩6. Extend $\phi$ to a bijection $Q(F) \cong Q(G)$ such that $\forall x, y \in Q(F).\phi(x + y) =$
        $\phi(x) + \phi(y)$ and $\forall x, y \in Q(F).\phi(xy) = \phi(x)\phi(y)$

  ⟨2⟩1. Define $\phi(x/y) = \phi(x)/\phi(y)$

⟨1⟩7. $\phi$ is unique.

  ⟨2⟩1. LET: $\theta$ satisfy the theorem.

  ⟨2⟩2. For all $x \in N(F)$ we have $\theta(x) = \phi(x)$

  ⟨2⟩3. For all $x \in I(F)$ we have $\theta(x) = \phi(x)$

  ⟨2⟩4. For all $x \in Q(F)$ we have $\theta(x) = \phi(x)$

□

## 14.2   Ordered Fields

**Definition 14.2.1** (Ordered Field)**.** An *ordered field* is an ordered commutative ring that is a field.

**Proposition 14.2.2.** *Every ordered field $F$ has characteristic 0.*

PROOF: We have $0 < n$ for all $n \in N(F)$. □

**Proposition 14.2.3.** *Let $F$ be a field of characteristic 0. Then there exists a unique relation $<$ on $Q(F)$ that makes $Q(F)$ into an ordered field.*

PROOF: Easy. □

**Corollary 14.2.3.1.** *Let $F$ and $G$ be ordered fields. Let $\phi$ be the unique field isomorphism between $Q(F)$ and $Q(G)$. Then $\phi$ is an ordered field isomorphism.*

**Definition 14.2.4** (Archimedean)**.** An ordered field $F$ is *Archimedean* iff

$$\forall x \in F.\exists n \in N(F).n > x \ .$$

**Proposition 14.2.5.** *Let $F$ be an Archimedean ordered field. Let $x, y \in F$ with $x > 0$. Then there exists $n \in N(F)$ such that $nx > y$.*

PROOF: Pick $n > y/x$. $\square$

**Proposition 14.2.6.** *Let $F$ be an Archimedean ordered field. For all $x, y \in F$, if $x < y$, then there exists $r \in Q(F)$ such that $x < r < y$.*

PROOF:
⟨1⟩1. CASE: $x > 0$
  ⟨2⟩1. PICK $n \in N(F)$ such that $n(y - x) > 1$
    PROOF: Proposition 14.2.5.
  ⟨2⟩2. $ny > 1 + nx$
  ⟨2⟩3. LET: $m$ be the least element of $N(F)$ such that $m > nx$.
  ⟨2⟩4. $m - 1 \leq nx$
  ⟨2⟩5. $nx < m < ny$
  ⟨2⟩6. $x < m/n < y$
⟨1⟩2. CASE: $x \leq 0$
  ⟨2⟩1. PICK $k \in N(F)$ such that $k > -x$
  ⟨2⟩2. $0 < x + k < y + k$
  ⟨2⟩3. PICK $r \in Q(F)$ such that $x + k < r < y + k$
    PROOF: ⟨1⟩1
  ⟨2⟩4. $x < r - k < y$

**Definition 14.2.7** (Complete). An ordered field $F$ is *complete* iff every nonempty subset of $F$ bounded above has a least upper bound.

**Proposition 14.2.8.** *Every complete ordered field is Archimedean.*

PROOF:
⟨1⟩1. LET: $F$ be a complete ordered field.
⟨1⟩2. LET: $x \in F$
⟨1⟩3. ASSUME: for a contradiction there is no member of $N(F)$ greater than $x$.
⟨1⟩4. $x$ is an upper bound for $N(F)$.
⟨1⟩5. LET: $y = \sup N(F)$
⟨1⟩6. PICK $n \in N(F)$ such that $y - 1 < n$
⟨1⟩7. $y < n + 1$
⟨1⟩8. Q.E.D.
  PROOF: This is a contradiction.
$\square$

**Proposition 14.2.9.** *Let $F$ be a complete ordered field and $a \in F$ be nonnegative. Then there exists $b \in F$ such that $b^2 = a$.*

PROOF:
⟨1⟩1. LET: $B = \{x \in F \mid 0 \leq x \leq 1 + a\}$
⟨1⟩2. LET: $\phi : B \to B$ be the function
$$\phi(x) = x + \frac{1}{2(1 + a)}(a - x^2) \ .$$

⟨1⟩3. $\phi$ is strictly monotone.
  ⟨2⟩1. LET: $0 \le x < y \le 1 + a$
  ⟨2⟩2. $1 - \frac{x+y}{2(1+a)} > 0$
  ⟨2⟩3. $\phi(y) - \phi(x) = (y - x)(1 - \frac{x+y}{2(1+a)}) > 0$
  ⟨2⟩4. $\phi(x) < \phi(y)$
⟨1⟩4. PICK $b \in B$ such that $\phi(b) = b$.
  PROOF: Knaster Fixed-Point Theorem.
⟨1⟩5. $b^2 = a$
☐

**Theorem 14.2.10** (Uniqueness of the Complete Ordered Field)**.** *If $F$ and $G$ are complete ordered fields, then there exists a unique bijection $\phi : F \cong G$ such that, for all $x, y \in F$,*

$$\phi(x + y) = \phi(x) + \phi(y)$$
$$\phi(xy) = \phi(x)\phi(y)$$

*This bijection also satisfies: for all $x, y \in F$,*

$$x < y \Leftrightarrow \phi(x) < \phi(y) \ .$$

PROOF:
⟨1⟩1. PICK a bijection $\phi : Q(F) \cong Q(G)$ such that, for all $x, y \in Q(F)$,
$$\phi(x + y) = \phi(x) + \phi(y)$$
$$\phi(xy) = \phi(x)\phi(y)$$
$$x < y \Leftrightarrow \phi(x) < \phi(y)$$
  PROOF: Corollary 14.2.3.1.
⟨1⟩2. $Q(F)$ intersects every interval in $F$.
  PROOF: Proposition 14.2.6.
⟨1⟩3. $Q(G)$ intersects every interval in $G$.
  PROOF: Proposition 14.2.6.
⟨1⟩4. PICK an order isomorphism $\psi : F \cong G$ that extends $\phi$.
  PROOF: Theorem 5.1.21.
⟨1⟩5. $\forall x, y \in F.\psi(x + y) = \psi(x) + \psi(y)$
  ⟨2⟩1. LET: $x, y \in F$
  ⟨2⟩2. $\psi(x) + \psi(y) \not< \psi(x + y)$
    ⟨3⟩1. ASSUME: for a contradiction $\psi(x) + \psi(y) < \psi(x + y)$
    ⟨3⟩2. PICK $r' \in Q(G)$ such that $\psi(x) < r' < \psi(x + y) - \psi(y)$
    ⟨3⟩3. PICK $s' \in Q(G)$ such that $\psi(y) < s' < \psi(x + y) - r'$
    ⟨3⟩4. $r' + s' < \psi(x + y)$
    ⟨3⟩5. PICK $r, s \in Q(F)$ such that $\phi(r) = r'$ and $\phi(s) = s'$
    ⟨3⟩6. $\phi(r + s) = r' + s'$
    ⟨3⟩7. $\psi(x) < \psi(r)$
    ⟨3⟩8. $\psi(y) < \psi(s)$
    ⟨3⟩9. $\psi(x + y) > \psi(r + s)$
    ⟨3⟩10. $x < r$

⟨3⟩11. $y < s$
⟨3⟩12. $x + y > r + s$
⟨3⟩13. Q.E.D.
  PROOF: This is a contradiction.
⟨2⟩3. $\psi(x + y) \not< \psi(x) + \psi(y)$
  PROOF: Similar.
⟨1⟩6. $\forall x, y \in F.\psi(xy) = \psi(x)\psi(y)$
  ⟨2⟩1. LET: $x, y \in F$
  ⟨2⟩2. CASE: $x$ and $y$ are positive.
    ⟨3⟩1. $\psi(x)\psi(y) \not< \psi(xy)$
      ⟨4⟩1. ASSUME: for a contradiction $\psi(x)\psi(y) < \psi(xy)$
      ⟨4⟩2. PICK $r' \in Q(G)$ such that $\psi(x) < r' < \psi(xy)/\psi(y)$
      ⟨4⟩3. PICK $s' \in Q(G)$ such that $\psi(y) < s' < \psi(xy)/r'$
      ⟨4⟩4. $r's' < \psi(xy)$
      ⟨4⟩5. PICK $r, s \in Q(F)$ such that $\phi(r) = r'$ and $\phi(s) = s'$
      ⟨4⟩6. $\phi(rs) = r's'$
      ⟨4⟩7. $x < r$, $y < s$ and $rs < xy$
      ⟨4⟩8. Q.E.D.
        PROOF: This is a contradiction.
    ⟨3⟩2. $\psi(xy) \not< \psi(x)\psi(y)$
      PROOF: Similar.
  ⟨2⟩3. CASE: $x$ and $y$ are not both positive.
    PROOF: Follows from ⟨2⟩2 since $\psi(-x) = -\psi(x)$ by ⟨1⟩5.
⟨1⟩7. For any field isomorphism $\theta : F \cong G$, we have $\theta = \psi$.
  ⟨2⟩1. $\theta \restriction Q(F) = \phi$
    PROOF: Theorem 14.1.11.
  ⟨2⟩2. $\theta$ is strictly monotone.
    ⟨3⟩1. LET: $x, y \in F$ with $x < y$
    ⟨3⟩2. $y - x > 0$
    ⟨3⟩3. PICK $z \in F$ such that $z^2 = y - x$
    ⟨3⟩4. $\theta(z)^2 = \theta(y) - \theta(x)$
    ⟨3⟩5. $\theta(y) - \theta(x) > 0$
    ⟨3⟩6. $\theta(x) < \theta(y)$
  ⟨2⟩3. $\theta = \psi$
    PROOF: By the uniqueness of $\psi$.
☐

# Chapter 15

# Number Systems

## 15.1   The Integers

**Definition 15.1.1.** The set of *integers* $\mathbb{Z}$ is the quotient set $\mathbb{N}^2/\sim$, where $(m, n) \sim (p, q)$ iff $m + q = n + p$.

   We prove$\sim$ is an equivalence relation on $\mathbb{N}^2$.

PROOF:
$\langle 1 \rangle 1.$ $\sim$ is reflexive.
   PROOF: For all $m, n \in \mathbb{N}$ we have $m + n = n + m$.
$\langle 1 \rangle 2.$ $\sim$ is symmetric.
   PROOF: If $m + q = n + p$ then $p + n = q + m$.
$\langle 1 \rangle 3.$ $\sim$ is transitive.
   $\langle 2 \rangle 1.$ ASSUME: $(m, n) \sim (p, q) \sim (r, s)$
   $\langle 2 \rangle 2.$ $m + q = n + p$ and $p + s = q + r$
   $\langle 2 \rangle 3.$ $m + q + s = n + q + r$
   $\langle 2 \rangle 4.$ $m + s = n + r$
      PROOF: By cancellation.
☐

**Definition 15.1.2** (Addition)**.** Define *addition* $+$ on $\mathbb{Z}$ by $[(m, n)] + [(p, q)] = [(m + p, n + q)]$.

   We prove this is well-defined.

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

**Proposition 15.1.3.** *Addition on $\mathbb{Z}$ is commutative.*

PROOF: $[(m, n)] + [(p, q)] = [(m+p, n+q)] = [(p+m, q+n)] = [(p, q)] + [(m, n)]$.
☐

**Proposition 15.1.4.** *Addition on $\mathbb{Z}$ is associative.*

**Proposition 15.1.14.** *Multiplication on $\mathbb{Z}$ is associative.*

Proof:
$$
\begin{aligned}
[(m,n)]([(p,q)][(r,s)]) &= [(m,n)][(pr+qs, ps+qr)]\\
&= [(mpr+mqs+nps+nqr, mps+mqr+npr+nqs)]\\
&= [(mp+nq, mq+np)][(r,s)]\\
&= ([(m,n)][(p,q)])[(r,s)] \qquad\qquad \square
\end{aligned}
$$

**Proposition 15.1.15.** *Multiplication distributes over addition.*

Proof:
$$
\begin{aligned}
[(m,n)]([(p,q)]+[(r,s)]) &= [(m,n)][(p+r, q+s)]\\
&= [(mp+mr+nq+ns, np+nr+mq+ms)]\\
[(m,n)][(p,q)]+[(m,n)][(r,s)] &= [(mp+nq, mq+np)]+[(mr+ns, ms+nr)]\\
&= [(mp+nq+mr+ns, mq+np+ms+nr)] \quad \square
\end{aligned}
$$

**Proposition 15.1.16.** *For any integer $a$ we have $a1 = a$.*

Proof: Since $[(m,n)][(1,0)] = [(m1+n0, m0+n1)] = [(m,n)]$. $\square$

**Proposition 15.1.17.** *For any integeres $a$ and $b$, if $ab = 0$ then $a = 0$ or $b = 0$.*

Proof:
$\langle 1\rangle 1$. Assume:  $[(m,n)][(p,q)] = [(0,0)]$
$\langle 1\rangle 2$.  $mp+nq = mq+np$
$\langle 1\rangle 3$. Assume:  $[(m,n)] \neq [(0,0)]$
$\langle 1\rangle 4$.  $m \neq n$
    Prove:   $p = q$
$\langle 1\rangle 5$. Case:  $m < n$
  $\langle 2\rangle 1$.  $p \not< q$
    Proof: If $p < q$ then $mq+np < mp+nq$ by Proposition 8.4.6.
  $\langle 2\rangle 2$.  $q \not< p$
    Proof: If $q < p$ then $mp+nq < mq+np$ by Proposition 8.4.6.
  $\langle 2\rangle 3$.  $p = q$
    Proof: By trichotomy.
$\langle 1\rangle 6$. Case:  $n < m$
  Proof: Similar.
$\square$

**Proposition 15.1.18.** *The integers $\mathbb{Z}$ form an integral domain.*

Proof: Propositions 15.1.13, 15.1.14, 15.1.15, 15.1.16, 15.1.17, 15.1.10. $\square$

**Definition 15.1.19.** Define $<$ on $\mathbb{Z}$ by $[(m,n)] < [(p,q)]$ if and only if $m+q < n+p$.
    We prove this is well-defined.

Proof:

⟨1⟩1.  ASSUME: $m + n' = n + m'$ and $p + q' = q + p'$.
    PROVE:   $m + q < n + p$ if and only if $m' + q' < n' + p'$
⟨1⟩2.  $m + q < n + p$ if and only if $m' + q' < n' + p'$
  PROOF:

$$m + q < n + p \Leftrightarrow m + n' + q < n + n' + p \qquad \text{(Corollary 6.5.7.1)}$$
$$\Leftrightarrow m' + n + q < n + n' + p$$
$$\Leftrightarrow m' + q < n' + p \qquad \text{(Corollary 6.5.7.1)}$$
$$\Leftrightarrow m' + q + p' < n' + p + p' \qquad \text{(Corollary 6.5.7.1)}$$
$$\Leftrightarrow m' + q' + p < n' + p + p'$$
$$\Leftrightarrow m' + q' < n' + p' \qquad \text{(Corollary 6.5.7.1)}\ \square$$

**Proposition 15.1.20.** *The ordering on the integers agrees with the ordering on the natural numbers.*

PROOF: We have $[(m, 0)] < [(n, 0)]$ iff $m < n$. $\square$

**Proposition 15.1.21.** $<$ *is a linear order on* $\mathbb{Z}$.

PROOF:
⟨1⟩1.  $<$ is irreflexive.
  PROOF: We never have $m + n < m + n$.
⟨1⟩2.  $<$ is transitive.
  ⟨2⟩1.  ASSUME:  $[(m, n)] < [(p, q)] < [(r, s)]$
  ⟨2⟩2.  $m + q < n + p$ and $p + s < q + r$
  ⟨2⟩3.  $m + q + s < n + q + r$
    PROOF: $m + q + s < n + p + s < n + q + r$
  ⟨2⟩4.  $m + s < n + r$
    PROOF: Corollary 6.5.7.1.
⟨1⟩3.  $<$ is total.
  PROOF: Given natural numbers $m$, $n$, $p$ and $q$, either $m + q < n + p$, or $m + q = n + p$, or $n + p < m + q$.
$\square$

**Definition 15.1.22** (Positive)**.** An integer $a$ is *positive* iff $a > 0$.

**Theorem 15.1.23.** *For any integers $a$, $b$ and $c$, we have $a < b$ if and only if $a + c < b + c$.*

PROOF:
⟨1⟩1.  If $a < b$ then $a + c < b + c$.
  ⟨2⟩1.  LET: $a = [(m, n)]$, $b = [(p, q)]$ and $c = [(r, s)]$.
  ⟨2⟩2.  ASSUME: $a < b$
  ⟨2⟩3.  $m + q < n + p$
  ⟨2⟩4.  $m + r + q + s < n + r + p + s$
  ⟨2⟩5.  $[(m + r, n + s)] < [(p + r, q + s)]$
  ⟨2⟩6.  $a + c < b + c$

$\langle 1 \rangle 2$. If $a + c < b + c$ then $a < b$.
    PROOF: From $\langle 1 \rangle 1$ and Proposition 5.2.6.
▯

**Proposition 15.1.24.** *Let $a$, $b$ and $c$ be integers. If $0 < c$, then $a < b$ if and only if $ac < bc$.*

PROOF:
$\langle 1 \rangle 1$. LET: $c = [(r, s)]$
$\langle 1 \rangle 2$. ASSUME: $0 < c$
$\langle 1 \rangle 3$. $s < r$
$\langle 1 \rangle 4$. For all integers $a$ and $b$, if $a < b$ then $ac < bc$
    $\langle 2 \rangle 1$. LET: $a = [(m, n)]$, $b = [(p, q)]$.
    $\langle 2 \rangle 2$. ASSUME: $a < b$
    $\langle 2 \rangle 3$. $m + q < n + p$
    $\langle 2 \rangle 4$. $(m + q)r + (p + n)s < (m + q)s + (p + n)r$
      PROOF: Proposition 8.4.6, $\langle 1 \rangle 3$, $\langle 2 \rangle 3$.
    $\langle 2 \rangle 5$. $mr + ns + ps + qr < ms + nr + pr + qs$
    $\langle 2 \rangle 6$. $[(mr + ns, ms + nr)] < [(pr + qs, ps + qr)]$
    $\langle 2 \rangle 7$. $ac < bc$
$\langle 1 \rangle 5$. For all integers $a$ and $b$, if $ac < bc$ then $a < b$
    PROOF: From $\langle 1 \rangle 4$ and Proposition 5.2.6.
▯

**Proposition 15.1.25.** *Let $a$ be a positive integer. For any integer $b$, there exists $k \in \mathbb{N}$ such that $b < ak$.*

PROOF:
$\langle 1 \rangle 1$. CASE: $b \leq 0$
    PROOF: Take $k = 1$.
$\langle 1 \rangle 2$. CASE: $b > 0$
    PROOF: Take $k = b + 1$.
▯

## 15.2   The Rationals

**Definition 15.2.1** (Rational Numbers)**.** The set $\mathbb{Q}$ of *rational numbers* is the field of fractions over the integers.

**Proposition 15.2.2.** *For any integers $a$ and $b$, we have $[(a, 1)] = [(b, 1)]$ iff $a = b$.*

PROOF: Immediate from definitions. ▯

    Henceforth we identify any integer $a$ with the rational number $[(a, 1)]$.

**Proposition 15.2.3.** *Addition on the rationals agrees with addition on the integers.*

Proof: $[(a, 1)] + [(b, 1)] = [(a \cdot 1 + b \cdot 1, 1 \cdot 1)] = [(a + b, 1)]$. $\square$

**Proposition 15.2.4.** *Multiplication on the rationals agrees with multiplication on the integers.*

Proof: $[(a, 1)][(b, 1)] = [(ab, 1)]$ $\square$

**Definition 15.2.5.** Define the ordering $<$ on the rationals by: if $b$ and $d$ are positive, then $[(a, b)] < [(c, d)]$ iff $ad < bc$.

    We prove this is well-defined.

Proof:
$\langle 1 \rangle 1$. For any rational $q$, there exist integers $a$, $b$ with $b$ positive such that
    $q = [(a, b)]$.
  Proof: Since $[(a, b)] = [(-a, -b)]$, and if $b \neq 0$ then one of $b$ and $-b$ is
  positive.
$\langle 1 \rangle 2$. If $b$, $b'$, $d$ and $d'$ are positive, $[(a, b)] = [(a', b')]$, and $[(c, d)] = [(c', d')]$,
    then $ad < bc$ iff $a'd' < b'c'$.
  Proof:
  $\langle 2 \rangle 1$. If $ad < bc$ then $a'd' < b'c'$.
    $\langle 3 \rangle 1$. Assume: $ad < bc$
    $\langle 3 \rangle 2$. $ab'd < bb'c$
    $\langle 3 \rangle 3$. $a'bd < bb'c$
    $\langle 3 \rangle 4$. $a'd < b'c$
    $\langle 3 \rangle 5$. $a'dd' < b'cd'$
    $\langle 3 \rangle 6$. $a'dd' < b'c'd$
    $\langle 3 \rangle 7$. $a'd' < b'c'$
  $\langle 2 \rangle 2$. If $a'd' < b'c'$ then $ad < bc$.
    Proof: Similar.
$\square$

**Proposition 15.2.6.** *The ordering on the rationals agrees with the ordering on the integers.*

Proof: We have $[(a, 1)] < [(b, 1)]$ if and only if $a < b$. $\square$

**Proposition 15.2.7.** *The relation $<$ is a linear ordering on $\mathbb{Q}$.*

Proof:
$\langle 1 \rangle 1$. $<$ is irreflexive.
  Proof: We never have $ab < ab$.
$\langle 1 \rangle 2$. $<$ is transitive.
  $\langle 2 \rangle 1$. Assume: $[(a, b)] < [(c, d)] < [(e, f)]$ where $b$, $d$ and $f$ are positive.
  $\langle 2 \rangle 2$. $ad < bc$ and $cf < de$
  $\langle 2 \rangle 3$. $adf < bde$
    Proof: $adf < bcf < bde$
  $\langle 2 \rangle 4$. $af < be$
$\langle 1 \rangle 3$. $<$ is total.
  Proof: For any integers $a$, $b$, $c$, $d$, we have $ad < bc$ or $ad = bc$ or $bc < ad$.

□

**Proposition 15.2.8.** *For any rationals $r$, $s$ and $t$, we have $r < s$ if and only if $r + t < s + t$.*

PROOF:
⟨1⟩1.  LET: $a$, $b$, $c$, $d$, $e$, $f$ be integers with $b$, $d$ and $f$ positive.
⟨1⟩2.  $[(a,b)] + [(e,f)] < [(c,d)] + [(e,f)]$ if and only if $[(a,b)] < [(c,d)]$.
  PROOF:
$$[(a,b)] + [(e,f)] < [(c,d)] + [(e,f)] \Leftrightarrow [(af + be, bf)] < [(cf + de, df)]$$
$$\Leftrightarrow (af + be)df < (cf + de)bf$$
$$\Leftrightarrow afdf + bedf < cfbf + debf$$
$$\Leftrightarrow afdf < cfbf$$
$$\Leftrightarrow ad < bc$$
$$\Leftrightarrow [(a,b)] < [(c,d)]$$

□

**Corollary 15.2.8.1.** *For any rational $r$, we have $r < 0$ if and only if $0 < -r$.*

**Definition 15.2.9** (Absolute Value)**.** For any rational $r$, the *absolute value* of $r$ is defined by
$$|r| := \begin{cases} -r & \text{if } 0 < -r \\ r & \text{otherwise} \end{cases}$$

**Proposition 15.2.10.** *For any rationals $r$, $s$ and $t$, if $t$ is positive then $r < s$ iff $rt < st$.*

PROOF:
⟨1⟩1.  LET: $r = [(a,b)]$, $s = [(c,d)]$ and $t = [(e,f)]$ where $b$, $d$ and $f$ are positive.
⟨1⟩2.  ASSUME: $0 < t$
⟨1⟩3.  $e > 0$
⟨1⟩4.  $rt < st$ iff $r < s$
  PROOF:
$$rt < st \Leftrightarrow [(ae, bf)] < [(ce, df)]$$
$$\Leftrightarrow aedf < cebf$$
$$\Leftrightarrow ad < bc$$
$$\Leftrightarrow r < s$$

□

**Corollary 15.2.10.1.** *The rationals form an ordered field.*

**Proposition 15.2.11.** *Let $p$ be a positive rational. For any rational number $r$, there exists $k \in \mathbb{N}$ such that $r < pk$.*

PROOF:
⟨1⟩1.  LET: $p = a/b$ and $r = c/d$ where $a$, $b$ and $d$ are positive.

$\langle 1 \rangle 2$. PICK $k \in \mathbb{N}$ such that $bc < adk$
  PROOF: Proposition 15.1.25.
$\langle 1 \rangle 3$. $r < pk$
$\square$

**Proposition 15.2.12.** $\mathbb{Q} \approx \mathbb{N}$

PROOF: Arrange the rationals in order $0/1$, $1/1$, $1/2$, $0/2$, $-1/2$, $-1/1$, $-2/1$, $-2/2$, $-2/3$, $-1/3$, $0/3$, $1/3$, $2/3$, etc. then remove all duplicates. $\square$

## 15.3   The Real Numbers

**Definition 15.3.1** (Cauchy Sequence)**.** A *Cauchy sequence* is a sequence $(q_n)$ of rationals such that, for every positive rational $\epsilon$, there exists $k \in \mathbb{N}$ such that $\forall m, n > k.|q_m - q_n| < \epsilon$.

**Definition 15.3.2** (Dedekind Cut)**.** A *Dedekind cut* is a set $x \subseteq \mathbb{Q}$ such that:

1. $\emptyset \neq x \neq \mathbb{Q}$

2. $x$ is closed downwards.

3. $x$ has no greatest member.

  The set $\mathbb{R}$ of *real numbers* is the set of Dedekind cuts.

**Proposition 15.3.3.** *For any rational $q$, we have $\{r \in \mathbb{Q} \mid r < q\} \in \mathbb{R}$.*

PROOF:
$\langle 1 \rangle 1$. LET: $q \in \mathbb{Q}$
$\langle 1 \rangle 2$. LET: $q \downarrow = \{r \mid r < q\}$
$\langle 1 \rangle 3$. $q \downarrow \neq \emptyset$
  PROOF: We have $q - 1 \in q \downarrow$.
$\langle 1 \rangle 4$. $q \downarrow \neq \mathbb{Q}$
  PROOF: Since $q \notin q \downarrow$.
$\langle 1 \rangle 5$. $q \downarrow$ is closed downwards.
  PROOF: Trivial.
$\langle 1 \rangle 6$. $q \downarrow$ has no greatest element.
  PROOF: For all $r \in q \downarrow$ we have $r < (q + r)/2 \in q \downarrow$.
$\square$

**Proposition 15.3.4.** *For rationals $q$ and $r$, we have $q = r$ if and only if $\{s \in \mathbb{Q} \mid s < q\} = \{s \in \mathbb{Q} \mid s < r\}$.*

PROOF:
$\langle 1 \rangle 1$. LET: $q \downarrow = \{s \in \mathbb{Q} \mid s < q\}$
$\langle 1 \rangle 2$. LET: $r \downarrow = \{s \in \mathbb{Q} \mid s < r\}$
$\langle 1 \rangle 3$. If $q = r$ then $q \downarrow = r \downarrow$
  PROOF: Trivial.

$\langle 1 \rangle 4$.  If $q < r$ then $q \downarrow \neq r \downarrow$
   PROOF: We have $q \in r \downarrow$ and $q \notin q \downarrow$.
$\langle 1 \rangle 5$.  If $r < q$ then $q \downarrow \neq r \downarrow$
   PROOF: We have $r \in q \downarrow$ and $q \notin q \downarrow$.
$\square$

   Henceforth we identify a rational $q$ with the real number $\{r \in \mathbb{Q} \mid r < q\}$.

**Definition 15.3.5.** Define the ordering $<$ on $\mathbb{R}$ by: $x < y$ iff $x \subsetneq y$.

**Proposition 15.3.6.** *The ordering on the reals agrees with the ordering on the rationals.*

PROOF:
$\langle 1 \rangle 1$.  LET:  $q, r \in \mathbb{Q}$
$\langle 1 \rangle 2$.  LET:  $q \downarrow = \{s \in \mathbb{Q} \mid s < q\}$.
$\langle 1 \rangle 3$.  LET:  $r \downarrow = \{s \in \mathbb{Q} \mid s < r\}$.
      PROVE:   $q < r$ iff $q \downarrow \subsetneq r \downarrow$
$\langle 1 \rangle 4$.  If $q < r$ then $q \downarrow \subsetneq r \downarrow$
   $\langle 2 \rangle 1$.  ASSUME:  $q < r$
   $\langle 2 \rangle 2$.  $q \downarrow \subseteq r \downarrow$
      PROOF: If $s < q$ then $s < r$.
   $\langle 2 \rangle 3$.  $q \downarrow \neq r \downarrow$
      PROOF: Proposition 15.3.4.
$\langle 1 \rangle 5$.  If $q \downarrow \subsetneq r \downarrow$ then $q < r$
   $\langle 2 \rangle 1$.  ASSUME:  $q \downarrow \subsetneq r \downarrow$
   $\langle 2 \rangle 2$.  PICK $s \in r \downarrow$ such that $s \notin q \downarrow$
   $\langle 2 \rangle 3$.  $q \leq s < r$
$\square$

**Proposition 15.3.7.** *The ordering $<$ is a linear ordering on $\mathbb{R}$.*

PROOF:
$\langle 1 \rangle 1$.  $<$ is irreflexive.
   PROOF: No set is a proper subset of itself.
$\langle 1 \rangle 2$.  $<$ is transitive.
   PROOF: Since the relationship $\subsetneq$ is transitive on the class of all sets.
$\langle 1 \rangle 3$.  $<$ is total.
   $\langle 2 \rangle 1$.  LET:  $x$, $y$ be Dedekind cuts.
   $\langle 2 \rangle 2$.  ASSUME:  $x \nsubseteq y$
         PROVE:   $y \subsetneq x$
   $\langle 2 \rangle 3$.  PICK $q \in x$ such that $q \notin y$
   $\langle 2 \rangle 4$.  LET:  $r \in y$
         PROVE:   $r \in x$
   $\langle 2 \rangle 5$.  $q \nleq r$
      PROOF: Since $y$ is closed downwards.
   $\langle 2 \rangle 6$.  $r < q$
   $\langle 2 \rangle 7$.  $r \in x$

        PROOF: Since $x$ is closed downwards.
☐

**Proposition 15.3.8.** *Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound.*

PROOF:
⟨1⟩1. LET: $A$ be a bounded nonempty subset of $\mathbb{R}$.
⟨1⟩2. $\bigcup A$ is a Dedekind cut.
  ⟨2⟩1. $\bigcup A \neq \emptyset$
    ⟨3⟩1. PICK $x \in A$
    ⟨3⟩2. PICK $q \in x$
    ⟨3⟩3. $q \in \bigcup A$
  ⟨2⟩2. $\bigcup A \neq \mathbb{Q}$
    ⟨3⟩1. PICK an upper bound $u$ for $A$
    ⟨3⟩2. PICK $q \notin u$
       PROVE:  $q \notin \bigcup A$
    ⟨3⟩3. ASSUME: for a contradiction $q \in \bigcup A$
    ⟨3⟩4. PICK $x \in A$ such that $q \in x$
    ⟨3⟩5. $x \leq u$
    ⟨3⟩6. $q \in u$
    ⟨3⟩7. Q.E.D.
      PROOF: This is a contradiction.
  ⟨2⟩3. $\bigcup A$ is closed downwards.
    ⟨3⟩1. LET: $q \in \bigcup A$ and $r < q$
    ⟨3⟩2. PICK $x \in A$ such that $q \in x$
    ⟨3⟩3. $r \in x$
    ⟨3⟩4. $r \in \bigcup A$
  ⟨2⟩4. $\bigcup A$ has no greatest element.
    ⟨3⟩1. LET: $q \in \bigcup A$
    ⟨3⟩2. PICK $x \in A$ such that $q \in x$
    ⟨3⟩3. PICK $r \in x$ such that $q < r$
    ⟨3⟩4. $r \in \bigcup A$
⟨1⟩3. $\bigcup A$ is an upper bound for $A$.
  PROOF: For all $x \in A$ we have $x \subseteq \bigcup A$.
⟨1⟩4. For any upper bound $u$ for $\bigcup A$ we have $\bigcup A \leq u$.
  PROOF: If $\forall x \in A.x \subseteq u$ we have $\bigcup A \subseteq u$.
☐

**Definition 15.3.9** (Addition)**.** Define *addition* $+$ on the reals by

$$x + y := \{q + r \mid q \in x, r \in y\} \ .$$

We prove this is well-defined.

PROOF:
⟨1⟩1. LET: $x, y \in \mathbb{R}$
    PROVE:  $X + y$ is a Dedekind cut.

$\langle 1\rangle 2.$  $x + y \neq \emptyset$
  PROOF: Pick $q \in x$ and $r \in y$; then $q + r \in x + y$.
$\langle 1\rangle 3.$  $x + y \neq \mathbb{Q}$
  $\langle 2\rangle 1.$  PICK $q \notin x$ and $r \notin y$
      PROVE:   $q + r \notin x + y$
  $\langle 2\rangle 2.$  ASSUME: for a contradiction $q + r \in x + y$
  $\langle 2\rangle 3.$  PICK $q' \in x$ and $r' \in y$ such that $q + r = q' + r'$
  $\langle 2\rangle 4.$  $q' < q$ and $r' < r$
  $\langle 2\rangle 5.$  $q' + r' < q + r$
  $\langle 2\rangle 6.$  Q.E.D.
    PROOF: This is a contradiction.
$\langle 1\rangle 4.$  $x + y$ is closed downwards.
  $\langle 2\rangle 1.$  LET: $q \in x$ and $r \in y$
  $\langle 2\rangle 2.$  LET: $s < q + r$
      PROVE:   $s \in x + y$
  $\langle 2\rangle 3.$  $s - r < q$
  $\langle 2\rangle 4.$  $s - r \in x$
  $\langle 2\rangle 5.$  $s = (s - r) + r \in x + y$
$\langle 1\rangle 5.$  $x + y$ has no greatest element.
  $\langle 2\rangle 1.$  LET: $q \in x$ and $r \in y$
      PROVE:   There exists $s \in x + y$ such that $q + r < s$
  $\langle 2\rangle 2.$  PICK $q' \in x$ and $r' \in y$ such that $q < q'$ and $r < r'$
  $\langle 2\rangle 3.$  $q + r < q' + r' \in x + y$

⬜

**Proposition 15.3.10.** *Addition on the reals agrees with addition on the rationals.*

PROOF:
$\langle 1\rangle 1.$  LET: $q, r \in \mathbb{Q}$
$\langle 1\rangle 2.$  $q \downarrow + r \downarrow \subseteq (q + r) \downarrow$
  PROOF: If $s_1 < q$ and $s_2 < r$ then $s_1 + s_2 < q + r$.
$\langle 1\rangle 3.$  $(q + r) \downarrow \subseteq q \downarrow + r \downarrow$
  $\langle 2\rangle 1.$  LET: $s < q + r$
  $\langle 2\rangle 2.$  $s - r < q$
  $\langle 2\rangle 3.$  PICK $t$ such that $s - r < t < q$
  $\langle 2\rangle 4.$  $s - t < r$
  $\langle 2\rangle 5.$  $s = t + (s - t) \in q \downarrow + r \downarrow$

⬜

**Proposition 15.3.11.** *Addition is associative.*

PROOF:

$$
\begin{aligned}
x + (y + z) &= \{q + r \mid q \in x, r \in y + z\} \\
&= \{q + s_1 + s_2 \mid q \in x, s_1 \in y, s_2 \in z\} \\
&= \{r + s_2 \mid r \in x + y, s_2 \in z\} \\
&= (x + y) + z
\end{aligned}
$$

⬜

**Proposition 15.3.12.** *Addition is commutative.*

PROOF:

$$x + y = \{q + r \mid q \in x, r \in y\}$$
$$= \{r + q \mid r \in y, q \in x\}$$
$$= y + x \qquad\qquad \Box$$

**Proposition 15.3.13.** *For any $x \in \mathbb{R}$ we have $x + 0 = x$.*

PROOF:
$\langle 1 \rangle 1.\ x + 0 \subseteq x$
   PROOF: If $q \in x$ and $r < 0$ then $q + r < q$ so $q + r \in x$.
$\langle 1 \rangle 2.\ x \subseteq x + 0$
   $\langle 2 \rangle 1.$ LET: $q \in x$
   $\langle 2 \rangle 2.$ PICK $r \in x$ such that $q < r$.
     PROOF: $x$ has no greatest element.
   $\langle 2 \rangle 3.\ q - r < 0$
   $\langle 2 \rangle 4.\ q = r + (q - r) \in x + 0$
$\Box$

**Definition 15.3.14.** For $x \in \mathbb{R}$, define $-x := \{q \in \mathbb{Q} \mid \exists r > q.\ -r \notin x\}$.

**Proposition 15.3.15.** *For all $x \in \mathbb{R}$ we have $-x \in \mathbb{R}$.*

PROOF:
$\langle 1 \rangle 1.$ LET: $x \in \mathbb{R}$
$\langle 1 \rangle 2.\ -x \neq \emptyset$
   $\langle 2 \rangle 1.$ PICK $s \notin x$
   $\langle 2 \rangle 2.\ -s - 1 \in -x$
$\langle 1 \rangle 3.\ -x \neq \mathbb{Q}$
   $\langle 2 \rangle 1.$ PICK $s \in x$
      PROVE:  $-s \notin -x$
   $\langle 2 \rangle 2.$ ASSUME: for a contradiction $-s \in -x$
   $\langle 2 \rangle 3.$ PICK $r > -s$ such that $-r \notin x$
   $\langle 2 \rangle 4.\ -r < s$
   $\langle 2 \rangle 5.$ Q.E.D.
     PROOF: This contradicts the fact that $x$ is closed downwards.
$\langle 1 \rangle 4.\ -x$ is closed downwards.
   PROOF: Immediate from definition.
$\langle 1 \rangle 5.\ -x$ has no greatest element.
   $\langle 2 \rangle 1.$ LET: $q \in -x$
   $\langle 2 \rangle 2.$ PICK $r > q$ such that $-r \notin x$
   $\langle 2 \rangle 3.$ PICK $s$ such that $q < s < r$
   $\langle 2 \rangle 4.\ s \in -x$
$\Box$

**Lemma 15.3.16.** *Let $p$ be a positive rational number. For any real number $x$, there exists a rational $q \in x$ such that $p + q \notin x$.*

Proof:

⟨1⟩1. Pick $q_0 \in x$

⟨1⟩2. There exists $k \in \mathbb{N}$ such that $q_0 + kp \notin x$

   ⟨2⟩1. Pick $q_1 \notin x$

   ⟨2⟩2. Pick $k \in \mathbb{N}$ such that $q_1 - q_0 < pk$

     Proof: Proposition 15.2.11.

   ⟨2⟩3. $q_1 < q_0 + kp$

   ⟨2⟩4. $q_0 + kp \notin x$

⟨1⟩3. Let: $k$ be the least natural number such that $q_0 + kp \notin x$

⟨1⟩4. $k \neq 0$

   Proof: ⟨1⟩1

⟨1⟩5. Let: $q = q_0 + (k-1)p$

⟨1⟩6. $q \in x$ and $q + p \notin x$.

$\square$

**Proposition 15.3.17.** *For every real $x$ we have $x + (-x) = 0$.*

Proof:

⟨1⟩1. Let: $x$ be a real number.

⟨1⟩2. $x + (-x) \subseteq 0$

   ⟨2⟩1. Let: $q_1 \in x$ and $q_2 \in -x$

   ⟨2⟩2. Pick $r > q_2$ such that $-r \notin x$

   ⟨2⟩3. $q_1 < -r$

   ⟨2⟩4. $r < -q_1$

   ⟨2⟩5. $q_2 < -q_1$

   ⟨2⟩6. $q_1 + q_2 < 0$

⟨1⟩3. $0 \subseteq x + (-x)$

   ⟨2⟩1. Let: $p < 0$

   ⟨2⟩2. $0 < -p$

   ⟨2⟩3. Pick $q \in x$ such that $q - p/2 \notin x$

     Proof: Lemma 15.3.16.

   ⟨2⟩4. Let: $s = p/2 - q$

   ⟨2⟩5. $-s \notin x$

   ⟨2⟩6. $p - q < s$

   ⟨2⟩7. $p - q \in -x$

   ⟨2⟩8. $p \in x + (-x)$

$\square$

**Corollary 15.3.17.1.** *The reals form an Abelian group under addition.*

**Proposition 15.3.18.** *For any reals $x$, $y$ and $z$, we have $x < y$ if and only if $x + z < y + z$.*

Proof:

⟨1⟩1. $\forall x, y, z \in \mathbb{R}.x \leq y \Rightarrow x + z \leq y + z$

   ⟨2⟩1. Let: $x, y, z \in \mathbb{R}$

   ⟨2⟩2. Assume: $x \leq y$

   ⟨2⟩3. For all $q \in x$ and $r \in z$ we have $q + r \in y + z$

$\langle 1 \rangle 2.$ $\forall x, y, z \in \mathbb{R}. x + z = y + z \Leftrightarrow x = y$
   PROOF: Proposition 12.1.4.
$\langle 1 \rangle 3.$ $\forall x, y, z \in \mathbb{R}. x < y \Rightarrow x + z < y + z$
$\langle 1 \rangle 4.$ Q.E.D.
   PROOF: Proposition 5.2.6.
☐

**Definition 15.3.19** (Absolute Value)**.** The *absolute value* of a real number $x$ is defined to be
$$|x| = \begin{cases} x & \text{if } 0 \leq x \\ -x & \text{if } x < 0 \end{cases}$$

**Definition 15.3.20** (Multiplication)**.** Define *multiplication* $\cdot$ on $\mathbb{R}$ as follows:

- If $x$ and $y$ are non-negative then

$$xy = 0 \cup \{rs \mid 0 \leq r \in x \land 0 \leq s \in y\} \ .$$

- If $x$ and $y$ are both negative then

$$xy = (-x)(-y) \ .$$

- If one of $x$ and $y$ is negative and one is non-negative then

$$xy = -(|x||y|) \ .$$

We prove this is well-defined.

PROOF:
$\langle 1 \rangle 1.$ LET: $x$ and $y$ be non-negative reals.
     PROVE:   $xy$ is real.
$\langle 1 \rangle 2.$ $xy \neq \emptyset$
  PROOF: Since $-1 \in xy$.
$\langle 1 \rangle 3.$ $xy \neq \mathbb{Q}$
   $\langle 2 \rangle 1.$ PICK $r \notin x$ and $s \notin y$
      PROVE:   $rs \notin xy$
   $\langle 2 \rangle 2.$ $0 \leq r$ and $0 \leq s$
    PROOF: Since $0 \subseteq x$ and $0 \subseteq y$.
   $\langle 2 \rangle 3.$ ASSUME: for a contradiction $rs \in xy$
   $\langle 2 \rangle 4.$ PICK $r'$ and $s'$ such that $0 \leq r' \in x$, $0 \leq s' \in y$ and $rs = r's'$
   $\langle 2 \rangle 5.$ $r' < r$
   $\langle 2 \rangle 6.$ $s' < s$
   $\langle 2 \rangle 7.$ $r's' < rs$
   $\langle 2 \rangle 8.$ Q.E.D.
    PROOF: This is a contradiction.
$\langle 1 \rangle 4.$ $xy$ is closed downwards.
   $\langle 2 \rangle 1.$ LET: $q \in xy$ and $r < q$

$\langle 2 \rangle$2.  Case: $q \in 0$
   Proof: Then $r < q < 0$ so $r \in xy$
$\langle 2 \rangle$3.  Case: $q = s_1 s_2$ where $0 \le s_1 \in x$ and $0 \le s_2 \in y$
   $\langle 3 \rangle$1.  Assume: w.l.o.g. $0 \le r$
   $\langle 3 \rangle$2.  $0 < s_1$ and $0 < s_2$
   $\langle 3 \rangle$3.  $r/s_2 < s_1$
   $\langle 3 \rangle$4.  $r/s_2 \in x$
   $\langle 3 \rangle$5.  $r = (r/s_2)s_2 \in xy$
$\langle 1 \rangle$5.  $xy$ has no greatest element.
   $\langle 2 \rangle$1.  Let: $q \in xy$
   $\langle 2 \rangle$2.  Case: $q \in 0$
      Proof: $q < q/2 \in 0$
   $\langle 2 \rangle$3.  Case: $q = rs$ where $0 \le r \in x$ and $0 \le s \in y$
      $\langle 3 \rangle$1.  Pick $r'$ and $s'$ with $r < r' \in x$ and $s < s' \in y$
      $\langle 3 \rangle$2.  $q < r's' \in xy$
☐

**Proposition 15.3.21.** *Multiplication is commutative.*

Proof: Immediate from definition.  ☐

**Proposition 15.3.22.** *Multiplication is associative.*

Proof:
$\langle 1 \rangle$1.  For non-negative reals $x$, $y$ and $z$, we have $x(yz) = (xy)z$
   Proof: It computes to $0 \cup \{qrs \mid 0 \le q \in x, 0 \le r \in y, 0 \le s \in z\}$.
$\langle 1 \rangle$2.  For all reals $x$, $y$ and $z$, we have $x(yz) = (xy)z$
   Proof: It is equal to $|x||y||z|$ if an even number of them are negative, and
   $-(|x||y||z|)$ otherwise.
☐

**Proposition 15.3.23.** *Multiplication distributes over addition.*

Proof:
$\langle 1 \rangle$1.  For all non-negative reals $x$, $y$ and $z$, we have $x(y + z) = xy + xz$
   $\langle 2 \rangle$1.  Let: $x$, $y$ and $z$ be non-negative reals.
   $\langle 2 \rangle$2.  $x(y + z) \subseteq xy + xz$
      $\langle 3 \rangle$1.  Let: $q \in x(y + z)$
      $\langle 3 \rangle$2.  Case: $q < 0$
         Proof: Then we have $q/2 \in xy$ and $q/2 \in xz$ so $q \in xy + xz$.
      $\langle 3 \rangle$3.  Case: $q = rs$ where $0 \le r \in x$ and $0 \le s \in y + z$
         $\langle 4 \rangle$1.  Pick $s_1 \in y$ and $s_2 \in z$ such that $s = s_1 + s_2$
         $\langle 4 \rangle$2.  $rs_1 \in xy$
            Proof: If $s_1 < 0$ then $rs_1 < 0$ so $rs_1 \in xy$. If $0 \le s_1$ then we also
            have $rs_1 \in xy$.
         $\langle 4 \rangle$3.  $rs_2 \in xz$
            Proof: Similar.
         $\langle 4 \rangle$4.  $q \in xy + xz$

PROOF: Since $q = rs_1 + rs_2$.

$\langle 2 \rangle 3$. $xy + xz \subseteq x(y + z)$

   $\langle 3 \rangle 1$. LET: $q \in xy$ and $r \in xz$.

      PROVE:  $q + r \in x(y + z)$

   $\langle 3 \rangle 2$. CASE: $q < 0$ and $r < 0$

     PROOF: Then $q + r < 0$ so $q + r \in x(y + z)$.

   $\langle 3 \rangle 3$. CASE: $q < 0$ and $r = r_1 r_2$ where $0 \leq r_1 \in x$ and $0 \leq r_2 \in z$

     $\langle 4 \rangle 1$. $q + r < r$

     $\langle 4 \rangle 2$. $q + r \in xz$

     $\langle 4 \rangle 3$. ASSUME: w.l.o.g. $0 \leq q + r$

       PROOF: Otherwise $q + r \in x(y + z)$ immediately.

     $\langle 4 \rangle 4$. PICK $s_1$, $s_2$ with $0 \leq s_1 \in x$, $0 \leq s_2 \in y$ and $q + r = s_1 s_2$

     $\langle 4 \rangle 5$. $s_2 \in y + z$

       PROOF: Since $0 \in z$ so $s_2 = s_2 + 0 \in y + z$.

     $\langle 4 \rangle 6$. $q + r \in x(y + z)$

   $\langle 3 \rangle 4$. CASE: $q = q_1 q_2$ where $0 \leq q_1 \in x$ and $0 \leq q_2 \in y$ and $r < 0$

     PROOF: Similar.

   $\langle 3 \rangle 5$. CASE: $q = q_1 q_2$ where $0 \leq q_1 \in x$ and $0 \leq q_2 \in y$ and $r = r_1 r_2$ where
          $0 \leq r_1 \in x$ and $0 \leq r_2 \in z$

     $\langle 4 \rangle 1$. ASSUME: w.l.o.g. $q_1 \leq r_1$

     $\langle 4 \rangle 2$. $q + r \leq r_1(q_2 + r_2) \in x(y + z)$

$\langle 1 \rangle 2$. For any negative real $x$ and non-negative reals $y$ and $z$, we have $x(y+z) = xy + xz$

  PROOF:

$$x(y + z) = -(-x)(y + z) = -((-x)y + (-x)z) \qquad (\langle 1 \rangle 1)$$
$$= -((-x)y) - ((-x)z)$$
$$= xy + xz$$

$\langle 1 \rangle 3$. For any non-negative real $x$ and reals $y$ and $z$ with one negative and one
      non-negative, we have $x(y + z) = xy + xz$

  $\langle 2 \rangle 1$. ASSUME: w.l.o.g. $y$ is negative and $z$ is non-negative.

  $\langle 2 \rangle 2$. CASE: $0 \leq y + z$

    PROOF:

$$xy + xz = xy + x(-y + y + z)$$
$$= -(x(-y)) + x(-y + y + z)$$
$$= -(x(-y)) + x(-y) + x(y + z) \qquad (\langle 1 \rangle 1)$$
$$= x(y + z)$$

  $\langle 2 \rangle 3$. CASE: $y + z < 0$

    $\langle 3 \rangle 1$. $-y - z > 0$

    $\langle 3 \rangle 2$. $-y = z - y - z$

    $\langle 3 \rangle 3$. $xy + xz = x(y + z)$

Proof:
$$
\begin{aligned}
xy + xz &= -(x(-y)) + xz \\
&= -(x(z - y - z)) + xz \\
&= -(xz + x(-y - z)) + xz && (\langle 1 \rangle 1) \\
&= -xy - x(-y - z) + xz \\
&= -x(-y - z) \\
&= x(y + z)
\end{aligned}
$$

⟨1⟩4. For any non-negative real $x$ and negative reals $y$ and $z$, we have $x(y+z) = xy + xz$

Proof:
$$
\begin{aligned}
x(y + z) &= -x(-y - z) \\
&= -(x(-y) + x(-z)) && (\langle 1 \rangle 1) \\
&= -x(-y) - x(-z) \\
&= xy + xz
\end{aligned}
$$

⟨1⟩5. For any negative real $x$ and reals $y$ and $z$ with one negative and one non-negative, we have $x(y + z) = xy + xz$

⟨2⟩1. Assume: w.l.o.g. $y$ is negative and $z$ is non-negative.

⟨2⟩2. Case: $0 \le y + z$

Proof:
$$
\begin{aligned}
x(y + z) &= -((-x)(y + z)) \\
&= -((-x)y + (-x)z) && (\langle 1 \rangle 3) \\
&= -((-x)y) - ((-x)z) \\
&= (-x)(-y) - ((-x)z) \\
&= xy + xz
\end{aligned}
$$

⟨2⟩3. Case: $y + z < 0$

Proof:
$$
\begin{aligned}
x(y + z) &= (-x)(-y - z) \\
&= (-x)(-y) + (-x)(-z) && (\langle 1 \rangle 3) \\
&= xy + xz
\end{aligned}
$$

⟨1⟩6. For any negative reals $x$, $y$ and $z$, we have $x(y + z) = xy + xz$

Proof:
$$
\begin{aligned}
x(y + z) &= (-x)(-y - z) \\
&= (-x)(-y) + (-x)(-z) && (\langle 1 \rangle 1) \\
&= xy + xz
\end{aligned}
$$

☐

**Proposition 15.3.24.** *For any real $x$ we have $x1 = x$.*

Proof:

⟨1⟩1. Case: $0 \le x$

⟨2⟩1. $x1 \subseteq x$

⟨3⟩1. Let: $q \in x1$

⟨3⟩2. CASE: $q < 0$
    PROOF: Then $q \in x$ because $0 \leq x$.
⟨3⟩3. $q = rs$ where $0 \leq r \in x$ and $0 \leq s < 1$
    PROOF: Then $q < r$ so $q \in x$.
⟨2⟩2. $x \subseteq x1$
    ⟨3⟩1. LET: $q \in x$
    ⟨3⟩2. ASSUME: w.l.o.g. $0 \leq q$
    ⟨3⟩3. PICK $r$ such that $q < r \in x$
    ⟨3⟩4. $0 \leq q/r < 1$
    ⟨3⟩5. $q = r(q/r) \in x1$
⟨1⟩2. CASE: $x < 0$
  PROOF:
$$x1 = -((-x)1)$$
$$= -(-x) \qquad\qquad (\langle 1 \rangle 1)$$
$$= x$$

☐

**Lemma 15.3.25.** *Let $x \in \mathbb{R}$ and $c$ be a positive rational. Then there exists $a \in x$ and a non-least rational upper bound $b$ for $x$ such that $b - a = c$.*

PROOF:
⟨1⟩1. PICK $a_1 \in x$ such that if $x$ has a rational supremum $s$ then $a_1 > s - c$
⟨1⟩2. There exists a natural number $n$ such that $a_1 + nc$ is an upper bound for $x$.
    ⟨2⟩1. PICK a non-least upper bound $b_1$ for $x$.
    ⟨2⟩2. PICK a natural number $n$ such that $nc > b_1 - a_1$
        PROOF: Proposition 15.2.11.
    ⟨2⟩3. $a_1 + nc > b_1$
    ⟨2⟩4. $a_1 + nc$ is an upper bound for $x$.
⟨1⟩3. LET: $k$ be the least natural number such that $a_1 + kc$ is an upper bound for $x$.
⟨1⟩4. $a_1 + (k-1)c \in x$
⟨1⟩5. $a_1 + kc$ is not the supremum of $x$.
    ⟨2⟩1. ASSUME: for a contradiction $a_1 + kc$ is the supremum of $x$.
    ⟨2⟩2. $a_1 > a_1 + (k-1)c$
        PROOF: ⟨1⟩1
    ⟨2⟩3. Q.E.D.
        PROOF: This is a contradiction.
⟨1⟩6. LET: $a = a_1 + (k-1)c$
⟨1⟩7. LET: $b = a_1 + kc$
⟨1⟩8. $b - a = c$
☐

**Proposition 15.3.26.** *For any non-zero real $x$, there exists a real $y$ such that $xy = 1$.*

PROOF:

⟨1⟩1. CASE: $0 < x$

  ⟨2⟩1. LET: $y = \{q \in \mathbb{Q} \mid q \leq 0\} \cup \{u^{-1} \mid u$ is an upper bound for $x$ but not the supremum of $x\}$

  ⟨2⟩2. $y$ is a real number.

    ⟨3⟩1. $y \neq \emptyset$

      PROOF: Since $0 \in y$.

    ⟨3⟩2. $y \neq \mathbb{Q}$

      ⟨4⟩1. PICK $q \in x$ such that $0 < q$

      ⟨4⟩2. $q^{-1} \notin y$

    ⟨3⟩3. $y$ is closed downwards.

      ⟨4⟩1. LET: $q \in y$ and $r < q$

        PROVE:   $r \in y$

      ⟨4⟩2. ASSUME: w.l.o.g. $0 < r$

      ⟨4⟩3. $q^{-1}$ is a non-least upper bound for $x$.

      ⟨4⟩4. $q^{-1} < r^{-1}$

      ⟨4⟩5. $r^{-1}$ is a non-least upper bound for $x$.

      ⟨4⟩6. $r \in y$

    ⟨3⟩4. $y$ has no greatest element.

      ⟨4⟩1. LET: $q \in y$

        PROVE:   There exists $r \in y$ such that $q < r$

      ⟨4⟩2. CASE: $q \leq 0$

        ⟨5⟩1. PICK a non-least upper bound $u$ for $x$.

        ⟨5⟩2. $q < u^{-1} \in x$

      ⟨4⟩3. CASE: $q = u^{-1}$ where $u$ is a non-least upper bound for $x$.

        ⟨5⟩1. PICK a non-least upper bound $v$ with $v < u$

        ⟨5⟩2. $u^{-1} < v^{-1} \in y$

  ⟨2⟩3. $0 < y$

  ⟨2⟩4. $xy \subseteq 1$

    ⟨3⟩1. LET: $q \in xy$

    ⟨3⟩2. ASSUME: w.l.o.g. $0 < q$

    ⟨3⟩3. PICK $0 < r \in x$ and $0 < s \in y$ such that $q = rs$

    ⟨3⟩4. $s^{-1}$ is a non-least upper bound for $x$

    ⟨3⟩5. $r < s^{-1}$

    ⟨3⟩6. $rs < 1$

  ⟨2⟩5. $1 \subseteq xy$

    ⟨3⟩1. LET: $q < 1$

      PROVE:   $q \in xy$

    ⟨3⟩2. ASSUME: w.l.o.g. $0 < q$

    ⟨3⟩3. PICK $a_1$ with $0 < a_1 \in x$

    ⟨3⟩4. $(1 - q)a_1 > 0$

    ⟨3⟩5. PICK $a \in x$ and a non-least upper bound $w$ of $x$ such that $w - a = (1 - q)a_1$

      PROOF: Lemma 15.3.25.

    ⟨3⟩6. $w - a < (1 - q)w$

    ⟨3⟩7. $qw < a$

    ⟨3⟩8. $w < a/q$

    ⟨3⟩9. $a/q$ is a non-least upper bound for $x$

$\langle 3 \rangle 10.$  $q/a \in y$
$\langle 3 \rangle 11.$  $q \in xy$
$\langle 1 \rangle 2.$  CASE:  $x < 0$
  $\langle 2 \rangle 1.$  PICK $y$ such that $(-x)y = 1$
    PROOF: $\langle 1 \rangle 1$
  $\langle 2 \rangle 2.$  $x(-y) = 1$
☐

**Proposition 15.3.27.** *For real numbers $x$, $y$ and $z$, if $0 < z$ then $x < y$ if and only if $xz < yz$.*

PROOF:
$\langle 1 \rangle 1.$  For any real numbers $x$, $y$ and $z$, if $0 < z$ and $x < y$ then $xz < yz$
  $\langle 2 \rangle 1.$  LET: $x$, $y$ and $z$ be real numbers.
  $\langle 2 \rangle 2.$  ASSUME: $0 < z$ and $x < y$.
  $\langle 2 \rangle 3.$  $y = x + (y - x)$
  $\langle 2 \rangle 4.$  $y - x > 0$
  $\langle 2 \rangle 5.$  $(y - x)z > 0$
  $\langle 2 \rangle 6.$  $yz > xz$
    PROOF:

$$yz = (x + (y - x))z$$
$$= xz + (y - x)z$$
$$> xz$$

$\langle 1 \rangle 2.$  For any real numbers $x$, $y$ and $z$, if $0 < z$ and $xz < yz$ then $x < y$
  PROOF: Proposition 5.2.6.
☐

**Corollary 15.3.27.1.** *The real numbers form a complete ordered field.*

**Proposition 15.3.28.**
$$(0, 1) \approx \mathbb{R}$$

PROOF: The function $f(x) = (2x - 1)/(x - x^2)$ is a bijection between $(0, 1)$ and $\mathbb{R}$. ☐

**Proposition 15.3.29.**
$$|\mathbb{R}| = 2^{\aleph_0}$$

PROOF:
$\langle 1 \rangle 1.$  $(0, 1) \preccurlyeq 2^{\mathbb{N}}$
  PROOF: The function $H$ where $H(x)(n)$ is the $n$th binary digit of the binary expansion of $x$ is an injection.
$\langle 1 \rangle 2.$  $2^{\mathbb{N}} \preccurlyeq \mathbb{R}$
  PROOF: Map $f$ to the real number in $[0, 1/9]$ whose $n + 1$st decimal digit is $f(n)$.
☐

**Proposition 15.3.30.** *The set of algebraic numbers is countable.*

PROOF: There are countably many integer polynomials, each with finitely many roots. ☐

**Corollary 15.3.30.1.** *There are uncountably many transcendental numbers.*

**Proposition 15.3.31.** *Let $A$ be a set of disks in the plane, no two of which intersect. Then $A$ is countable.*

PROOF: Every circle includes a point with rational coordinates. Define $f : \{q \in \mathbb{Q}^2 \mid \exists C \in A.q \in C\} \to A$ by $f(q) = C$ iff $q \in C$. Then $f$ is surjective. ☐

**Proposition 15.3.32.** *There exists an uncountable set of circles in the plane that do not intersect.*

PROOF: The set of all circles with origin O is uncountable. ☐

# Chapter 16

# Complex Analysis

**Definition 16.0.1.** For $p \geq 1$, let $l^p$ be the set of all sequences of complex numbers $(x_n)$ such that $\sum_{n=1}^{\infty} |x_n|^p < \infty$.

**Proposition 16.0.2.** *If $(x_n), (y_n) \in l^p$ then $(x_n + y_n) \in l^p$.*

PROOF:
$\langle 1 \rangle 1$. LET: $(x_n), (y_n) \in l^p$
$\langle 1 \rangle 2$. $\sum_{n=1}^{\infty} |x_n + y_n|^p \leq 2^p(\sum_{n=1}^{\infty} |x_n|^p + \sum_{n=1}^{\infty} |y_n|^p)$
 PROOF:
 $\langle 2 \rangle 1$. For all $n \in \mathbb{N}$ we have $|x_n + y_n|^p \leq 2^p(|x_n|^p + |y_n|^p)$.
  PROOF:
$$|x_n + y_n|^p \leq (|x_n| + |y_n|)^p \qquad \text{(Triangle Inequality)}$$
$$\leq (2\max(|x_n|, |y_n|))^p$$
$$\leq 2^p(|x_n|^p + |y_n|^p)$$

$\square$

**Theorem 16.0.3** (Hölder's Inequality). *Let $p$ and $q$ be reals such that $p > 1$, $q > 1$ and $1/p + 1/q = 1$. Let $(x_n) \in l^p$ and $(y_n) \in l^q$. Then*

$$\sum_n |x_n y_n| \leq \left( \sum_n |x_n|^p \right)^{1/p} \left( \sum_n |y_n|^q \right)^{1/q}$$

PROOF:
$\langle 1 \rangle 1$. ASSUME: w.l.o.g. neither $(x_n)$ nor $(y_n)$ are all zero.
$\langle 1 \rangle 2$. For $0 \leq x \leq 1$ we have
$$x^{1/p} \leq \frac{1}{p}x + \frac{1}{q} \quad .$$
 $\langle 2 \rangle 1$. LET: $f(x) = x/p + 1/q - x^{1/p}$
 $\langle 2 \rangle 2$. $f'(x) = 1/p(1 - x^{(1-p)/p})$
 $\langle 2 \rangle 3$. $f'(x) \geq 0$ for all $x \in [0, 1]$
 $\langle 2 \rangle 4$. $f$ is a monotonically decreasing function on $[0, 1]$

$\langle 2 \rangle 5.$  $f(0) = 1/q$
$\langle 2 \rangle 6.$  $f(1) = 0$
$\langle 2 \rangle 7.$  $f(x) \geq 0$ for all $x \in [0, 1]$
$\langle 1 \rangle 3.$ For any $a, b \geq 0$ we have

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q} \ .$$

$\quad \langle 2 \rangle 1.$ CASE: $a^p \leq b^q$
$\quad\quad \langle 3 \rangle 1.$  $ab^{-q/p} \leq \frac{1}{p} \frac{a^p}{b^q} + \frac{1}{q}$
$\quad\quad\quad$ PROOF: Substituting $x = a^p/b^q$ in $\langle 1 \rangle 2$.
$\quad\quad \langle 3 \rangle 2.$  $ab^{1-q} \leq \frac{1}{p} \frac{a^p}{b^q} + \frac{1}{q}$
$\quad\quad\quad$ PROOF: From $\langle 3 \rangle 1$ since $1 - q = -q/p$.
$\quad\quad \langle 3 \rangle 3.$  $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$
$\quad\quad\quad$ PROOF: Multiplying $\langle 3 \rangle 2$ by $b^q$.
$\quad \langle 2 \rangle 2.$ CASE: $b^q \leq a^p$
$\quad\quad$ PROOF: Similar.
$\langle 1 \rangle 4.$ For any integers $1 \leq j \leq n$, we have

$$\frac{|x_j|}{\left(\sum_{k=1}^{n} |x_k|^p\right)^{1/p}} \frac{|y_j|}{\left(\sum_{k=1}^{n} |y_k|^q\right)^{1/q}} \leq \frac{1}{p} \frac{|x_j|^p}{\sum_{k=1}^{n} |x_k|^p} + \frac{1}{q} \frac{|y_j|^q}{\sum_{k=1}^{n} |y_k|^q}$$

$\quad$ PROOF: From $\langle 1 \rangle 3$ substituting

$$a = \frac{|x_j|}{\left(\sum_{k=1}^{n} |x_k|^p\right)^{1/p}} \text{ and } b = \frac{|y_j|}{\left(\sum_{k=1}^{n} |y_k|^q\right)^{1/q}}$$

$\langle 1 \rangle 5.$ For any positive integer $n$ we have

$$\frac{\sum_{k=1}^{n} |x_k||y_k|}{\left(\sum_{k=1}^{n} |x_k|^p\right)^{1/p} \left(\sum_{k=1}^{n} |y_k|^q\right)^{1/q}} \leq 1$$

$\quad$ PROOF:

$$\frac{\sum_{j=1}^{n} |x_j||y_j|}{\left(\sum_{k=1}^{n} |x_k|^p\right)^{1/p} \left(\sum_{k=1}^{n} |y_k|^q\right)^{1/q}} \leq \frac{1}{p} + \frac{1}{q} \quad \text{(Summing } \langle 1 \rangle 4 \text{ from } j = 1 \text{ to } n)$$

$$= 1$$

$\langle 1 \rangle 6.$

$$\sum_{n} |x_n y_n| \leq \left(\sum_{n} |x_n|^p\right)^{1/p} \left(\sum_{n} |y_n|^q\right)^{1/q}$$

$\quad$ PROOF: Taking the limit $n \to \infty$ in $\langle 1 \rangle 5$.
□

**Theorem 16.0.4** (Minkowski's Inequality)**.** *Let $p \geq 1$. Let $(x_n), (y_n) \in l^p$.*
*Then*

$$\left(\sum_{n=1}^{\infty} |x_n + y_n|^p\right)^{1/p} \leq \left(\sum_{n=1}^{\infty} |x_n|^p\right)^{1/p} + \left(\sum_{n=1}^{\infty} |y_n|^p\right)^{1/p}$$

PROOF:
$\langle 1 \rangle 1.$ CASE: $p = 1$
$\quad$ PROOF: This is just the Triangle Inequality.
$\langle 1 \rangle 2.$ CASE: $p > 1$
$\quad \langle 2 \rangle 1.$ LET: $q = p/(p - 1)$

⟨2⟩2.

$$\sum_{n=1}^{\infty} |x_n + y_n|^p \leq \left(\sum_{n=1}^{\infty} |x_n|^p\right)^{1/p} \left(\sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)}\right)^{1/q}$$
$$+ \left(\sum_{n=1}^{\infty} |y_n|^p\right)^{1/p} \left(\sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)}\right)^{1/q}$$

PROOF:

⟨3⟩1. $(|x_n + y_n|^{p-1}) \in l^q$

  PROOF:

$$\sum_{n=1}^{\infty} |x_n + y_n|^{(p-1)q} = \sum_{n=1}^{\infty} |x_n + y_n|^p \qquad (⟨2⟩2)$$
$$< \infty \qquad \text{(Proposition 16.0.2)}$$

⟨3⟩2. Q.E.D.

  PROOF:

$$\sum_{n=1}^{\infty} |x_n + y_n|^p = \sum_{n=1}^{\infty} |x_n + y_n||x_n + y_n|^{p-1}$$
$$\leq \sum_{n=1}^{\infty} |x_n||x_n + y_n|^{p-1} + \sum_{n=1}^{\infty} |y_n||x_n + y_n|^{p-1}$$
$$\leq \left(\sum_{n=1}^{\infty} |x_n|^p\right)^{1/p} \left(\sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)}\right)^{1/q}$$
$$+ \left(\sum_{n=1}^{\infty} |y_n|^p\right)^{1/p} \left(\sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)}\right)^{1/q} \qquad \text{(Hölder's Inequality, ⟨2⟩2)}$$

⟨2⟩3.

$$\sum_{n=1}^{\infty} |x_n + y_n|^p \leq \left\{ \left(\sum_{n=1}^{\infty} |x_n|^p\right)^{1/p} + \left(\sum_{n=1}^{\infty} |y_n|^p\right)^{1/p} \right\} \left(\sum_{n=1}^{\infty} |x_n + y_n|^p\right)^{1/q}$$

⟨3⟩1. $q(p-1) = p$

  PROOF: ⟨2⟩2

⟨3⟩2. Q.E.D.

  PROOF: From ⟨2⟩2, ⟨3⟩1.

☐

# Part I

# Linear Algebra

# Chapter 17

# Vector Spaces

## 17.1 Vector Spaces

**Definition 17.1.1** (Vector Space). Let $K$ be either $\mathbb{R}$ or $\mathbb{C}$. A *vector space* over $K$ is a triple $(V, +, \cdot)$ such that:

- $V$ is a nonempty set, whose elemnts are called *vectors*;

- $+ : V^2 \to V$

- $\cdot : K \times V \to V$

such that the following hold for all $u, v, w \in V$ and $\alpha, \beta \in K$:

1. $u + v = v + u$

2. $u + (v + w) = (u + v) + w$

3. For every $u, v \in V$ there exists $w \in V$ such that $u + w = v$

4. $\alpha(\beta v) = (\alpha\beta)v$

5. $(\alpha + \beta)v = \alpha v + \beta v$

6. $\alpha(u + v) = \alpha u + \alpha v$

7. $1v = v$

Elements of $K$ are called *scalars*.

We write *real vector space* for 'vector space over $\mathbb{R}$', and *complex vector space* for 'vector space over $\mathbb{C}$'.

**Proposition 17.1.2.** *Let $K$ be either $\mathbb{R}$ and $\mathbb{C}$. The set $\{0\}$ is a vector space over $K$ under the unique functions $+ : \{0\}^2 \to \{0\}$, $\cdot : K \times \{0\} \to \{0\}$.*

PROOF: Each axiom holds trivially because $x = y$ holds for all $x, y \in \{0\}$. $\square$

**Proposition 17.1.3.** *The set $\mathbb{R}$ is a real vector space under real addition and real multiplication.*

PROOF: TODO — after we have proved these facts about $\mathbb{R}$. $\square$

**Proposition 17.1.4.** *The set $\mathbb{C}$ is a real vector space under complex addition and complex multiplication.*

PROOF: TODO

**Proposition 17.1.5.** *The set $\mathbb{C}$ is a complex vector space under complex addition and complex multiplication.*

PROOF: TODO

**Proposition 17.1.6.** *Let $K$ be either $\mathbb{R}$ or $\mathbb{C}$. Let $\{V_i\}_{i\in I}$ be a family of vector spaces over $K$. Then $\prod_{i\in I} V_i$ is a vector space over $K$ under the operations given by*

$$\{x_i\}_{i\in I} + \{y_i\}_{i\in I} = \{x_i + y_i\}_{i\in I}$$
$$\alpha\{x_i\}_{i\in I} = \{\alpha x_i\}_{i\in I}$$

PROOF: Each axiom follows from the corresponding axiom in $V_i$. $\square\square$

**Corollary 17.1.6.1.** *Let $V$ be a vector space over $K$. For any set $I$, we have $V^I$ is a vector space over $K$.*

**Corollary 17.1.6.2.** *Let $n \in \mathbb{Z}_+$. Then $\mathbb{R}^n$ is a real vector space, and $\mathbb{C}^n$ is both a real and a complex vector space, under*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

**Proposition 17.1.7.** *Let $V$ be a vector space over $K$. Then there exists a unique $0 \in V$ such that, for all $v \in V$, we have $v + 0 = v$.*

PROOF:
$\langle 1\rangle 1$. There exists $0 \in V$ such that $\forall v \in V. v + 0 = v$
  $\langle 2\rangle 1$. Pick $v \in V$
  $\langle 2\rangle 2$. Pick $0 \in V$ such that $v + 0 = v$
    PROOF: Axiom 3.
  $\langle 2\rangle 3$. For all $u \in V$, we have $u + 0 = u$
    $\langle 3\rangle 1$. LET: $u \in V$
    $\langle 3\rangle 2$. PICK $u' \in V$ such that $v + u' = u$
      PROOF: Axiom 3.
    $\langle 3\rangle 3$. $u + 0 = u$

$$
\begin{aligned}
u + 0 &= v + u' + 0 & (\langle 3\rangle 2)\\
&= v + u' & (\langle 2\rangle 2)\\
&= u & (\langle 3\rangle 2)
\end{aligned}
$$

$\langle 1 \rangle 2$. If $0, 0' \in V$ are such that $\forall v \in V.v + 0 = v$ and $\forall v \in V.v + 0' = v$, then $0 = 0'$.

    $\langle 2 \rangle 1$. LET: $0, 0' \in V$
    $\langle 2 \rangle 2$. ASSUME: $\forall v \in V.v + 0 = v$
    $\langle 2 \rangle 3$. ASSUME: $\forall v \in V.v + 0' = v$
    $\langle 2 \rangle 4$. $0 = 0'$

$$
\begin{aligned}
0 = 0 + 0' \qquad\qquad &(\langle 2 \rangle 2) \\
= 0' \qquad\qquad &(\langle 2 \rangle 3)
\end{aligned}
$$

$\square$

**Proposition 17.1.8.** *Let $V$ be a vector space. For any $v \in V$, there exists a unique $-v \in V$ such that $v + (-v) = 0$.*

PROOF:
$\langle 1 \rangle 1$. LET: $v \in V$
$\langle 1 \rangle 2$. There exists $-v \in V$ such that $v + (-v) = u$
    PROOF: Axiom 3.
$\langle 1 \rangle 3$. If $v + x = 0$ and $v + y = 0$ then $x = y$
    $\langle 2 \rangle 1$. ASSUME: $v + x = 0$
    $\langle 2 \rangle 2$. ASSUME: $v + y = 0$
    $\langle 2 \rangle 3$. $x = y$
      PROOF:

$$
\begin{aligned}
x = x + 0 \qquad\qquad &(\text{Proposition } 17.1.7) \\
= x + v + y \qquad\qquad &(\langle 2 \rangle 2) \\
= 0 + y \qquad\qquad &(\langle 2 \rangle 1) \\
= y \qquad\qquad &(\text{Proposition } 17.1.7)
\end{aligned}
$$

$\square$

**Proposition 17.1.9.** *Let $V$ be a vector space. For any $u, v \in V$, there exists a unique $u - v \in V$ such that $v + (u - v) = u$, namely $u - v = u + (-v)$.*

PROOF:
$\langle 1 \rangle 1$. LET: $u, v \in V$
$\langle 1 \rangle 2$. $v + (u + (-v)) = u$
    PROOF:

$$
\begin{aligned}
v + u + (-v) = u + 0 \qquad\qquad &(\text{Proposition } 17.1.8) \\
= u \qquad\qquad &(\text{Proposition } 17.1.7)
\end{aligned}
$$

$\langle 1 \rangle 3$. For all $x \in V$, if $v + x = u$ then $x = u + (-v)$.
    $\langle 2 \rangle 1$. LET: $x \in V$
    $\langle 2 \rangle 2$. ASSUME: $v + x = u$
    $\langle 2 \rangle 3$. $x = u + (-v)$
      PROOF:

$$
\begin{aligned}
u + (-v) = v + x + (-v) \qquad\qquad &(\langle 2 \rangle 2) \\
= x + 0 \qquad\qquad &(\text{Proposition } 17.1.8) \\
= x \qquad\qquad &(\text{Proposition } 17.1.7)
\end{aligned}
$$

☐

**Proposition 17.1.10.** *Let $V$ be a vector space over $K$. Let $u, v, w \in V$. If $u + v = u + w$ then $v = w$.*

PROOF:
⟨1⟩1. ASSUME: $u + v = u + w$
⟨1⟩2. $v = w$
   PROOF:

$$
\begin{aligned}
v &= v + 0 && \text{(Proposition 17.1.7)} \\
&= v + u + (-u) && \text{(Proposition 17.1.8)} \\
&= w + u + (-u) && (\langle 1 \rangle 1) \\
&= w + 0 && \text{(Proposition 17.1.8)} \\
&= w && \text{(Proposition 17.1.7)}
\end{aligned}
$$

**Proposition 17.1.11.** *Let $V$ be a vector space over $K$. Let $\lambda \in K$. Then $\lambda 0 = 0$.*

PROOF:
⟨1⟩1. $\lambda 0 + \lambda 0 = \lambda 0 + 0$
   PROOF:

$$
\begin{aligned}
\lambda 0 + \lambda 0 &= \lambda(0 + 0) && \text{(Axiom 6)} \\
&= \lambda 0 && \text{(Proposition 17.1.7)}
\end{aligned}
$$

⟨1⟩2. $\lambda 0 = 0$
   PROOF: Proposition 17.1.10.
☐

**Proposition 17.1.12.** *Let $V$ be a vector space over $K$. Let $\lambda \in K$ and $v \in V$. If $\lambda v = 0$ then $\lambda = 0$ or $v = 0$.*

PROOF:
⟨1⟩1. ASSUME: $\lambda \neq 0$
⟨1⟩2. ASSUME: $\lambda v = 0$
⟨1⟩3. $v = 0$
   PROOF:

$$
\begin{aligned}
v &= 1v && \text{(Axiom 7)} \\
&= \lambda^{-1}\lambda v \\
&= \lambda^{-1}0 && (\langle 1 \rangle 2) \\
&= 0
\end{aligned}
$$

☐

**Proposition 17.1.13.** *Let $V$ be a vector space over $K$. For all $v \in V$ we have $0v = 0$.*

PROOF:
⟨1⟩1. $0v + 0 = 0v + 0v$

$$0v + 0 = 0v \qquad \text{(Proposition 17.1.7)}$$
$$= (0 + 0)v$$
$$= 0v + 0v \qquad \text{(Axiom 5)}$$

⟨1⟩2. $0v = 0$
  PROOF: Proposition 17.1.10, ⟨1⟩1.

□

**Proposition 17.1.14.** *Let $V$ be a vector space over $K$. Let $v \in V$. Then $(-1)v = -v$.*

PROOF:
⟨1⟩1. $v + (-1)v = 0$
  PROOF:

$$v + (-1)v = 1v + (-1)v \qquad \text{(Axiom 7)}$$
$$= (1 + (-1))v \qquad \text{(Axiom 5)}$$
$$= 0v$$
$$= 0 \qquad \text{(Proposition 17.1.13)}$$

⟨1⟩2. Q.E.D.
  PROOF: Proposition 17.1.8.

□

## 17.2 Subspaces

**Definition 17.2.1** (Subspace)**.** Let $V$ be a vector space over $K$ and $U \subseteq V$. Then $U$ is a *subspace* of $V$ iff $\forall \alpha, \beta \in K.\forall u, v \in U.\alpha u + \beta v \in U$. It is a *proper* subspace iff in addition $U \neq V$.

**Proposition 17.2.2.** *Let $V$ be a vector space over $K$ and $U$ a subspace of $V$. Then $U$ is a vector space over $K$ under the restrictions of the operations of $V$.*

PROOF: Each of the axioms follows from the corresponding axiom in $V$. For axiom 3, we have if $u, v \in U$ then $v - u = 1v + (-1)u \in U$. □

**Proposition 17.2.3.** *Every vector space is a subspace of itself.*

PROOF: Trivial. □

**Proposition 17.2.4.** *Let $\Omega$ be a subset of $\mathbb{R}^N$. Let $\mathcal{C}(\Omega)$ be the set of all continuous functions $\Omega \to \mathbb{C}$. Then $\mathcal{C}(\Omega)$ is a subspace of $\mathbb{C}^\Omega$.*

PROOF: If $f, g : \Omega \to \mathbb{C}$ are continuous then so is $\alpha f + \beta g$. □

**Proposition 17.2.5.** *Let $\Omega$ be an open set in $\mathbb{R}^N$. Let $\mathcal{C}^k(\Omega)$ be the set of all continuous functions $\Omega \to \mathbb{C}$ with continuous partial derivatives of order $k$. Then $\mathcal{C}^k(\Omega)$ is a subspace of $\mathbb{C}^\Omega$.*

PROOF: If $f, g : \Omega \to \mathbb{C}$ have continuous partial derivatives of order $k$ then so does $\alpha f + \beta g$. □

**Proposition 17.2.6.** *Let $\Omega$ be an open set in $\mathbb{R}^N$. Let $\mathcal{C}^\infty(\Omega)$ be the set of all infinitely differentiable functions $\Omega \to \mathbb{C}$. Then $\mathcal{C}^\infty(\Omega)$ is a subspace of $\mathbb{C}^\Omega$.*

PROOF: If $f, g : \Omega \to \mathbb{C}$ are infinitely differentiable then so is $\alpha f + \beta g$. □

**Proposition 17.2.7.** *Let $\Omega$ be an open set in $\mathbb{R}^N$. Let $\mathcal{P}(\Omega)$ be the set of all polynomials in $N$ variables considered as functions $\Omega \to \mathbb{C}$. Then $\mathcal{P}(\Omega)$ is a subspace of $\mathbb{C}^\Omega$.*

PROOF: If $f, g : \Omega \to \mathbb{C}$ are polynomials in $N$ variables then so is $\alpha f + \beta g$. □

**Proposition 17.2.8.** *Let $V$ be a vector space and $U_1$, $U_2$ subspaces of $V$. If $U_1 \subseteq U_2$ then $U_1$ is a subspace of $U_2$.*

PROOF: Trivial. □

**Proposition 17.2.9.** *Let $V$ be a vector space over $K$ . The intersection of a set of subspaces of $V$ is a subspace of $V$.*

PROOF:
$\langle 1 \rangle 1$. LET: $\mathcal{U}$ be a set of subspaces of $V$.
$\langle 1 \rangle 2$. LET: $u, v \in \bigcap \mathcal{U}$ and $\lambda, \mu \in K$
$\langle 1 \rangle 3$. $\lambda u + \mu v \in \bigcap \mathcal{U}$
   $\langle 2 \rangle 1$. LET: $U \in \mathcal{U}$
   $\langle 2 \rangle 2$. $u, v \in U$
      PROOF: $\langle 1 \rangle 2$, $\langle 2 \rangle 1$.
   $\langle 2 \rangle 3$. $\lambda u + \beta v \in U$
      PROOF: $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$.
□

**Proposition 17.2.10.** *The set of all bounded complex sequences is a proper subspace of $\mathbb{C}^\mathbb{N}$.*

PROOF: If $(x_n)$ and $(y_n)$ are bounded then so is $(\lambda x_n + \mu y_n)$. □

**Proposition 17.2.11.** *The set of all convergent complex sequences is a proper subspace of the space of all bounded complex sequences.*

PROOF: If $(x_n)$ and $(y_n)$ converge then so does $(\lambda x_n + \mu y_n)$. □

**Proposition 17.2.12.** *The set $l^p$ of all sequences $(x_n)$ in $\mathbb{C}$ such that $\sum_n |x_n|^p < \infty$ is a subspace of $\mathbb{C}^\mathbb{N}$.*

PROOF: It is closed under addition by Proposition 16.0.2, and it is easy to see that it is closed under scalar multiplication. □

## 17.3   Linear Independence and Bases

**Definition 17.3.1** (Linear Combination)**.** Let $V$ be a vector space over $K$. Let $v, v_1, \ldots, v_n \in V$. Then $v$ is a *linear combination* of $v_1$, ..., $v_n$ iff there exist scalars $\lambda_1, \ldots, \lambda_n \in K$ such that

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \ .$$

**Definition 17.3.2** (Linearly Independent)**.** Let $V$ be a vector space over $K$. Let $A \subseteq V$. Then $A$ is *linearly independent* iff, for all $\lambda_1, \ldots, \lambda_n \in K$ and $v_1, \ldots, v_n \in A$, if $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ then $\lambda_1 = \cdots = \lambda_n = 0$.

**Definition 17.3.3** (Span)**.** Let $V$ be a vector space over $K$ and $A \subseteq V$. The *span* of $A$, or the subspace of $V$ *spanned* by $A$, is the set of all linear combinations of vectors in $A$.

**Proposition 17.3.4.** *Let $V$ be a vector space over $K$ and $A \subseteq V$. Then* $\operatorname{span} A$ *is a subspace of $V$.*

PROOF: Given $\alpha, \beta \in K$ and $\lambda_1 u_1 + \cdots + \lambda_m u_m, \mu_1 v_1 + \cdots + \mu_n v_n \in \operatorname{span} A$, we have

$$\alpha(\lambda_1 u_1 + \cdots + \lambda_m u_m) + \beta(\mu_1 v_1 + \cdots + \mu_n v_n)$$
$$= \alpha\lambda_1 u_1 + \cdots + \alpha\lambda_m u_m + \beta\mu_1 v_1 + \cdots + \beta\mu_n v_n$$
$$\in \operatorname{span} A \qquad \qquad \qquad \square$$

**Definition 17.3.5** (Basis)**.** Let $V$ be a vector space over $K$ and $B \subseteq V$. Then $B$ is a *basis* for $V$ iff $B$ is linearly independent and $\operatorname{span} B = V$.

**Definition 17.3.6** (Finite Dimensional)**.** A vector space is *finite dimensional* iff there exists a finite basis; otherwise it is *infinite dimensional.*

**Proposition 17.3.7.** *In a finite dimensional space, any two bases have the same size.*

TODO

**Definition 17.3.8** (Dimension)**.** The *dimension* of a finite dimensional vector space $V$, $\dim V$, is the number of vectors in any basis.

**Proposition 17.3.9.** *Let $K$ be either $\mathbb{R}$ or $\mathbb{C}$. Then $K^n$ as a vector space over $K$ has dimension $n$.*

PROOF: The vectors with one component 1 and all other components 0 form a basis. $\square$

**Proposition 17.3.10.** *As a real vector space, $\mathbb{C}^n$ has dimension $2n$.*

PROOF: The vectors with one component either 1 or $i$ and all other components 0 form a basis. $\square$

**Proposition 17.3.11.** *Let $\Omega$ be a nonempty open set in $\mathbb{R}^n$. The space $\mathcal{C}(\Omega)$ is infinite dimensional.*

PROOF: Let $\pi_1 : \mathbb{R}^n \to \mathbb{R}$ be the first projection. The functions $1$, $\pi_1(x)$, $\pi_1(x)^2$, $\pi_1(x)^3$, ... form an infinite linearly independent set in $\mathcal{C}(\Omega)$. □

**Proposition 17.3.12.** *The spaces $\mathcal{C}^k(\mathbb{R}^n)$ and $\mathcal{C}^\infty(\mathbb{R}^n)$ are infinite dimensional.*

PROOF: The monomials $1$, $x$, $x^2$, ... form an infinite linearly independent set. □

## 17.4   Linear Mappings

**Definition 17.4.1** (Kernel)**.** Let $U$ and $V$ be vector spaces and $T : U \to V$. The *kernel* of $T$ is
$$\ker T := \{u \in U \mid T(u) = 0\} \ .$$

**Definition 17.4.2** (Linear Mapping)**.** Let $U$ and $V$ be vector spaces over $K$. A function $L : U \to V$ is a *linear mapping* iff $\forall x, y \in U.\forall \alpha, \beta \in K.L(\alpha x + \beta y) = \alpha L(x) + \beta L(y)$.

**Proposition 17.4.3.** *Let $U$ and $V$ be vector spaces over $K$. The set of linear mappings from $U$ to $V$ is a subspace of $V^U$.*

## 17.5   Eigenvalues and Eigenvectors

**Definition 17.5.1** (Eigenvalue and Eigenvector)**.** Let $V$ be a vector space over $K$. Let $A : V \to V$ be a linear transformation. Let $v \in V$ and $\lambda \in K$. Then $v$ is an *eigenvector* of $A$ with *eigenvalue* $\lambda$ iff $A(v) = \lambda v$.

# Chapter 18

# Normed Spaces

**Definition 18.0.1** (Norm)**.** Let $K$ be either $\mathbb{R}$ or $\mathbb{C}$. Let $V$ be a vector space over $K$. A *norm* on $V$ is a function $\| \ \| : V \to \mathbb{R}$ such that, for all $u, v \in V$ and $\lambda \in K$:

1. If $\|v\| = 0$ then $v = 0$.

2. $\|\lambda v\| = |\lambda| \|v\|$

3. (*Triangle Inequality*) $\|u + v\| \le \|u\| + \|v\|$

A *normed space* over $K$ is a pair $(V, \| \ \|)$ where $V$ is a vector space over $K$ and $\| \ \|$ is a norm on $V$.

**Proposition 18.0.2.** *In a normed space, $\|0\| = 0$.*

PROOF: $\|0\| = |0| \|0\| = 0$ by Axiom 2. $\square$

**Proposition 18.0.3.** *Let $V$ be a normed vector space over $K$. For all $v \in V$ we have $\|v\| \ge 0$.*

PROOF:
$$
\begin{aligned}
0 &= \|0\| & \text{(Proposition 18.0.2)} \\
&= \|v - v\| \\
&\le \|v\| + \| - v\| & \text{(Triangle Inequality)} \\
&= 2\|v\| & \text{(Axiom 2)}
\end{aligned}
$$

**Proposition 18.0.4.** *Let $V$ be a normed space. Let $u, v \in V$. Then*

$$\big| \|u\| - \|v\| \big| \le \|u - v\| \ .$$

PROOF:

$$\|u\| \leq \|u - v\| + \|v\| \qquad \text{(Triangle Inequality)}$$
$$\therefore \|u\| - \|v\| \leq \|u - v\|$$
$$\|v\| \leq \|v - u\| + \|u\| \qquad \text{(Triangle Inequality)}$$
$$= \|u - v\| + \|u\| \qquad \text{(Axiom 2)}$$
$$\therefore \|v\| - \|u\| \leq \|u - v\|$$

**Definition 18.0.5** (Euclidean Norm)**.** The *Euclidean norm* on $K^n$ is defined by

$$\|(x_1, \ldots, x_n)\| = \sqrt{|x_1|^2 + \cdots + |x_n|^2} \ .$$

**Proposition 18.0.6.** *The Euclidean norm on $K^n$ is a norm.*

PROOF:
$\langle 1 \rangle 1.$ If $\|\vec{x}\| = 0$ then $\vec{x} = \vec{0}$
  PROOF: If $\sqrt{|x_1|^2 + \cdots + |x_n|^2} = 0$ then $x_1 = \cdots = x_n = 0$.
$\langle 1 \rangle 2.$ $\|\lambda \vec{x}\| = |\lambda| \|\vec{x}\|$
  PROOF:

$$\|\lambda \vec{x}\| \sqrt{|\lambda x_1|^2 + \cdots + |\lambda x_n|^2}$$
$$= \sqrt{|\lambda|^2 |x_1|^2 + \cdots + |\lambda|^2 |x_n|^2}$$
$$= |\lambda| \sqrt{|x_1|^2 + \cdots + |x_n|^2}$$
$$= |\lambda| \|\vec{x}\|$$

$\langle 1 \rangle 3.$ $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$
  PROOF:

$$\|\vec{u} + \vec{v}\|^2 = |u_1 + v_1|^2 + \cdots + |u_n + v_n|^2$$
$$= |u_1|^2 + \cdots + |u_n|^2 + |v_1|^2 + \cdots + |v_n|^2$$
$$+ 2|u_1||v_1| + \cdots + 2|u_n||v_n|$$
$$\leq \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2|u_1 v_1 + \cdots + u_n v_n|$$
$$\leq \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2\|\vec{u}\|\|\vec{v}\| \qquad \text{(Cauchy-Schwarz)}$$
$$= (\|\vec{u}\| + \|\vec{v}\|)^2$$

□

**Corollary 18.0.6.1.** *The absolute value function $|\ |$ is a norm on $K$.*

**Proposition 18.0.7.** *The function $\|\vec{x}\| = |x_1| + \cdots + |x_n|$ is a norm on $\mathbb{C}^n$.*

PROOF:
$\langle 1 \rangle 1.$ If $\|\vec{x}\| = 0$ then $\vec{x} = \vec{0}$
  PROOF: If $|x_1| + \cdots + |x_n| = 0$ then $x_1 = \cdots = x_n = 0$.
$\langle 1 \rangle 2.$ $\|\lambda \vec{x}\| = |\lambda| \|\vec{x}\|$

PROOF:
$$\|\lambda\vec{x}\||\lambda x_1| + \cdots + |\lambda x_n|$$

$$= |\lambda|(|x_1| + \cdots + |x_n|)$$
$$= |\lambda|\|\vec{x}\|$$

$\langle 1\rangle 3.$ $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$
  PROOF:
$$\|\vec{u} + \vec{v}\|^2 = |u_1 + v_1| + \cdots + |u_n + v_n|$$
$$\leq |u_1| + |v_1| + \cdots + |u_n| + |v_n|$$
$$= \|\vec{u}\| + \|\vec{v}\|$$

□

**Proposition 18.0.8.** *The function $\|\vec{x}\| = \max(|x_1|, \ldots, |x_n|)$ is a norm on $\mathbb{C}^n$.*

PROOF:
$\langle 1\rangle 1.$ If $\|\vec{x}\| = 0$ then $\vec{x} = \vec{0}$
  PROOF: If $\max(|x_1|, \ldots, |x|n|) = 0$ then $x_1 = \cdots = x_n = 0$.
$\langle 1\rangle 2.$ $\|\lambda\vec{x}\| = |\lambda|\|\vec{x}\|$
  PROOF:
$$\|\lambda\vec{x}\| = \max(|\lambda x_1|, \ldots, |\lambda x_n|)$$
$$= |\lambda| \max(|x_1|, \ldots, |x_n|)$$
$$= |\lambda|\|\vec{x}\|$$
$\langle 1\rangle 3.$ $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$
  PROOF:
$$\|\vec{u} + \vec{v}\| = \max(|u_1 + v_1|, \ldots, |u_n + v_n|)$$
$$\leq \max(|u_1| + |v_1|, \ldots, |u_n| + |v_n|)$$
$$\leq \max(|u_1|, \ldots, |u_n|) + \max(|v_1|, \ldots, |v_n|)$$

□

**Definition 18.0.9** (Uniform Convergence Norm)**.** Let $\Omega$ be a closed bounded subset of $\mathbb{R}^n$. The *uniform convergence norm* on $\mathcal{C}(\Omega)$ is the function defined by $\|f\| = \max_{x \in \Omega} |f(x)|$.

**Proposition 18.0.10.** *Let $\Omega$ be a closed bounded subset of $\mathbb{R}^n$. The uniform convergence norm is a norm on $\mathcal{C}(\Omega)$.*

PROOF:
$\langle 1\rangle 1.$ If $\|f\| = 0$ then $f = 0$
  PROOF: If $\max_x |f(x)| = 0$ then $f(x) = 0$ for all $x$.
$\langle 1\rangle 2.$ $\|\lambda f\| = |\lambda|\|f\|$
  PROOF:
$$\|\lambda f\| = \max_x |\lambda f(x)|$$
$$= |\lambda| \max_x |f(x)|$$
$$= |\lambda|\|f\|$$

$\langle 1 \rangle 3.$ $\|f + g\| \le \|f\| + \|g\|$
 PROOF:

$$\|f + g\| = \max_x |f(x) + g(x)|$$
$$\le \max_x (|f(x)| + |g(x)|)$$
$$\le \max_x |f(x)| + \max_x |g(x)|$$
$$= \|f\| + \|g\|$$

$\square$

**Proposition 18.0.11.** *Let $p \ge 1$. The function $\|(z_n)\| = (\sum_{n=1}^{\infty} |z_n|^p)^{1/p}$ is a norm on $l^p$.*

PROOF:
$\langle 1 \rangle 1.$ If $\|(z_n)\| = 0$ then $(z_n) = (0)$
 PROOF: If $(\sum_n |z_n|^p)^{1/p} = 0$ then $\sum_n |z_n|^p = 0$ so $|z_n|^p = 0$ for all $n$, and so $z_n = 0$ for all $n$.
$\langle 1 \rangle 2.$ $\|(\lambda z_n)\| = |\lambda| \|(z_n)\|$
 PROOF:

$$\|(\lambda z_n)\| = \left( \sum_n |\lambda z_n|^p \right)^{1/p}$$
$$= |\lambda| \left( \sum_n |z_n|^p \right)^{1/p}$$
$$= |\lambda| |(z_n)|$$

$\langle 1 \rangle 3.$ The triangle inequality holds.
PROOF: This is Minkowski's Inequality. $\square$

**Proposition 18.0.12.** *Let $V$ be a normed space and $U$ a vector subspace of $V$. Then $U$ is a normed space under the restriction of the norm to $U$.*

PROOF: Each axiom follows from the fact it holds in $V$. $\square$

**Proposition 18.0.13.** *Let $V$ be a normed space over $K$. Let $x_1$, ..., $x_n$ be linearly independent elements of $V$. Then there exists a real number $c > 0$ such that, for all $\alpha_1, \ldots, \alpha_n \in K$, we have*

$$\|\alpha_1 x_1 + \cdots + \alpha_n x_n\| \ge c(|\alpha_1| + \cdots + |\alpha_n|) \ .$$

PROOF:
$\langle 1 \rangle 1.$ Define $f : K^n \to \mathbb{R}$ by
$$f(\alpha_1, \ldots, \alpha_n) = \|\alpha_1 x_1 + \cdots + \alpha_n x_n\|$$
$\langle 1 \rangle 2.$ $f$ is continuous.
 $\langle 2 \rangle 1.$ LET: $(\alpha_1, \ldots, \alpha_n) \in K^n$ and $\epsilon > 0$
 $\langle 2 \rangle 2.$ LET: $\delta = \epsilon / (\|x_1\| + \cdots + \|x_n\|)$
  PROOF: $x_1$, ..., $x_n$ are not all zero because they are linearly independent.
 $\langle 2 \rangle 3.$ LET: $(\beta_1, \ldots, \beta_n)$ with $|\alpha_i - \beta_i| < \delta$ for all $i$

$\langle 2 \rangle 4.$ $\|(\alpha_1 x_1 + \cdots + \alpha_n x_n) - (\beta_1 x_1 + \beta_n x_n)\| < \epsilon$
    PROOF:

$$\|(\alpha_1 x_1 + \cdots + \alpha_n x_n) - (\beta_1 x_1 + \beta_n x_n)\|$$

$$\leq |\alpha_1 - \beta_1|\|x_1\| + \cdots + |\alpha_n - \beta_n|\|x_n\| \qquad \text{(Axioms 2 and 3)}$$

$$< \delta(\|x_1\| + \cdots + \|x_n\|) \qquad\qquad\qquad (\langle 2 \rangle 3)$$

$$= \epsilon \qquad\qquad\qquad\qquad\qquad\qquad (\langle 2 \rangle 2)$$

$\langle 1 \rangle 3.$ PICK $(\beta_1, \ldots, \beta_n) \in \{(\beta_1, \ldots, \beta_n) \in K^n \mid |\beta_1| + \cdots + |\beta_n| = 1\}$ at which
    $f$ attains its minimum.
  PROOF: Extreme Value Theorem.
$\langle 1 \rangle 4.$ Let $c = f(\beta_1, \ldots, \beta_n)$
$\langle 1 \rangle 5.$ $c > 0$
  PROOF: Linear independence.
$\langle 1 \rangle 6.$ LET: $\alpha_1, \ldots, \alpha_n \in K$
$\langle 1 \rangle 7.$ $\|\alpha_1 x_1 + \cdots + \alpha_n x_n\| \geq c(|\alpha_1| + \cdots + |\alpha_n|)$
  $\langle 2 \rangle 1.$ ASSUME: w.l.o.g. $\alpha_1 \ldots, \alpha_n$ are not all zero.
  $\langle 2 \rangle 2.$ LET: $\beta_i = \alpha_i / (|\alpha_1| + \cdots + |\alpha_n|)$ for $i = 1, \ldots, n$
  $\langle 2 \rangle 3.$ $|\beta_1| + \cdots + |\beta_n| = 1$
  $\langle 2 \rangle 4.$ $f(\beta_1, \ldots, \beta_n) \geq c$
  $\langle 2 \rangle 5.$ Q.E.D.
    PROOF: Multiply both sides by $|\alpha_1| + \cdots + |\alpha_n|$.
☐

**Proposition 18.0.14.** *Let $V$ be a normed space over $K$. Define $d : V^2 \to \mathbb{R}$ by $d(x, y) = \|x - y\|$. Then $d$ is a metric on $V$.*

PROOF:
$\langle 1 \rangle 1.$ For all $x, y \in V$ we have $d(x, y) \geq 0$
  PROOF: Proposition 18.0.3.
$\langle 1 \rangle 2.$ For all $x, y \in V$ we have $d(x, y) = 0$ iff $x = y$
  $\langle 2 \rangle 1.$ If $d(x, y) = 0$ then $x = y$
    PROOF: Axiom 1.
  $\langle 2 \rangle 2.$ If $x = y$ then $d(x, y) = 0$
    PROOF: Proposition 18.0.2.
$\langle 1 \rangle 3.$ $\forall x, y \in V . d(x, y) = d(y, x)$
  PROOF: By Axiom 2.
$\langle 1 \rangle 4.$ $\forall x, y, z \in V . d(x, z) \leq d(x, y) + d(y, z)$
  PROOF: By Axiom 3.
☐

Henceforth we identify any normed space with this metric space.

## 18.1 Convergence

**Proposition 18.1.1.** *Let $V$ be a normed space over $K$. Let $(x_n)$ be a sequence in $V$ and $l \in V$. Then $x_n \to l$ as $n \to \infty$ in $V$ if and only if $\|x_n - l\| \to 0$ as $n \to \infty$ in $\mathbb{R}$.*

PROOF: Immediate from definitions. □

**Proposition 18.1.2.** *In a normed space, a sequence has at most one limit.*

PROOF:
$\langle 1 \rangle 1$.  LET: $V$ be a vector space over $K$.
$\langle 1 \rangle 2$.  ASSUME: $x_n \to l$ and $x_n \to m$ as $n \to \infty$.
$\langle 1 \rangle 3$.  ASSUME: for a contradiction $l \neq m$
$\langle 1 \rangle 4$.  LET: $\epsilon = \|l - m\|/2$
$\langle 1 \rangle 5$.  PICK $N$ such that $\forall n \geq N.\|x_n - l\| < \epsilon$ and $\forall n \geq N.\|x_n - m\| < \epsilon$
    PROOF: $\langle 1 \rangle 2$, $\langle 1 \rangle 4$
$\langle 1 \rangle 6$.  $\|l - m\| < \|l - m\|$
    PROOF:
$$\|l - m\| \leq \|x_N - l\| + \|x_N - m\| \qquad \text{(Triangle Inequality)}$$
$$< 2\epsilon \qquad\qquad (\langle 1 \rangle 5)$$
$$= \|l - m\| \qquad\qquad (\langle 1 \rangle 4$$
$\langle 1 \rangle 7$.  Q.E.D.
    PROOF: This is a contradiction.
□

**Definition 18.1.3** (Bounded)**.** Let $V$ be a normed space over $K$. A sequence $(x_n)$ in $V$ is *bounded* iff there exists $B$ such that $\forall n \leq N.\|x_n\| < B$.

**Proposition 18.1.4.** *Every convergent sequence is bounded.*

PROOF:
$\langle 1 \rangle 1$.  LET: $x_n \to l$ as $n \to \infty$
$\langle 1 \rangle 2$.  PICK $N$ such that $\forall n \geq N.\|x_n - l\| < 1$
$\langle 1 \rangle 3$.  LET: $B = \max(\|x_1\|, \|x_2\|, \ldots, \|x_{N-1}\|, \|l\| + 1)$
$\langle 1 \rangle 4$.  LET: $n \in \mathbb{N}$
$\langle 1 \rangle 5$.  $\|x_n\| \leq B$
    $\langle 2 \rangle 1$.  CASE: $n < N$
        PROOF: $\|x_n\| \leq B$ from $\langle 1 \rangle 3$.
    $\langle 2 \rangle 2$.  CASE: $n \geq N$
        PROOF:
$$\|x_n\| \leq \|l\| + \|x_n - l\| \qquad \text{(Triangle Inequality)}$$
$$< \|l\| + 1 \qquad\qquad (\langle 1 \rangle 2)$$
$$\leq B \qquad\qquad (\langle 1 \rangle 3)$$
□

**Proposition 18.1.5.** *Let $V$ be a normed space over $K$. If $x_n \to l$ as $n \to \infty$ in $V$, and $\lambda_n \to \lambda$ as $n \to \infty$ in $K$, then $\lambda_n x_n \to \lambda l$ as $n \to \infty$.*

PROOF:
$\langle 1 \rangle 1$.  LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2$.  LET: $x_n \to l$ as $n \to \infty$
$\langle 1 \rangle 3$.  LET: $\lambda_n \to \lambda$ as $n \to \infty$

$\langle 1 \rangle 4$. LET: $\epsilon > 0$

$\langle 1 \rangle 5$. PICK $N$ such that, for all $n \geq N$, we have $\|x_n - l\| < \epsilon/2|\lambda|$ and $|\lambda_n - \lambda| < \sqrt{\epsilon/2}$ and $\|x_n\| < \sqrt{\epsilon/2}$

$\langle 1 \rangle 6$. LET: $n \geq N$

$\langle 1 \rangle 7$. $\|\lambda_n x_n - \lambda l\| < \epsilon$

PROOF:

$$\begin{aligned}
\|\lambda_n x_n - \lambda l\| &\leq \|\lambda_n x_n - \lambda x_n\| + \|\lambda x_n - \lambda l\| && \text{(Triangle Inequality)} \\
&= |\lambda_n - \lambda|\|x_n\| + |\lambda|\|x_n - l\| && \text{(Axiom 2)} \\
&< \sqrt{\epsilon/2}\sqrt{\epsilon/2} + |\lambda|\epsilon/2|\lambda| && (\langle 1 \rangle 5) \\
&= \epsilon
\end{aligned}$$

☐

**Proposition 18.1.6.** *Let $V$ be a normed space over $K$. If $x_n \to l$ and $y_n \to m$ as $n \to \infty$, then $x_n + y_n \to l + m$ as $n \to \infty$.*

PROOF:

$\langle 1 \rangle 1$. LET: $\epsilon > 0$

$\langle 1 \rangle 2$. PICK $N$ such that, for all $n \geq N$, we have $\|x_n - l\| < \epsilon/2$ and $\|y_n - m\| < \epsilon/2$

$\langle 1 \rangle 3$. LET: $n \geq N$

$\langle 1 \rangle 4$. $\|(x_n + y_n) - (l + m)\| < \epsilon$

PROOF:

$$\begin{aligned}
\|(x_n + y_n) - (l + m)\| &\leq \|x_n - l\| + \|y_n - m\| && \text{(Triangle Inequality)} \\
&< \epsilon/2 + \epsilon/2 && (\langle 1 \rangle 2) \\
&= \epsilon
\end{aligned}$$

☐

**Definition 18.1.7** (Uniform Convergence)**.** Let $\Omega$ be a closed bounded subset of $\mathbb{R}^n$. Let $(f_n)$ be a sequence in $\mathcal{C}(\Omega)$ and $f \in \mathcal{C}(\Omega)$. Then $(f_n)$ *converges uniformly* to $f$ iff, for every $\epsilon > 0$, there exists $N$ such that $\forall x \in \Omega. \forall n \geq N.|f_n(x) - f(x)| < \epsilon$.

**Proposition 18.1.8.** *Let $\Omega$ be a closed bounded subset of $\mathbb{R}^n$. Let $(f_n)$ be a sequence in $\mathcal{C}(\Omega)$ and $f \in \mathcal{C}(\Omega)$. Then $(f_n)$ converges uniformly to $f$ iff $f_n$ converges to $f$ under the uniform convergence norm.*

PROOF:

$(f_n)$ converges to $f$ under the uniform convergence norm

$\Leftrightarrow \forall \epsilon > 0. \exists N. \forall n \geq N. \|f_n - f\| < \epsilon$

$\Leftrightarrow \forall \epsilon > 0. \exists N. \forall n \geq N. \forall x \in X.|f_n(x) - f(x)| < \epsilon$     ☐

**Definition 18.1.9** (Pointwise Convergence)**.** Let $(f_n)$ be a sequence in $\mathcal{C}([0,1])$ and $f \in \mathcal{C}([0,1])$. Then $(f_n)$ *converges pointwise* to $f$ iff, for all $t \in [0,1]$, we have $|f_n(t) - f(t)| \to 0$ as $n \to \infty$.

**Proposition 18.1.10.** *There is no norm $n$ on $\mathcal{C}([0,1])$ such that, for every sequence $(f_n)$ and function $f$ in $\mathcal{C}([0,1])$, we have $(f_n)$ converges pointwise to $f$ if and only if $(f_n)$ converges to $f$ under $n$.*

PROOF:

⟨1⟩1. ASSUME: for a contradiction $\| \ \|$ is a norm on $\mathcal{C}([0,1])$ such that, for every sequence $(f_n)$ and function $f$ in $\mathcal{C}([0,1])$, we have $(f_n)$ converges pointwise to $f$ if and only if $(f_n)$ converges to $f$ under $\| \ \|$.

⟨1⟩2. For $n \in \mathbb{Z}_+$, define $g_n \in \mathcal{C}([0,1])$ by

$$g_n(t) = \begin{cases} 2^n t & \text{if } 0 \le t \le 2^{-n} \\ 2 - 2^n t & \text{if } 2^{-n} \le t \le 2^{1-n} \\ 0 & \text{if } 2^{1-n} \le t \le 1 \end{cases}$$

⟨1⟩3. For all $n$, $\|g_n\| \ne 0$

   PROOF: Axiom 1.

⟨1⟩4. For $n \in \mathbb{Z}_+$, define $f_n \in \mathcal{C}([0,1])$ by $f_n = g_n / \|g_n\|$

⟨1⟩5. For all $n$, $\|f_n\| = 1$

   PROOF: Axiom 2.

⟨1⟩6. $(f_n)$ does not converge under $\| \ \|$

⟨1⟩7. $(f_n)$ converges pointwise to 0.

⟨1⟩8. This is a contradiction.

□

**Definition 18.1.11** (Equivalence of Norms)**.** Let $\| \ \|_1$ and $\| \ \|_2$ be two norms on the same vector space $V$. Then the norms are *equivalent* if and only if, for any sequence $(x_n)$ in $V$ and $l \in V$, we have that $(x_n)$ converges to $l$ under $\| \ \|_1$ if and only if $(x_n)$ converges to $l$ under $\| \ \|_2$.

**Theorem 18.1.12.** *Let $\| \ \|_1$ and $\| \ \|_2$ be two norms on the same vector space $E$ over $K$. Then $\| \ \|_1$ and $\| \ \|_2$ are equivalent if and only if there exist positive real numbers $\alpha$ and $\beta$ such that, for all $x \in E$,*

$$\alpha \|x\|_1 \le \|x\|_2 \le \beta \|x\|_1 \ .$$

PROOF:

⟨1⟩1. If $\| \ \|_1$ and $\| \ \|_2$ are equivalent then there exist positive real numbers $\alpha$ and $\beta$ such that, for all $x \in E$, $\alpha \|x\|_1 \le \|x\|_2 \le \beta \|x\|_1$.

  ⟨2⟩1. ASSUME: $\| \ \|_1$ and $\| \ \|_2$ are equivalent.

  ⟨2⟩2. There exists $\alpha > 0$ such that, for all $x \in E$, we have $\alpha \|x\|_1 \le \|x\|_2$

    ⟨3⟩1. ASSUME: for a contradiction there is no $\alpha > 0$ such that, for all $x \in E$, we have $\alpha \|x\|_1 \le \|x\|_2$.

    ⟨3⟩2. For all $n \in \mathbb{Z}_+$, PICK $x_n \in E$ such that $1/n \|x_n\|_1 > \|x\|_2$

    ⟨3⟩3. For all $n \in \mathbb{Z}_+$,

      LET:

$$y_n = \frac{1}{\sqrt{n}} \frac{x_n}{\|x_n\|_2}$$

    ⟨3⟩4. $(y_n)$ converges to 0 under $\| \ \|_2$

    ⟨3⟩5. $(y_n)$ converges to 0 under $\| \ \|_1$

    ⟨3⟩6. For all $n \in \mathbb{Z}_+$, we have $\|y_n\| > \sqrt{n}$

    ⟨3⟩7. This is a contradiction.

  ⟨2⟩3. There exists $\beta > 0$ such that, for all $x \in E$, we have $\|x\|_2 \le \beta \|x\|_1$

    PROOF: Similar.

$\langle 1 \rangle 2$. If there exist positive real numbers $\alpha$ and $\beta$ such that, for all $x \in E$, $\alpha \|x\|_1 \le \|x\|_2 \le \beta \|x\|_1$. then $\| \ \|_1$ and $\| \ \|_2$ are equivalent.

    $\langle 2 \rangle 1$. ASSUME: $\alpha$ and $\beta$ are positive reals with $\forall x \in E.\alpha \|x\|_1 \le \|x\|_2 \le \beta \|x\|_1$.

    $\langle 2 \rangle 2$. Let $(x_n)$ be a sequence in $E$ and $l \in E$

    $\langle 2 \rangle 3$. If $(x_n)$ converges to $l$ under $\| \ \|_1$ then $(x_n)$ converges to $l$ under $\| \ \|_2$.

        $\langle 3 \rangle 1$. ASSUME: $(x_n)$ converges to $l$ under $\| \ \|_1$

        $\langle 3 \rangle 2$. LET: $\epsilon > 0$

        $\langle 3 \rangle 3$. PICK $N$ such that $\forall n \ge N.\|x_n - l\|_1 < \epsilon/\beta$

        $\langle 3 \rangle 4$. $\forall n \ge N.\|x_n - l\|_2 < \epsilon$

    $\langle 2 \rangle 4$. If $(x_n)$ converges to $l$ under $\| \ \|_2$ then $(x_n)$ converges to $l$ under $\| \ \|_1$.

    PROOF: Similar.

□

**Theorem 18.1.13.** *Any two norms on a finite dimensional vector space are equivalent.*

PROOF:

$\langle 1 \rangle 1$. LET: $V$ be a finite dimensional vector space over $K$.

$\langle 1 \rangle 2$. ASSUME: w.l.o.g. $\dim V > 0$

$\langle 1 \rangle 3$. PICK a basis $\{e_1, \dots, e_n\}$ for $V$.

$\langle 1 \rangle 4$. LET: $\| \ \|_0 : V \to \mathbb{R}$ be the function: $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\|_0 = |\alpha_1| + \cdots + |\alpha_n|$.

$\langle 1 \rangle 5$. $\| \ \|_0$ is a norm.

    $\langle 2 \rangle 1$. If $\|v\|_0 = 0$ then $v = 0$

    PROOF: If $|\alpha_1| + \cdots + |\alpha_n| = 0$ then $\alpha_1 = \cdots = \alpha_n = 0$ so $\alpha_1 e_1 + \cdots + \alpha_n e_n = 0$.

    $\langle 2 \rangle 2$. $\|\lambda v\|_0 = |\lambda| \|v\|_0$

    PROOF:

$$\|\lambda(\alpha_1 e_1 + \cdots + \alpha_n e_n)\|_0 = \|\lambda \alpha_1 e_1 + \cdots + \lambda \alpha_n e_n\|_0$$
$$= |\lambda \alpha_1| + \cdots + |\lambda \alpha_n| \qquad (\langle 1 \rangle 4)$$
$$= |\lambda|(|\alpha_1| + \cdots + |\alpha_n|)$$
$$= |\lambda| \|\alpha_1 e_1 + \cdots + \alpha_n e_n\|_0 \qquad (\langle 1 \rangle 4)$$

    $\langle 2 \rangle 3$. $\|u + v\|_0 \le \|u\|_0 + \|v\|_0$

    PROOF:

$$\|(\alpha_1 e_1 + \cdots + \alpha_n e_n) + (\beta_1 e_1 + \cdots + \beta_n e_n)\| = |\alpha_1 + \beta_1| + \cdots + |\alpha_n + \beta_n|$$
$$\le |\alpha_1| + \cdots + |\alpha_n| + |\beta_1| + \cdots + |\beta_n|$$
$$= \|\alpha_1 e_1 + \cdots + \alpha_n e_n\|_0 + \|\beta_1 e_1 + \cdots + \beta_n e_n\|_0$$

$\langle 1 \rangle 6$. Any norm on $V$ is equivalent to $\| \ \|_0$.

    $\langle 2 \rangle 1$. LET: $\| \ \|$ be any norm on $V$.

    $\langle 2 \rangle 2$. PICK $\alpha > 0$ such that, for all $\alpha_1, \dots, \alpha_n \in K$, we have $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\| \ge \alpha(|\alpha_1| + \cdots + |\alpha_n|)$

    PROOF: Proposition 18.0.13, $\langle 2 \rangle 1$, $\langle 1 \rangle 3$.

    $\langle 2 \rangle 3$. LET: $\beta = \max(\|e_1\|, \dots, \|e_n\|)$

    $\langle 2 \rangle 4$. $\beta > 0$

    PROOF: $e_1, \dots, e_n$ cannot all be zero by $\langle 1 \rangle 3$.

$\langle 2 \rangle 5$. For all $x \in V$ we have $\alpha \|x\|_0 \leq \|x\| \leq \beta \|x\|_0$

$\quad \langle 3 \rangle 1$. LET: $x \in V$

$\quad \langle 3 \rangle 2$. $\alpha \|x\|_0 \leq \|x\|$

$\quad\quad$ PROOF: $\langle 1 \rangle 3$, $\langle 1 \rangle 4$, $\langle 2 \rangle 2$.

$\quad \langle 3 \rangle 3$. $\|x\| \leq \beta \|x\|_0$

$\quad\quad \langle 4 \rangle 1$. LET: $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$

$\quad\quad \langle 4 \rangle 2$. Q.E.D.

$\quad\quad\quad$ PROOF:

$$
\begin{aligned}
\|x\| &= \|\alpha_1 e_1 + \cdots + \alpha_n e_n\| && (\langle 4 \rangle 1) \\
&\leq |\alpha_1| \|e_1\| + \cdots + |\alpha_n| \|e_n\| && (\langle 2 \rangle 1) \\
&\leq \beta(|\alpha_1| + \cdots + |\alpha_n|) && (\langle 2 \rangle 3) \\
&= \beta \|x\|_0 && (\langle 1 \rangle 4)
\end{aligned}
$$

$\langle 2 \rangle 6$. Q.E.D.

$\quad$ PROOF: Theorem 18.1.12, $\langle 1 \rangle 5$, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$.

□

**Definition 18.1.14** (Open Ball). Let $V$ be a normed space over $K$. Let $x \in V$. Let $r > 0$. The *open ball* with *centre* $x$ and *radius* $r$ is

$$ B(x, r) := \{ y \in V \mid \|y - x\| < r \} \ . $$

**Definition 18.1.15** (Closed Ball). Let $V$ be a normed space over $K$. Let $x \in V$. Let $r > 0$. The *closed ball* with *centre* $x$ and *radius* $r$ is

$$ \overline{B}(x, r) := \{ y \in V \mid \|y - x\| \leq r \} \ . $$

**Definition 18.1.16** (Sphere). Let $V$ be a normed space over $K$. Let $x \in V$. Let $r > 0$. The *sphere* with *centre* $x$ and *radius* $r$ is

$$ S(x, r) := \{ y \in V \mid \|y - x\| = r \} \ . $$

**Definition 18.1.17** (Open Set). Let $V$ be a normed space over $K$. A set $S \subseteq V$ is *open* iff, for all $x \in S$, there exists $\epsilon > 0$ such that $B(x, \epsilon) \subseteq S$.

**Proposition 18.1.18.** *Equivalent norms define the same set of open sets.*

PROOF:

$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.

$\langle 1 \rangle 2$. LET: $\| \ \|_1$ and $\| \ \|_2$ be equivalent norms on $V$.

$\langle 1 \rangle 3$. PICK reals $\alpha, \beta > 0$ such that, for all $x \in V$, we have $\alpha \|x\|_1 \leq \|x\|_2 \leq \beta \|x\|_1$

$\langle 1 \rangle 4$. LET: $S \subseteq V$

$\langle 1 \rangle 5$. If $S$ is open under $\| \ \|_1$ then $S$ is open under $\| \ \|_2$.

$\quad \langle 2 \rangle 1$. ASSUME: $S$ is open under $\| \ \|_1$.

$\quad \langle 2 \rangle 2$. LET: $x \in S$

$\quad \langle 2 \rangle 3$. PICK $\epsilon > 0$ such that $\{ y \in V \mid \|x - y\|_1 < \epsilon \} \subseteq S$.

$\quad \langle 2 \rangle 4$. LET: $\delta = \alpha \epsilon$

$\langle 2 \rangle 5.$  $\{y \in V \mid \|x - y\|_2 < \delta\} \subseteq S$

$\langle 1 \rangle 6.$  If $S$ is open under $\|\ \|_2$ then $S$ is open under $\|\ \|_1$.

PROOF: Similar.

☐

**Proposition 18.1.19.** *Every open ball is open.*

PROOF:

$\langle 1 \rangle 1.$  LET: $V$ be a normed space over $K$.

$\langle 1 \rangle 2.$  LET: $c \in V$ and $r > 0$
    PROVE:  $B(c, r)$ is open.

$\langle 1 \rangle 3.$  LET: $x \in B(c, r)$

$\langle 1 \rangle 4.$  LET: $\epsilon = r - \|x - c\|$
    PROVE:  $B(x, \epsilon) \subseteq B(c, r)$

$\langle 1 \rangle 5.$  LET: $y \in B(x, \epsilon)$
    PROVE:  $y \in B(c, r)$

$\langle 1 \rangle 6.$  $\|y - c\| < r$
   PROOF:

$$\begin{aligned} \|y - c\| &\leq \|y - x\| + \|x - c\| && \text{(Triangle Inequality)} \\ &< \epsilon + \|x - c\| && (\langle 1 \rangle 5) \\ &= r && (\langle 1 \rangle 4) \end{aligned}$$

☐

**Proposition 18.1.20.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$. Then $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega.g(x) < f(x)\}$ is open.*

PROOF:

$\langle 1 \rangle 1.$  LET: $g \in U$

$\langle 1 \rangle 2.$  LET: $\epsilon = \max_{x \in \Omega}(f(x) - g(x))$
    PROVE:  $B(g, \epsilon) \subseteq S$

$\langle 1 \rangle 3.$  $\epsilon > 0$

$\langle 1 \rangle 4.$  LET: $h \in B(g, \epsilon/2)$
    PROVE:  $h \in S$

$\langle 1 \rangle 5.$  LET: $x \in \Omega$

$\langle 1 \rangle 6.$  $h(x) < f(x)$
   PROOF:

$$\begin{aligned} h(x) &\leq g(x) + \epsilon/2 && (\langle 1 \rangle 4) \\ &< g(x) + \epsilon && (\langle 1 \rangle 3) \\ &\leq f(x) && (\langle 1 \rangle 2) \end{aligned}$$

☐

**Proposition 18.1.21.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$. Then $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega.g(x) > f(x)\}$ is open.*

PROOF: Given $g \in U$, let $\epsilon = \max_x(g(x) - f(x))/2$. Then $B(g, \epsilon) \subseteq U$. ☐

**Proposition 18.1.22.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$ be such that $f(x) > 0$ for all $x \in \Omega$. Then $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega.|g(x)| < f(x)\}$ is open.*

PROOF: Given $g \in U$, let $\epsilon = \max_x(f(x) - |g(x)|)/2$. Then $B(g, \epsilon) \subseteq U$. □

**Proposition 18.1.23.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$ be such that $f(x) > 0$ for all $x \in \Omega$. Then $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega.|g(x)| > f(x)\}$ is open.*

PROOF: Given $g \in U$, let $\epsilon = \max_x(|g(x)| - f(x))/2$. Then $B(g, \epsilon) \subseteq U$. □

**Proposition 18.1.24.** *The union of a set of open sets is open.*

PROOF:
$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2$. LET: $\mathcal{U}$ be a set of open sets in $V$.
$\langle 1 \rangle 3$. LET: $x \in \bigcup \mathcal{U}$
$\langle 1 \rangle 4$. PICK $U \in \mathcal{U}$ such that $x \in U$.
$\langle 1 \rangle 5$. PICK $\epsilon > 0$ such that $B(x, \epsilon) \subseteq U$
$\langle 1 \rangle 6$. $B(x, \epsilon) \subseteq \bigcup \mathcal{U}$
□

**Proposition 18.1.25.** *The intersection of two open sets is open.*

PROOF:
$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2$. LET: $U_1$ and $U_2$ be open sets in $V$.
$\langle 1 \rangle 3$. LET: $x \in U_1 \cap U_2$
$\langle 1 \rangle 4$. PICK $\epsilon_1 > 0$ such that $B(x, \epsilon_1) \subseteq U_1$
$\langle 1 \rangle 5$. PICK $\epsilon_2 > 0$ such that $B(x, \epsilon_2) \subseteq U_2$
$\langle 1 \rangle 6$. LET: $\epsilon = \min(\epsilon_1, \epsilon_2)$
$\langle 1 \rangle 7$. $B(x, \epsilon) \subseteq U_1 \cap U_2$
□

**Proposition 18.1.26.** *In any normed space, $\emptyset$ is open.*

PROOF: Vacuous. □

**Proposition 18.1.27.** *In any normed space $V$, the whole space $V$ is open.*

PROOF: For any $x \in V$ we have $B(x, 1) \subseteq V$. □

**Definition 18.1.28** (Closed Set)**.** Let $V$ be a normed space over $K$. A set $S \subseteq V$ is *closed* iff $V - S$ is open.

**Proposition 18.1.29.** *Every closed ball is closed.*

PROOF:
$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2$. LET: $c \in V$ and $r > 0$
        PROVE:    $\overline{B}(c, r)$ is closed.
$\langle 1 \rangle 3$. LET: $x \in V - \overline{B}(c, r)$
$\langle 1 \rangle 4$. LET: $\epsilon = \|x - c\| - r$
        PROVE:    $B(x, \epsilon) \subseteq V - \overline{B}(c, r)$

$\langle 1 \rangle 5$. $\epsilon > 0$
  PROOF: Since $\|x - c\| > r$ by $\langle 1 \rangle 3$.
$\langle 1 \rangle 6$. LET: $y \in B(x, \epsilon)$
$\langle 1 \rangle 7$. $\|y - c\| > r$
  PROOF:

$$
\begin{aligned}
\|y - c\| &\geq \|x - c\| - \|x - y\| && \text{(Triangle Inequality)} \\
&> \|x - c\| - \epsilon && (\langle 1 \rangle 6) \\
&= r && (\langle 1 \rangle 4)
\end{aligned}
$$

$\Box$

**Proposition 18.1.30.** *The intersection of a set of closed sets is closed.*

PROOF: From Proposition 18.1.24. $\Box$

**Proposition 18.1.31.** *The union of two closed sets is closed.*

PROOF: From Proposition 18.1.25. $\Box$

**Proposition 18.1.32.** *Every sphere is closed.*

PROOF: $S(c, r) = \overline{B}(c, r) - B(c, r)$. $\Box$

**Proposition 18.1.33.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$. Then $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega . g(x) \leq f(x)\}$ is closed.*

PROOF: It is $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . g(x) > f(x)\}$. $\Box$

**Proposition 18.1.34.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$. Then $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega . g(x) \geq f(x)\}$ is closed.*

PROOF: It is $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . g(x) < f(x)\}$. $\Box$

**Proposition 18.1.35.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$. Then $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega . |g(x)| \leq f(x)\}$ is closed.*

PROOF: It is $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . |g(x)| > f(x)\}$. $\Box$

**Proposition 18.1.36.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $f \in \mathcal{C}(\Omega)$. Then $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega . |g(x)| \geq f(x)\}$ is closed.*

PROOF: It is $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . |g(x)| < f(x)\}$. $\Box$

**Proposition 18.1.37.** *Let $\Omega$ be a closed bounded set in $\mathbb{R}^n$. Let $x_0 \in \Omega$ and $\lambda \in \mathbb{C}$. Then $C = \{g \in \mathcal{C}(\Omega) \mid g(x_0) = \lambda\}$ is closed.*

PROOF: Given $g \in \mathcal{C}(\Omega) - C$, let $\epsilon = |g(x_0) - \lambda|/2$. Then $B(g, \epsilon) \subseteq \mathcal{C}(\Omega) - C$. $\Box$

**Proposition 18.1.38.** *In any normed space $V$, we have $\emptyset$ is closed.*

PROOF: Since $V - \emptyset = V$ is open. $\Box$

**Proposition 18.1.39.** *In any normed space $V$, the whole space $V$ is closed.*

PROOF: Since $V - V = \emptyset$ is open. $\square$

**Theorem 18.1.40.** *Let $V$ be a normed space over $K$. Let $S$ be a subset of $V$. Then $S$ is closed if and only if, for any sequence $(x_n)$ in $S$, if $x_n \to l$ as $n \to \infty$ then $l \in S$.*

PROOF:
$\langle 1 \rangle 1$. If $S$ is closed then, for any sequence $(x_n)$ in $S$, if $x_n \to l$ as $n \to \infty$ then $l \in S$.
  $\langle 2 \rangle 1$. ASSUME: $S$ is closed.
  $\langle 2 \rangle 2$. LET: $(x_n)$ be a sequence in $S$.
  $\langle 2 \rangle 3$. ASSUME: $x_n \to l$ as $n \to \infty$.
  $\langle 2 \rangle 4$. ASSUME: for a contradiction $l \notin S$.
  $\langle 2 \rangle 5$. PICK $\epsilon > 0$ such that $B(l, \epsilon) \subseteq V - S$
  $\langle 2 \rangle 6$. PICK $N$ such that $\forall n \geq N . x_n \in B(l, \epsilon)$
  $\langle 2 \rangle 7$. $x_N \in V - S$
  $\langle 2 \rangle 8$. This contradicts $\langle 2 \rangle 2$.
$\langle 1 \rangle 2$. If, for any sequence $(x_n)$ in $S$, if $x_n \to l$ as $n \to \infty$ then $l \in S$, then $S$ is closed.
  $\langle 2 \rangle 1$. ASSUME: for any sequence $(x_n)$ in $S$, if $x_n \to l$ as $n \to \infty$ then $l \in S$.
  $\langle 2 \rangle 2$. LET: $x \in V - S$
  $\langle 2 \rangle 3$. ASSUME: for a contradiction there is no $\epsilon > 0$ such that $B(x, \epsilon) \subseteq V - S$.
  $\langle 2 \rangle 4$. For $n \in \mathbb{Z}_+$, PICK $x_n \in B(x, 1/n) \cap S$
  $\langle 2 \rangle 5$. $x_n \to x$ as $n \to \infty$
  $\langle 2 \rangle 6$. $x \in S$
  $\langle 2 \rangle 7$. This contradicts $\langle 2 \rangle 2$.
$\square$

**Definition 18.1.41** (Closure)**.** Let $V$ be a normed space over $K$. Let $S$ be a subset of $V$. The *closure* of $S$, cl $S$, is the intersection of the set of closed sets that include $S$.

**Proposition 18.1.42.** *Let $V$ be a normed space over $K$. Let $S$ be a subset of $V$. Then the closure of $S$ is the smallest closed set that includes $S$.*

PROOF: Proposition 18.1.30. $\square$

**Theorem 18.1.43.** *Let $V$ be a normed space over $K$. Let $S$ be a subset of $V$. Then*

$$\text{cl } S = \{l \in V \mid \exists \text{ a sequence } (x_n) \text{ in } S . x_n \to l \text{ as } n \to \infty\} \ .$$

PROOF:
$\langle 1 \rangle 1$. For all $l \in \text{cl } S$, there exists a sequence $(x_n)$ in $S$ such that $x_n \to l$ as $n \to \infty$.
  $\langle 2 \rangle 1$. LET: $l \in \text{cl } S$
  $\langle 2 \rangle 2$. For $n \in \mathbb{Z}_+$, pick $x_n \in B(l, 1/n) \cap S$
    PROOF: There must be such an $x_n$ otherwise $S - B(l, 1/n)$ would be a smaller closed set that includes $S$.

$\langle 2 \rangle$3.  $x_n \to l$ as $n \to \infty$
$\langle 1 \rangle$2.  For any sequence $(x_n)$ in $S$, if $x_n \to l$ as $n \to \infty$ then $l \in \operatorname{cl} S$.
  PROOF: Theorem 18.1.40.

□

**Definition 18.1.44** (Dense)**.** Let $V$ be a normed space over $K$. Let $S \subseteq V$. Then $S$ is *dense* if and only if $\operatorname{cl} S = V$.

**Theorem 18.1.45** (Weierstrass Approximation Theorem)**.** *Let $a$ and $b$ be real numbers with $a < b$. In $\mathcal{C}([a, b])$, the set of polynomials is dense.*

PROOF:TODO

**Proposition 18.1.46.** *Let $p \geq 1$. The set of all sequences that have only finitely many non-zero terms is dense in $l^p$.*

PROOF:
$\langle 1 \rangle$1.  LET:  $(z_n) \in l^p$
$\langle 1 \rangle$2.  LET:  $\epsilon > 0$
    PROVE:   There exists a sequence $(x_n)$ with only finitely many non-zero
             terms such that $\left( \sum_{n=1}^{\infty} |z_n - x_n|^p \right)^{1/p} < \epsilon$
$\langle 1 \rangle$3.  PICK $N$ such that $| \sum_{n=1}^{\infty} |z_n|^p - \sum_{n=1}^{N} |z_n|^p | < \epsilon^p$
$\langle 1 \rangle$4.  LET:  $(x_n)$ be the sequence that agrees with $(z_n)$ up to term $N$, and then
          zeros after that.
$\langle 1 \rangle$5.  $\left( \sum_{n=1}^{\infty} |z_n - x_n|^p \right)^{1/p} < \epsilon$
    PROOF:

$$
\left( \sum_{n=1}^{\infty} |z_n - x_n|^p \right)^{1/p} = \left( \sum_{n=N+1}^{\infty} |z_n|^p \right)^{1/p} \qquad (\langle 1 \rangle 4)
$$

$$
< \epsilon \qquad (\langle 1 \rangle 2)
$$

□

**Theorem 18.1.47.** *Let $V$ be a normed space over $K$. Let $S \subseteq V$. Then the following are equivalent.*

  1. *$S$ is dense.*

  2. *For all $l \in V$, there exists a sequence $(x_n)$ in $S$ such that $x_n \to l$ as $n \to \infty$.*

  3. *Every nonempty open subset of $V$ intersects $S$.*

PROOF:
$\langle 1 \rangle$1.  $1 \Leftrightarrow 2$
    PROOF: Theorem 18.1.43.
$\langle 1 \rangle$2.  $1 \Rightarrow 3$
  $\langle 2 \rangle$1.  ASSUME: $S$ is dense.
  $\langle 2 \rangle$2.  LET: $U$ be a nonempty open subset of $V$.
  $\langle 2 \rangle$3.  $X - U$ does not include $S$.

PROOF: Lest we have $\operatorname{cl} S \subseteq X - U$.
$\langle 2 \rangle 4.$ $U$ intersects $S$.
$\langle 1 \rangle 3.$ $3 \Rightarrow 1$
$\quad \langle 2 \rangle 1.$ ASSUME: Every nonempty subset of $V$ intersects $S$.
$\quad \langle 2 \rangle 2.$ Every closed proper subset of $V$ does not include $S$.
$\quad \langle 2 \rangle 3.$ $\operatorname{cl} S = V$
□

**Definition 18.1.48** (Compact)**.** Let $V$ be a normed space over $K$ and $S \subseteq V$. Then $S$ is *compact* if and only if every sequence in $S$ has a convergent subsequence whose limit is in $S$.

**Proposition 18.1.49.** *In $K^n$, a set is compact if and only if it is bounded and closed.*

PROOF: TODO

**Definition 18.1.50** (Bounded)**.** Let $V$ be a normed space over $K$ and $S \subseteq V$. Then $S$ is *bounded* iff there exists $r > 0$ such that $V \subseteq B(0, r)$.

**Theorem 18.1.51.** *Every compact set is closed and bounded.*

PROOF:
$\langle 1 \rangle 1.$ LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2.$ LET: $S \subseteq V$ be compact.
$\langle 1 \rangle 3.$ $S$ is closed.
$\quad \langle 2 \rangle 1.$ LET: $(x_n)$ be a sequence in $S$ that converges to $l$
$\quad \langle 2 \rangle 2.$ PICK a sequence $(x_{n_r})$ that converges to $x \in S$
$\quad \quad$ PROOF: $\langle 1 \rangle 2, \langle 2 \rangle 1$
$\quad \langle 2 \rangle 3.$ $x_{n_r} \to l$ as $n \to \infty$
$\quad \quad$ PROOF: $\langle 2 \rangle 1, \langle 2 \rangle 2$
$\quad \langle 2 \rangle 4.$ $l = x$
$\quad \quad$ PROOF: Proposition 18.1.2.
$\quad \langle 2 \rangle 5.$ $l \in S$
$\quad \quad$ PROOF: $\langle 2 \rangle 2, \langle 2 \rangle 4$
$\quad \langle 2 \rangle 6.$ Q.E.D.
$\quad \quad$ PROOF: Theorem 18.1.40.
$\langle 1 \rangle 4.$ $S$ is bounded.
$\quad \langle 2 \rangle 1.$ ASSUME: for a contradiction $S$ is unbounded.
$\quad \langle 2 \rangle 2.$ For $n \in \mathbb{Z}_+$, PICK $x_n \in S - B(0, n)$
$\quad \langle 2 \rangle 3.$ PICK a convergent subsequence $(x_{n_r})$ that converges to $l$, say.
$\quad \langle 2 \rangle 4.$ PICK $N \in \mathbb{Z}_+$ such that $\|l\| < N$
$\quad \langle 2 \rangle 5.$ PICK $r$ such that $n_r > N$ and $\|x_{n_r} - l\| < N - \|l\|$
$\quad \langle 2 \rangle 6.$ $\|x_{n_r}\| < N < n_r$
$\quad \langle 2 \rangle 7.$ This contradicts $\langle 2 \rangle 2$.
□

**Proposition 18.1.52.** *In $\mathcal{C}([0, 1])$, the closed ball $\overline{B}(0, 1)$ is closed and bounded but not compact.*

PROOF: The sequence of functions $(x^n)$ is in $\overline{B}(0,1)$ but has no convergent subsequence. $\square$

**Theorem 18.1.53** (Riesz's Lemma)**.** *Let $V$ be a normed vector space over $K$. Let $X$ be a closed proper subspace of $V$. Let $0 < \epsilon < 1$. Then there exists $x \in V$ such that $\|x\| = 1$ and $\forall y \in X. \|x - y\| \geq \epsilon$.*

PROOF:
$\langle 1 \rangle 1$. PICK $z \in V - X$
$\langle 1 \rangle 2$. LET: $d = \inf_{x \in X} \|z - x\|$
$\langle 1 \rangle 3$. $d > 0$
  PROOF: Since $X$ is closed, there exists $e > 0$ such that $B(z, d) \subseteq V - X$ and hence $\|z - x\| \geq d$ for all $x \in X$.
$\langle 1 \rangle 4$. PICK $x_0 \in X$ such that $d \leq \|z - x_0\| \leq d/\epsilon$
  PROOF: One exists since $d/\epsilon$ is not a lower bound for $\{\|z - x\| \mid x \in X\}$.
$\langle 1 \rangle 5$. LET: $x = (z - x_0)/\|z - x_0\|$
$\langle 1 \rangle 6$. LET: $y \in X$
$\langle 1 \rangle 7$. $\|x - y\| \geq \epsilon$
  PROOF:

$$\|x - y\| = \left\| \frac{z - x_0}{\|z - x_0\|} - y \right\| \qquad (\langle 1 \rangle 5)$$

$$= \frac{1}{\|z - x_0\|} \|z - (x_0 + \|z - x_0\| y)\|$$

$$\geq \frac{1}{\|z - x_0\|} d \qquad (\langle 1 \rangle 2)$$

$$\geq \epsilon \qquad (\langle 1 \rangle 4)$$

$\square$

**Theorem 18.1.54.** *Let $V$ be a normed space over $K$. Then $V$ is finite dimensional if and only if $\overline{B}(0,1)$ is compact.*

PROOF:
$\langle 1 \rangle 1$. If $V$ is finite dimensional then $\overline{B}(0,1)$ is compact.
  $\langle 2 \rangle 1$. ASSUME: $V$ is finite dimensional.
  $\langle 2 \rangle 2$. PICK a basis $\{e_1, \ldots, e_n\}$
  $\langle 2 \rangle 3$. ASSUME: w.l.o.g. $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\| = |\alpha_1| + \cdots + |\alpha_n|$
  $\langle 2 \rangle 4$. LET: $(\alpha_{k1} e_1 + \cdots + \alpha_{kn} e_n)$ be a sequence in $\overline{B}(0,1)$
  $\langle 2 \rangle 5$. PICK a convergent subsequence $(\alpha_{k_r 1})$ of $(\alpha_{k1})$, a convergent subsequence $(\alpha_{k'_r} 2)$ of $(\alpha_{k_r 2})$, $\ldots$, a convergent subsequence $(\alpha_{k''_r} n)$.
  $\langle 2 \rangle 6$. $(\alpha_{k''_r 1} e_1 + \cdots + \alpha_{k''_r n} e_n)$ converges.
$\langle 1 \rangle 2$. If $V$ is infinite dimensional then $\overline{B}(0,1)$ is not compact.
  $\langle 2 \rangle 1$. ASSUME: $V$ is infinite dimensional.
  $\langle 2 \rangle 2$. Choose a sequence $(x_n)$ with $\|x_n\| = 1$ and $\|x_m - x_n\| \geq 1/2$ for $m \neq n$
    $\langle 3 \rangle 1$. ASSUME: $x_1, \ldots, x_n$ satisfy $\|x_i\| = 1$ and $\|x_i - x_j\| \geq 1/2$ for $i \neq j$
    $\langle 3 \rangle 2$. PICK $x_{n+1} \in V$ such that $\|x_{n+1}\| = 1$ and for all $y \in \mathrm{span}\{x_1, \ldots, x_n\}$ we have $\|x_{n+1} - y\| \geq 1/2$

$\langle 4 \rangle 1$.  span$\{x_1, \ldots, x_n\}$ is closed.
   $\langle 5 \rangle 1$.  LET:  $S = \text{span}\{x_1, \ldots, x_n\}$
   $\langle 5 \rangle 2$.  LET:  $(a_n)$ be a sequence in $S$ that converges to $a \in V$
        PROVE:    $a \in S$
   $\langle 5 \rangle 3$.  $(a_n)$ is a Cauchy sequence in $V$.
   $\langle 5 \rangle 4$.  $(a_n)$ is a Cauchy sequence in $S$.
   $\langle 5 \rangle 5$.  A finite dimensional normed space is a Banach space.
   $\langle 5 \rangle 6$.  $S$ is complete.
   $\langle 5 \rangle 7$.  $a \in S$
$\langle 4 \rangle 2$.  span$\{x_1, \ldots, x_n\}$ is a proper subspace of $V$.
   PROOF: $\langle 2 \rangle 1$
$\langle 4 \rangle 3$.  Q.E.D.
   PROOF: Riesz's Lemma.
$\langle 2 \rangle 3$.  ASSUME:  for a contradiction $(x_{n_r})$ is a subsequence that converges to $l$
$\langle 2 \rangle 4$.  For all $r \in \mathbb{N}$, we have $\|x_{n_r} - l\| + \|x_{n_{r+1}} - l\| \geq 1/2$
$\langle 2 \rangle 5$.  This is a contradiction.

$\square$

**Proposition 18.1.55.** *Let $V$ be a normed space. The closure of a subspace of $V$ is a subspace.*

PROOF:
$\langle 1 \rangle 1$.  LET:  $U$ be a subspace of $V$
$\langle 1 \rangle 2$.  LET:  $x, y \in \text{cl}\,U$ and $\alpha, \beta \in K$
$\langle 1 \rangle 3$.  PICK sequences $(x_n)$, $(y_n)$ in $U$ that converge to $x$ and $y$ respectively.
$\langle 1 \rangle 4$.  $\alpha x_n + \beta y_n \to \alpha x + \beta y$ as $n \to \infty$
$\langle 1 \rangle 5$.  $\alpha x + \beta y \in \text{cl}\,U$

$\square$

## 18.2  Continuous Linear Mappings

**Definition 18.2.1** (Continuous)**.** Let $U$ and $V$ be normed spaces. Let $f : U \to V$ and $x \in U$. Then $f$ is *continuous at* $x$ iff, for any sequence $(x_n)$ in $U$, if $x_n \to x$ as $n \to \infty$ then $f(x_n) \to f(x)$ as $n \to \infty$. The function $f$ is *continuous* iff $f$ is continuous at every point.

**Proposition 18.2.2.** *Let $V$ be a normed space. Then the norm is a continuous function $V \to \mathbb{R}$.*

PROOF: From Proposition 18.0.4.  $\square$

**Proposition 18.2.3.** *Let $U$ and $V$ be normed space. Let $f : U \to V$. Then the following are equivalent.*

1. *$f$ is continuous.*

2. *For any open set $S$ in $V$, we have $f^{-1}(S)$ is open in $U$.*

 3. *For any closed set $C$ in $V$, we have $f^{-1}(C)$ is closed in $U$.*

**Proposition 18.2.4.** *Let $U$ and $V$ be normed spaces over $K$. Let $T : U \to V$ be a linear transformation. If $T$ is continuous at some point, then it is continuous.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: $T$ is continuous at $u_0$

$\langle 1 \rangle 2$. LET: $x_n \to l$ as $n \to \infty$ in $U$

$\langle 1 \rangle 3$. $x_n - l + u_0 \to u_0$ as $n \to \infty$.

$\langle 1 \rangle 4$. $T(x_n - l + u_0) \to T(u_0)$ as $n \to \infty$.

$\langle 1 \rangle 5$. $T(x_n) - T(l) + T(u_0) \to T(u_0)$ as $n \to \infty$.

$\langle 1 \rangle 6$. $T(x_n) \to T(l)$ as $n \to \infty$.

$\square$

**Definition 18.2.5** (Bounded). Let $U$ and $V$ be normed spaces over $K$. Let $T : U \to V$ be a linear transformation. Then $T$ is *bounded* iff there exists $\alpha > 0$ such that, for all $x \in U$, we have $\|T(x)\| \leq \alpha \|x\|$.

**Theorem 18.2.6.** *Let $U$ and $V$ be normed spaces over $K$. Let $T : U \to V$ be a linear transformation. Then $T$ is continuous if and only if it is bounded.*

PROOF:

$\langle 1 \rangle 1$. If $T$ is continuous then $T$ is bounded.

 $\langle 2 \rangle 1$. ASSUME: $T$ is not bounded.

 $\langle 2 \rangle 2$. For $n \in \mathbb{Z}_+$, PICK $x_n \in U$ such that $\|T(x_n)\| > n\|x_n\|$.

 $\langle 2 \rangle 3$. For $n \in \mathbb{Z}_+$,
 LET:

$$y_n = \frac{x_n}{n\|x_n\|}$$

 $\langle 2 \rangle 4$. $y_n \to 0$ as $n \to \infty$

 $\langle 2 \rangle 5$. $T(y_n) \nrightarrow 0$ as $n \to \infty$

 $\langle 2 \rangle 6$. $T$ is not continuous.

$\langle 1 \rangle 2$. If $T$ is bounded then $T$ is continuous.

 $\langle 2 \rangle 1$. ASSUME: $T$ is bounded.

 $\langle 2 \rangle 2$. PICK $\alpha > 0$ such that $\forall x \in U.\|T(x)\| \leq \alpha\|x\|$.

 $\langle 2 \rangle 3$. $T$ is continuous at $0$.

 $\langle 3 \rangle 1$. LET: $(x_n)$ be a sequence that converges to $0$ in $U$

 $\langle 3 \rangle 2$. $T(x_n) \to 0$ as $n \to \infty$
 PROOF:

$$\|T(x_n)\| \leq \alpha\|x_n\| \qquad\qquad (\langle 2 \rangle 2)$$
$$\to 0 \qquad\qquad \text{as } n \to \infty$$

 $\langle 2 \rangle 4$. $T$ is continuous.
 PROOF: Proposition 18.2.4.

$\square$

**Proposition 18.2.7.** *Let $U$ and $V$ be normed spaces over $K$ where $U$ is finite dimensional. Let $T : U \to V$ be a linear transformation. Then $T$ is bounded.*

PROOF:

⟨1⟩1. PICK a basis $\{e_1, \ldots, e_n\}$ of unit vectors for $U$.

⟨1⟩2. LET: $M = \max(\|T(e_1)\|, \ldots, \|T(e_n)\|)$

⟨1⟩3. PICK $C > 0$ such that, for all $\alpha_1, \ldots, \alpha_n \in K$, we have $|\alpha_1| + \cdots + |\alpha_n| \leq C\|\alpha_1 e_1 + \cdots + \alpha_n e_n\|$

    PROOF: Theorem 18.1.13.

⟨1⟩4. LET: $x \in U$

    PROVE:    $\|T(x)\| \leq CM\|x\|$

⟨1⟩5. LET: $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$

⟨1⟩6. $\|T(x)\| \leq CM\|x\|$

    PROOF:

$$
\begin{aligned}
\|T(x)\| &= \|\alpha_1 T(e_1) + \cdots + \alpha_n T(e_n)\| && (T \text{ linear}) \\
&\leq |\alpha_1|\|T(e_1)\| + \cdots + |\alpha_n|\|T(e_n)\| && (\text{Triangle inequality}) \\
&\leq M(|\alpha_1| + \cdots + |\alpha_n|) && (\langle 1 \rangle 2) \\
&\leq CM\|x\| && (\langle 1 \rangle 3)
\end{aligned}
$$

∎

**Corollary 18.2.7.1.** *Let $U$ and $V$ be normed spaces over $K$ where $U$ is finite dimensional. Let $T : U \to V$ be a linear transformation. Then $T$ is continuous.*

**Proposition 18.2.8.** *Let $U$ and $V$ be normed spaces over $K$. Let $T : U \to V$ be a linear transformation. If $T$ is continuous, then $T$ is uniformly continuous.*

PROOF:

⟨1⟩1. ASSUME: $T$ is continuous

⟨1⟩2. PICK $B > 0$ such that $\forall x \in U.\|T(x)\| \leq B\|x\|$

⟨1⟩3. LET: $\epsilon > 0$

⟨1⟩4. LET: $\delta = \epsilon/B$

⟨1⟩5. LET: $x, y \in U$

⟨1⟩6. ASSUME: $\|x - y\| < \delta$

⟨1⟩7. $\|T(x) - T(y)\| < \epsilon$

    PROOF:

$$
\begin{aligned}
\|T(x) - T(y)\| &= \|T(x - y)\| && (T \text{ linear}) \\
&\leq B\|x - y\| && (\langle 1 \rangle 2) \\
&< B\delta && (\langle 1 \rangle 6) \\
&= \epsilon && (\langle 1 \rangle 4)
\end{aligned}
$$

∎

**Proposition 18.2.9.** *Let $U$ and $V$ be normed spaces over $K$. The set $\mathcal{B}(U, V)$ of all bounded linear maps from $U$ to $V$ forms a subspace of the space of all linear maps from $U$ to $V$.*

PROOF:

⟨1⟩1. LET: $S, T : U \to V$ be bounded linear maps and $\alpha, \beta \in K$.

    PROVE:    $\alpha S + \beta T$ is bounded.

⟨1⟩2. PICK $B, C > 0$ such that $\forall x \in U.\|S(x)\| \leq B\|x\|$ and $\|T(x)\| \leq C\|x\|$

⟨1⟩3. $\forall x \in U.\|(\alpha S + \beta T)(x)\| \leq (|\alpha|B + |\beta|C)\|x\|$

☐

**Proposition 18.2.10.** *Let $U$ and $V$ be normed spaces over $K$. Define the operator norm $\| \ \|$ on $\mathcal{B}(U,V)$ by $\|T\| := \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\}$. Then $\| \ \|$ is a norm on $\mathcal{B}(U,V)$.*

PROOF:
$\langle 1 \rangle 1$. For all $T \in \mathcal{B}(U,V)$, the set $\{\|T(x)\| \mid x \in U, \|x\| = 1\}$ is bounded above.
   $\langle 2 \rangle 1$. LET: $T \in \mathcal{B}(U,V)$
   $\langle 2 \rangle 2$. PICK $B$ such that $\forall x \in U.\|T(x)\| \le B\|x\|$.
   $\langle 2 \rangle 3$. $B$ is an upper bound for $\{\|T(x)\| \mid x \in U, \|x\| = 1\}$.
$\langle 1 \rangle 2$. If $\|T\| = 0$ then $T = 0$.
   $\langle 2 \rangle 1$. ASSUME: $\|T\| = 0$
   $\langle 2 \rangle 2$. LET: $x \in U$
       PROVE: $T(x) = 0$
   $\langle 2 \rangle 3$. ASSUME: w.l.o.g. $\|x\| \ne 0$
   $\langle 2 \rangle 4$. LET: $y = x/\|x\|$
   $\langle 2 \rangle 5$. $\|y\| = 1$
   $\langle 2 \rangle 6$. $\|T(y)\| = 0$
   $\langle 2 \rangle 7$. $T(y) = 0$
   $\langle 2 \rangle 8$. $T(x) = 0$
$\langle 1 \rangle 3$. For all $\lambda \in K$ and $T \in \mathcal{B}(U,V)$, we have $\|\lambda T\| = |\lambda| \|T\|$
   $\langle 2 \rangle 1$. LET: $\lambda \in K$ and $T \in \mathcal{B}(U,V)$
   $\langle 2 \rangle 2$. $\|\lambda T\| = |\lambda| \|T\|$
     PROOF:
$$\begin{aligned}
\|\lambda T\| &= \sup\{\|\lambda T(x)\| \mid x \in U, \|x\| = 1\} \\
&= \sup\{|\lambda|\|T(x)\| \mid x \in U, \|x\| = 1\} \\
&= |\lambda| \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\} \\
&= |\lambda| \|T\|
\end{aligned}$$
$\langle 1 \rangle 4$. For all $S, T \in \mathcal{B}(U,V)$, we have $\|S + T\| \le \|S\| + \|T\|$.
   $\langle 2 \rangle 1$. LET: $S, T \in \mathcal{B}(U,V)$
   $\langle 2 \rangle 2$. $\|S + T\| \le \|S\| + \|T\|$
     PROOF:
$$\begin{aligned}
\|S + T\| &= \sup\{\|S(x) + T(x)\| \mid x \in U, \|x\| = 1\} \\
&\le \sup\{\|S(x)\| + \|T(x)\| \mid x \in U, \|x\| = 1\} \\
&\le \sup\{\|S(x)\| \mid x \in U, \|x\| = 1\} + \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\} \\
&= \|S\| + \|T\|
\end{aligned}$$

☐

**Proposition 18.2.11.** *Let $U$ and $V$ be normed spaces. Let $T \in \mathcal{B}(U,V)$. Then $\|T\|$ is the least number such that $\forall u \in U.\|T(u)\| \le \|T\|\|u\|$.*

PROOF:
$\langle 1 \rangle 1$. $\forall u \in U.\|T(u)\| \le \|T\|\|u\|$
   $\langle 2 \rangle 1$. LET: $u \in U$
   $\langle 2 \rangle 2$. LET: $v = u/\|u\|$

$\langle 2 \rangle 3$. $\|T(v)\| \leq \|T\|$
$\langle 2 \rangle 4$. $\|T(u)\| \leq \|T\| \|u\|$
$\langle 1 \rangle 2$. If $\alpha$ satisfies $\forall u \in U. \|T(u)\| \leq \alpha \|u\|$, then $\|T\| \leq \alpha$
$\quad \langle 2 \rangle 1$. Assume: $\forall u \in U. \|T(u)\| \leq \alpha \|u\|$
$\quad \langle 2 \rangle 2$. For all $x \in U$, if $\|x\| = 1$ then $\|T(x)\| \leq \alpha$
$\quad \langle 2 \rangle 3$. $\|T\| \leq \alpha$
☐

**Proposition 18.2.12.** *Let $V$ be a normed space. Then $\mathrm{id}_V$ is a bounded linear function $V \to V$, and $\|\mathrm{id}_V\| = 1$.*

**Proposition 18.2.13.** *Let $U$ and $V$ be normed spaces. The constant zero function $U \to V$ is a bounded linear transformation with norm 0.*

**Proposition 18.2.14.** *Let $N \in \mathbb{N}$. Let $T : \mathbb{C}^N \to \mathbb{C}^N$ be a linear transformation with matrix $A = (a_{ij})$. Then $T$ is bounded and*

$$\|T\| \leq \sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} |a_{ij}|^2} \ .$$

**Definition 18.2.15** (Uniform Convergence)**.** Let $U$ and $V$ be normed spaces. Let $(T_n)$ be a sequence in $\mathcal{B}(U, V)$ and $T \in \mathcal{B}(U, V)$. Then $(T_n)$ *converges uniformly* to $T$ iff $(T_n)$ converges to $T$ under the standard norm defined above.

**Theorem 18.2.16.** *Let $U$ and $V$ be normed spaces. Let $T : U \to V$ be a continuous linear function. Then $\ker T$ is a closed subspace of $U$.*

PROOF:
$\langle 1 \rangle 1$. $\ker T$ is a subspace of $U$
$\quad$ PROOF: If $x, y \in \ker T$ and $\alpha, \beta \in K$ then $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) = 0$.
$\langle 1 \rangle 2$. $\ker T$ is closed.
$\quad$ PROOF: Let $(x_n)$ be a sequence in $\ker T$ and $x_n \to l$. Then $T(l) = \lim_{n \to \infty} T(x_n) = 0$.
☐

**Theorem 18.2.17.** *Let $U$ and $V$ be normed spaces. Let $W$ be a closed subspace of $U$ and $T : W \to V$ be a continuous linear mapping. Then the graph $G = \{(x, T(x)) \mid x \in W\}$ is closed in $U \times V$.*

PROOF:
$\langle 1 \rangle 1$. Assume: w.l.o.g. $T \neq 0$
$\langle 1 \rangle 2$. Let: $(x, y) \in (U \times V) - G$, i.e. $y \neq T(x)$
$\langle 1 \rangle 3$. Let: $\epsilon = \|y - T(x)\| > 0$
$\langle 1 \rangle 4$. Let: $x' \in W$ with $\|x - x'\| < \epsilon / 3 \|T\|$
$\langle 1 \rangle 5$. Let: $y' \in V$ with $\|y - y'\| < \epsilon / 3$
$\langle 1 \rangle 6$. $y' \neq T(x')$

PROOF:

$$\|y' - T(x')\| \geq \|y - T(x)\| - \|y - y'\| - \|T(x) - T(x')\|$$
$$> \epsilon/3$$
$$> 0$$

☐

**Theorem 18.2.18** (Diagonal Theorem). *Let $E$ be a normed space over $K$. Let $(x_{ij})$ be an infinite matrix of elements of $V$. If:*

1. *For all $j \in \mathbb{Z}_+$, we have $x_{ij} \to 0$ as $i \to \infty$;*

2. *Every increasing sequence of positive integers $(p_j)$ has a subsequence $(p_{j_r})$ such that*

$$\sum_{s=1}^{\infty} x_{p_{j_r} p_{j_s}} \to 0 \ as \ r \to \infty$$

*then $x_{ii} \to 0$ as $i \to \infty$.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: for a contradiction $x_{ii} \not\to 0$ as $i \to \infty$
$\langle 1 \rangle 2$. PICK $\epsilon > 0$ such that, for all $N$, there exists $n \geq N$ such that $\|x_{nn}\| \geq \epsilon$
$\langle 1 \rangle 3$. PICK an increasing sequence of integers $(p_j)$ such that $\|x_{p_j p_j}\| \geq \epsilon$ for all $j$.
$\langle 1 \rangle 4$. PICK a subsequence $(q_i)$ such that $\sum_{j=1}^{\infty} x_{q_i q_j} \to 0$ as $i \to \infty$
$\langle 1 \rangle 5$. For all $i$, we have $x_{q_i q_j} \to 0$ as $j \to \infty$
$\langle 1 \rangle 6$. For all $j$, we have $x_{q_i q_j} \to 0$ as $i \to \infty$
$\langle 1 \rangle 7$. Define a subsequence $(r_n)$ of $(q_i)$ by $r_1 = q_1$ and, for all $n$, $r_{n+1}$ is the first entry such that $r_{n+1} > r_n$, $\|x_{q_i r_n}\| < \epsilon/2^{n+1}$ for all $q_i \geq r_{n+1}$, and $\|x_{r_j r_{n+1}}\| < \epsilon/2^{n+2}$ for $j = 1, \ldots, n$.
$\langle 1 \rangle 8$. $\|x_{r_i r_j}\| < \epsilon/2^{j+1}$ for all $i, j$ such that $i \neq j$
$\langle 1 \rangle 9$. PICK a subsequence $(s_j)$ of $(r_j)$ such that $\sum_{j=1}^{\infty} x_{s_i s_j} \to 0$ as $i \to \infty$
$\langle 1 \rangle 10$. For all $i$ we have $\|\sum_{j=1}^{\infty} x_{s_i s_j}\| \geq \epsilon/2$
   PROOF:

$$\left\| \sum_{j=1}^{\infty} x_{s_i s_j} \right\| = \left\| x_{s_i s_i} + \sum_{i \neq j} x_{s_i s_j} \right\|$$

$$\geq \left| \|x_{s_i s_i}\| - \left\| \sum_{i \neq j} x_{s_i s_j} \right\| \right| \qquad \text{(Proposition 18.0.4)}$$

$$\geq \left| \|x_{s_i s_i}\| - \sum_{i \neq j} \|x_{s_i s_j}\| \right|$$

$$\geq \epsilon/2 \qquad\qquad\qquad (\langle 1 \rangle 2, \langle 1 \rangle 8)$$

$\langle 1 \rangle 11$. Q.E.D.
   PROOF: $\langle 1 \rangle 9$ and $\langle 1 \rangle 10$ form a contradiction.

☐

## 18.3   Banach Spaces

**Definition 18.3.1** (Cauchy Sequence)**.** Let $V$ be a normed space over $K$. A *Cauchy sequence* is a sequence of points $(x_n)$ such that, for every $\epsilon > 0$, there exists $N$ such that $\forall m, n \geq N.\|x_m - x_n\| < \epsilon$.

**Theorem 18.3.2.** *Let $V$ be a normed space over $K$. Let $(x_n)$ be a sequence in $V$. The following are equivalent.*

1. *$(x_n)$ is Cauchy.*

2. *For every pair of increasing sequences of positive integers $(p_n)$ and $(q_n)$, we have $\|x_{p_n} - x_{q_n}\| \to 0$ as $n \to \infty$.*

3. *For every increasing sequence of positive integers $(p_n)$, we have $\|x_{p_n} - x_n\| \to 0$ as $n \to \infty$.*

PROOF:
$\langle 1 \rangle 1.$  $1 \Rightarrow 2$
  $\langle 2 \rangle 1.$  ASSUME: $(x_n)$ is Cauchy.
  $\langle 2 \rangle 2.$  LET: $(p_n)$ and $(q_n)$ are increasing sequences of positive integers.
  $\langle 2 \rangle 3.$  LET: $\epsilon > 0$
  $\langle 2 \rangle 4.$  PICK $N$ such that $\forall m, n \geq N.\|x_m - x_n\| < \epsilon$
  $\langle 2 \rangle 5.$  $\forall n \geq N.\|x_{p_n} - x_{q_n}\| < \epsilon$
       PROOF: Since $p_n, q_n \geq n \geq N$.
$\langle 1 \rangle 2.$  $2 \Rightarrow 3$
  PROOF: Trivial.
$\langle 1 \rangle 3.$  $2 \Rightarrow 1$
  $\langle 2 \rangle 1.$  ASSUME: $(x_n)$ is not Cauchy
  $\langle 2 \rangle 2.$  Pick $\epsilon > 0$ such that, for every $N \in \mathbb{Z}_+$, there exist $m_N, n_N \geq N$ such that $\|x_{m_N} - x_{n_N}\| \geq \epsilon$
  $\langle 2 \rangle 3.$  ASSUME: w.l.o.g. $(m_N)$ and $(n_N)$ are increasing sequences.
  $\langle 2 \rangle 4.$  $\|x_{m_N} - x_{n_N}\| \not\to 0$ as $N \to \infty$.
$\langle 1 \rangle 4.$  $3 \Rightarrow 2$
  $\langle 2 \rangle 1.$  ASSUME: 3
  $\langle 2 \rangle 2.$  LET: $(p_n)$ and $(q_n)$ be increasing sequences of positive integers.
  $\langle 2 \rangle 3.$  LET: $\epsilon > 0$
  $\langle 2 \rangle 4.$  PICK $N$ such that $\forall n \geq N.\|x_{p_n} - x_n\| < \epsilon/2$ and $\forall n \geq N.\|x_{q_n} - x_n\| < \epsilon/2$
  $\langle 2 \rangle 5.$  $\forall n \geq N.\|x_{p_n} - x_{q_n}\| < \epsilon$
□

**Proposition 18.3.3.** *Every convergent sequence is Cauchy.*

PROOF:
$\langle 1 \rangle 1.$  LET: $x_n \to l$ as $n \to \infty$.
$\langle 1 \rangle 2.$  LET: $\epsilon > 0$
$\langle 1 \rangle 3.$  PICK $N$ such that $\forall n \geq N.\|x_n - l\| < \epsilon/2$

$\langle 1 \rangle 4$. For all $m, n \geq N$ we have $\|x_m - x_n\| < \epsilon$.

$\square$

**Proposition 18.3.4.** *In* $\mathcal{P}([0,1])$, *let*

$$P_n(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!} \ .$$

*Then* $(P_n)$ *is Cauchy but does not converge.*

PROOF: It converges to $e^x$ in $\mathcal{C}([0,1])$, therefore it is Cauchy in $\mathcal{C}([0,1])$, hence Cauchy in $\mathcal{P}([0,1])$. Since $e^x \notin \mathcal{P}([0,1])$, it does not converge in that space. $\square$

**Proposition 18.3.5.** *Let* $V$ *be a normed space over* $K$. *Let* $(x_n)$ *be a Cauchy sequence in* $V$. *Then* $(\|x_n\|)$ *converges in* $\mathbb{R}$.

PROOF:
$\langle 1 \rangle 1$. $(\|x_n\|)$ is Cauchy.
  $\langle 2 \rangle 1$. LET: $\epsilon > 0$
  $\langle 2 \rangle 2$. PICK $N$ such that $\forall m, n \geq N.\|x_m - x_n\| < \epsilon$
  $\langle 2 \rangle 3$. $\forall m, n \geq N.|\|x_m\| - \|x_n\|| < \epsilon$
    PROOF: Proposition 18.0.4.
$\langle 1 \rangle 2$. Q.E.D.
  PROOF: Since every Cauchy sequence in $\mathbb{R}$ converges.

$\square$

**Proposition 18.3.6.** *Every Cauchy sequence is bounded.*

PROOF:
$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2$. LET: $(x_n)$ be a Cauchy sequence in $V$.
$\langle 1 \rangle 3$. PICK $N$ such that $\forall m, n \geq N.\|x_m - x_n\| < 1$.
$\langle 1 \rangle 4$. LET: $B = \max(\|x_1\|, \ldots, \|x_{N-1}\|, \|x_N\| + 1$
$\langle 1 \rangle 5$. $\forall n.\|x_n\| \leq B$

$\square$

**Definition 18.3.7** (Banach Space)**.** A normed space $V$ over $K$ is *complete* or a *Banach space* iff every Cauchy sequence converges.

**Proposition 18.3.8.** $l^2$ *is complete.*

PROOF:
$\langle 1 \rangle 1$. LET: $(a_n)$ be a Cauchy sequence in $l^2$ where $a_n = (\alpha_{n1}, \alpha_{n2}, \ldots)$.
$\langle 1 \rangle 2$. For all $\epsilon > 0$, there exists $n_0 \in \mathbb{Z}_+$ such that $\forall m, n \geq n_0. \sum_{k=1}^{\infty} |\alpha_{mk} - \alpha_{nk}|^2 < \epsilon^2$.
$\langle 1 \rangle 3$. For every $k \in \mathbb{Z}_+$ and $\epsilon > 0$, there exists $n_0 \in \mathbb{Z}_+$ such that $\forall m, n \geq n_0.|\alpha_{mk} - \alpha_{nk}| < \epsilon$.
$\langle 1 \rangle 4$. For every $k \in \mathbb{Z}_+$, $(\alpha_{nk})$ is Cauchy in $\mathbb{C}$.
$\langle 1 \rangle 5$. For every $k \in \mathbb{Z}_+$, $(\alpha_{nk})$ converges in $\mathbb{C}$.
$\langle 1 \rangle 6$. For $k \in \mathbb{Z}_+$,

LET: $\alpha_k = \lim_{n \to \infty} \alpha_{nk}$

$\langle 1 \rangle 7$. Let $a$ be the sequence $(\alpha_k)$

$\langle 1 \rangle 8$. For all $\epsilon > 0$, there exists $n_0$ such that $\forall n \geq n_0. \sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2 \leq \epsilon^2$.
   PROOF: Letting $m \to \infty$ in $\langle 1 \rangle 2$.

$\langle 1 \rangle 9$. $a \in l^2$

   $\langle 2 \rangle 1$. PICK $n_0$ such that $\forall n \geq n_0. \sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2 \leq 1$
      PROOF: $\langle 1 \rangle 8$

   $\langle 2 \rangle 2$. $(\alpha_k - \alpha_{n_0 k}) \in l^2$

   $\langle 2 \rangle 3$. $(\alpha_{n_0 k}) \in l^2$
      PROOF: By $\langle 1 \rangle 1$ since the sequence is $a_{n_0}$.

   $\langle 2 \rangle 4$. $(\alpha_k) \in l^2$
      PROOF: Proposition 16.0.2.

$\langle 1 \rangle 10$. $a_n \to a$ as $n \to \infty$
   PROOF: By $\langle 1 \rangle 8$ since $\|a - a_n\| = \sqrt{\sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2}$.

□

**Proposition 18.3.9.** *Let $a$ and $b$ be real numbers with $a < b$. The space $\mathcal{C}([a,b])$ is complete.*

PROOF:

$\langle 1 \rangle 1$. LET: $X = [a, b]$

$\langle 1 \rangle 2$. LET: $(f_n)$ be a Cauchy sequence in $\mathcal{C}([a,b])$.

$\langle 1 \rangle 3$. For all $\epsilon > 0$, there exists $n_0$ such that $\forall n, m \geq n_0. \|f_n - f_m\| < \epsilon$.

$\langle 1 \rangle 4$. For all $\epsilon > 0$, there exists $n_0$ such that $\forall n, m \geq n_0. \forall x \in X. |f_n(x) - f_m(x)| < \epsilon$.

$\langle 1 \rangle 5$. For all $x \in [a, b]$, $(f_n(x))$ is Cauchy.

$\langle 1 \rangle 6$. Define $f : [a, b] \to \mathbb{C}$ by $f(x) = \lim_{n \to \infty} f_n(x)$.

$\langle 1 \rangle 7$. For all $\epsilon > 0$, there exists $n_0$ such that $\forall n \geq n_0. \forall x \in X. |f_n(x) - f(x)| < \epsilon$
   PROOF: Letting $m \to \infty$ in $\langle 1 \rangle 4$.

$\langle 1 \rangle 8$. $f$ is continuous

   $\langle 2 \rangle 1$. LET: $x_0 \in X$

   $\langle 2 \rangle 2$. LET: $\epsilon > 0$

   $\langle 2 \rangle 3$. PICK $n_0$ such that $\forall n \geq n_0. \forall x \in X. |f_n(x) - f(x)| < \epsilon/3$
      PROOF: By $\langle 1 \rangle 7$.

   $\langle 2 \rangle 4$. PICK $\delta > 0$ such that $\forall x \in X. |x - x_0| < \delta \Rightarrow |f_{n_0}(x) - f_{n_0}(x_0)| < \epsilon/3$
      PROOF: Since $f_{n_0}$ is continuous.

   $\langle 2 \rangle 5$. LET: $x \in X$

   $\langle 2 \rangle 6$. ASSUME: $|x - x_0| < \delta$

   $\langle 2 \rangle 7$. $|f(x) - f(x_0)| < \epsilon$
      PROOF:
$$|f(x) - f(x_0)| \leq |f(x) - f_{n_0}(x)| + |f_{n_0}(x) - f_{n_0}(x_0)| + |f_{n_0}(x_0) - f(x_0)| \quad \text{(Triangle Inequality)}$$
$$< \epsilon/3 + \epsilon/3 + \epsilon/3 \qquad\qquad (\langle 2 \rangle 3, \langle 2 \rangle 4)$$
$$= \epsilon$$

$\langle 1 \rangle 9$. $(f_n)$ converges to $f$ uniformly.
   PROOF: From $\langle 1 \rangle 7$

□

**Definition 18.3.10** (Series)**.** Let $V$ be a normed space over $K$. A *convergent series* in $V$ is a sequence $(x_n)$ in $V$ such that $(x_1 + \cdots + x_n)$ is a convergent sequence, in which case we write $\sum_{n=1}^{\infty} x_n$ for its limit.

**Definition 18.3.11** (Absolutely Convergent Series)**.** Let $V$ be a normed space over $K$. An *absolutely convergent series* in $V$ is a sequence $(x_n)$ such that $\sum_{n=1}^{\infty} \|x_n\| < \infty$.

**Proposition 18.3.12.** *In $\mathcal{P}([0,1])$, the series $\sum_{n=0}^{\infty} x^n/n!$ is absolutely convergent but not convergent.*

PROOF: Proposition 18.3.4. $\square$

**Theorem 18.3.13.** *A normed space is complete if and only if every absolutely convergent series is convergent.*

PROOF:
$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.
$\langle 1 \rangle 2$. If $V$ is complete then every absolutely convergent series is convergent.
$\quad \langle 2 \rangle 1$. ASSUME: $V$ is complete.
$\quad \langle 2 \rangle 2$. LET: $\sum_{n=1}^{\infty} a_n$ be absolutely convergent in $V$.
$\quad \langle 2 \rangle 3$. For $n \in \mathbb{Z}_{+}$,
$\qquad$ LET: $s_n = \sum_{k=1}^{n} a_k$
$\qquad$ .
$\quad \langle 2 \rangle 4$. $(s_n)$ is Cauchy.
$\quad \quad \langle 3 \rangle 1$. LET: $\epsilon > 0$
$\quad \quad \langle 3 \rangle 2$. PICK $k$ such that $\sum_{n=k+1}^{\infty} \|a_n\| < \epsilon$
$\quad \quad \langle 3 \rangle 3$. LET: $m > n > k$
$\quad \quad \langle 3 \rangle 4$. $\|s_m - s_n\| < \epsilon$
$\quad \quad \quad$ PROOF:

$$\|s_m - s_n\| = \left\| \sum_{i=n+1}^{m} a_i \right\| \qquad (\langle 2 \rangle 3, \langle 3 \rangle 3)$$

$$\leq \sum_{i=s+1}^{m} \|a_i\| \qquad \text{(Triangle inequality)}$$

$$\leq \sum_{i=k+1}^{\infty} \|a_i\|$$

$$< \epsilon \qquad (\langle 3 \rangle 2, \langle 3 \rangle 3)$$

$\quad \langle 2 \rangle 5$. $(s_n)$ converges.
$\langle 1 \rangle 3$. If every absolutely convergent series is convergent then $V$ is complete.
$\quad \langle 2 \rangle 1$. ASSUME: Every absolutely convergent series in $V$ is convergent.
$\quad \langle 2 \rangle 2$. LET: $(a_n)$ be a Cauchy sequence in $V$.
$\quad \langle 2 \rangle 3$. PICK a strictly increasing sequence of positive integers $(p_n)$ such that
$\qquad \forall k. \forall m, n \geq p_k. \|x_m - x_n\| < 2^{-k}$.
$\quad \langle 2 \rangle 4$. $\sum_{k=1}^{\infty} (x_{p_{k+1}} - x_{p_k})$ is absolutely convergent.

PROOF:

$$\sum_{k=1}^{\infty} \|x_{p_{k+1}} - x_{p_k}\| < \sum_{k=1}^{\infty} 2^{-k} \qquad (\langle 2 \rangle 3)$$

$$< \infty$$

$\langle 2 \rangle 5.$ $\sum_{k=1}^{\infty}(x_{p_{k+1}} - x_{p_k})$ is convergent.
  PROOF: $\langle 2 \rangle 1,$ $\langle 2 \rangle 5$
$\langle 2 \rangle 6.$ LET: $s = \sum_{k=1}^{\infty}(x_{p_{k+1}} - x_{p_k})$
$\langle 2 \rangle 7.$ $x_{p_k} \to s + x_{p_1}$ as $k \to \infty$.
  $\langle 3 \rangle 1.$ $\sum_{i=1}^{k}(x_{p_{i+1}} - x_{p_i}) \to s$ as $k \to \infty$
    PROOF: $\langle 2 \rangle 6$
  $\langle 3 \rangle 2.$ $x_{p_{k+1}} - x_{p_1} \to s$ as $k \to \infty$
$\langle 2 \rangle 8.$ $x_n \to s + x_{p_1}$ as $k \to \infty$.
  PROOF:
  $\langle 3 \rangle 1.$ LET: $\epsilon > 0$
  $\langle 3 \rangle 2.$ PICK $N$ such that $\forall k \geq N.\|x_{p_k} - (s + x_{p_1})\| < \epsilon/2$ and $\forall m, n \geq N.\|x_m - x_n\| < \epsilon/2$
    PROOF: $\langle 2 \rangle 2,$ $\langle 2 \rangle 7$
  $\langle 3 \rangle 3.$ $\forall n \geq N.\|x_n - (s + x_{p_1})\| < \epsilon$

$\Box$

**Theorem 18.3.14.** *A closed vector subspace of a Banach space is a Banach space.*

PROOF:
$\langle 1 \rangle 1.$ LET: $V$ be a Banach space over $K$.
$\langle 1 \rangle 2.$ LET: $U$ be a closed vector subspace of $V$.
$\langle 1 \rangle 3.$ LET: $(a_n)$ be a Cauchy sequence in $U$.
$\langle 1 \rangle 4.$ $(a_n)$ is a Cauchy sequence in $V$.
$\langle 1 \rangle 5.$ LET: $l = \lim_{n \to \infty} a_n$
$\langle 1 \rangle 6.$ $l \in U$
  PROOF: Theorem 18.1.40.
$\langle 1 \rangle 7.$ $a_n \to l$ as $n \to \infty$ in $U$.
$\Box$

**Definition 18.3.15** (Completion). Let $V$ be a normed space over $K$. A *completion* of $V$ consists of a normed space $W$ over $K$ and an injection $\phi : V \to W$ such that:

1. $\forall x, y \in V. \forall \alpha, \beta \in K. \phi(\alpha x + \beta y) = \alpha \phi(x) + \beta \phi(y)$

2. $\forall x \in V.\|\phi(x)\| = \|x\|$

3. $\phi(V)$ is dense in $W$.

4. $W$ is complete.

**Proposition 18.3.16.** *Every normed space has a completion.*

PROOF:

$\langle 1 \rangle 1$. LET: $V$ be a normed space over $K$.

$\langle 1 \rangle 2$. Let us say two Cauchy sequences $(x_n)$, $(y_n)$ ore *equivalent* iff $x_n - y_n \to 0$ as $n \to \infty$.

$\langle 1 \rangle 3$. Equivalence is an equivalence relation on the set of Cauchy sequences.

$\langle 1 \rangle 4$. LET: $W$ be the set of Cauchy sequences in $V$ quotiented by equivalence.

$\langle 1 \rangle 5$. Define addition and multiplication on $W$ by

$$[(x_n)] + [(y_n)] = [(x_n + y_n)]$$

$$\lambda[(x_n)] = [(\lambda x_n)]$$

$\langle 1 \rangle 6$. Define a norm on $W$ by $\|[(x_n)]\| = \lim_{n \to \infty} \|x_n\|$

$\langle 1 \rangle 7$. Define $\phi : V \to W$ by $\phi(v) = [(v)]$.

$\langle 1 \rangle 8$. $\phi$ is injective.

$\langle 1 \rangle 9$. $\forall x, y \in V. \forall \alpha, \beta \in K. \phi(\alpha x + \beta y) = \alpha \phi(x) + \beta \phi(y)$

$\langle 1 \rangle 10$. $\forall x \in V. \|\phi(x)\| = \|x\|$

$\langle 1 \rangle 11$. $\phi(V)$ is dense in $W$.

$\quad \langle 2 \rangle 1$. LET: $[(a_n)] \in W$ and $\epsilon > 0$.

$\qquad$ PROVE: $\quad B([(a_n)], \epsilon)$ intersects $\phi(V)$.

$\quad \langle 2 \rangle 2$. PICK $N$ such that $\forall m, n \geq N. \|a_m - a_n\| < \epsilon/2$

$\quad \langle 2 \rangle 3$. $\phi(a_N) \in B([(a_n)], \epsilon)$

$\qquad$ PROOF:

$$\|[(a_n)] - \phi(a_N)\| = \lim_{n \to \infty} \|a_n - a_N\|$$

$$\leq \epsilon/2 \qquad\qquad (\langle 2 \rangle 2)$$

$$< \epsilon$$

$\langle 1 \rangle 12$. $W$ is complete.

$\quad \langle 2 \rangle 1$. LET: $(X_n)$ be a Cauchy sequence in $W$.

$\quad \langle 2 \rangle 2$. For $n \in \mathbb{Z}_+$, PICK $x_n \in V$ such that

$$\|\phi(x_n) - X_n\| < 1/n \ .$$

$\quad \langle 2 \rangle 3$. $(x_n)$ is Cauchy in $V$.

$\qquad \langle 3 \rangle 1$. LET: $\epsilon > 0$

$\qquad \langle 3 \rangle 2$. PICK $N$ such that $\forall m, n \geq N. \|X_n - X_m\| < \epsilon/3$ and $1/N < \epsilon/3$

$\qquad \langle 3 \rangle 3$. LET: $m, n \geq N$

$\qquad \langle 3 \rangle 4$. $\|x_m - x_n\| < \epsilon$

$\qquad\quad$ PROOF:

$$\|x_m - x_n\| = \|\phi(x_m) - \phi(x_n)\|$$

$$\leq \|\phi(x_m) - X_m\| + \|X_m - X_n\| + \|X_n - \phi(x_n)\|$$

$$< \|X_m - X_n\| + 1/m + 1/n$$

$$< \epsilon$$

$\quad \langle 2 \rangle 4$. LET: $X = [(x_n)]$

$\quad \langle 2 \rangle 5$. $X_n \to X$ as $n \to \infty$

$\qquad$ PROOF:

$$\|X_n - X\| \leq \|X_n - \phi(x_n)\| + \|\phi(x_n) - X\|$$

$$< \|\phi(x_n) - X\| + 1/n$$

$$\to 0 \qquad\qquad\qquad \text{as } n \to \infty$$

$\square$

**Proposition 18.3.17.** *Let $U$ be a normed space and $V$ a Banach space. Then $\mathcal{B}(U,V)$ is a Banach space.*

PROOF:
$\langle 1\rangle 1.$ LET: $(T_n)$ be a Cauchy sequence in $\mathcal{B}(U,V)$
$\langle 1\rangle 2.$ For all $u \in U$, $(T_n(u))$ is a Cauchy sequence in $V$.
  $\langle 2\rangle 1.$ LET: $u \in U$
  $\langle 2\rangle 2.$ LET: $\epsilon > 0$
       PROVE:   $\exists N.\forall m, n \geq N.\|T_m(u) - T_n(u)\| < \epsilon$
  $\langle 2\rangle 3.$ ASSUME: w.l.o.g. $u \neq 0$
  $\langle 2\rangle 4.$ PICK $N$ such that $\forall m, n \geq N.\|T_m - T_n\| < \epsilon/\|u\|$
  $\langle 2\rangle 5.$ LET: $m, n \geq N$
  $\langle 2\rangle 6.$ $\|T_m(u) - T_n(u)\| < \epsilon$
     PROOF:
$$\|T_m(u) - T_n(u)\| \leq \|T_m - T_n\|\|u\| \qquad \text{(Proposition 18.2.11)}$$
$$< \epsilon$$
$\langle 1\rangle 3.$ Define $T : U \to V$ by $T(u) = \lim_{n\to\infty} T_n(u)$
$\langle 1\rangle 4.$ $T \in \mathcal{B}(U,V)$
  $\langle 2\rangle 1.$ For all $x, y \in U$ and $\alpha, \beta \in K$ we have $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$
    $\langle 3\rangle 1.$ LET: $x, y \in U$
    $\langle 3\rangle 2.$ LET: $\alpha, \beta \in K$
    $\langle 3\rangle 3.$ $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$
       PROOF:
$$\begin{aligned} T(\alpha x + \beta y) &= \lim_{n\to\infty} T_n(\alpha x + \beta y) \\ &= \lim_{n\to\infty} (\alpha T_n(x) + \beta T_n(y)) \\ &= \alpha T(x) + \beta T(y) \end{aligned}$$
  $\langle 2\rangle 2.$ $T$ is bounded.
    $\langle 3\rangle 1.$ PICK $N$ such that $\forall n \geq N.\|T_n - T\| < 1$
    $\langle 3\rangle 2.$ PICK $B > 0$ such that $\forall x \in U.\|T_N(x)\| \leq B\|x\|$
    $\langle 3\rangle 3.$ LET: $x \in U$
    $\langle 3\rangle 4.$ $\|T(x)\| \leq (B + 1)\|x\|$
       PROOF:
$$\begin{aligned} \|T(x)\| &\leq \|T_N(x) - T(x)\| + \|T(x)\| & \text{(Triangle inequality)} \\ &\leq \|T_N - T\|\|x\| + \|T\|\|x\| & \text{(Proposition 18.2.11)} \\ &< \|x\| + B\|x\| & (\langle 3\rangle 1, \langle 3\rangle 2) \\ &= (B + 1)\|x\| \end{aligned}$$
$\langle 1\rangle 5.$ $T_n \to T$ as $n \to \infty$
  $\langle 2\rangle 1.$ LET: $\epsilon > 0$
  $\langle 2\rangle 2.$ PICK $N$ such that $\forall m, n \geq N.\|T_m - T_n\| < \epsilon/2$
  $\langle 2\rangle 3.$ LET: $n \geq N$
       PROVE:   $\|T_n - T\| < \epsilon$
  $\langle 2\rangle 4.$ LET: $x \in U$ with $\|x\| = 1$
  $\langle 2\rangle 5.$ $\|T_n(x) - T(x)\| \leq \epsilon/2$
     PROOF: Let $n \to \infty$ in $\langle 2\rangle 2$.

▢

**Corollary 18.3.17.1.** *For any normed space $V$ over $K$, the space $\mathcal{B}(V, K)$ is a Banach space.*

**Theorem 18.3.18.** *Let $U$ be a normed space and $V$ a Banach space. Let $W$ be a subspace of $U$. Let $T : W \to V$ be a continuous linear transformation. Then $T$ has a unique extension to a continuous linear transformation $\operatorname{cl} W \to V$.*

PROOF:
⟨1⟩1. Define $S : \operatorname{cl} W \to V$ by: $S(x) = \lim_{n \to \infty} T(x_n)$, where $(x_n)$ is any sequence in $W$ that converges to $x$.
  ⟨2⟩1. For all $x \in \operatorname{cl} W$, there exists a sequence $(x_n)$ in $W$ that converges to $x$.
  PROOF: Theorem 18.1.43.
  ⟨2⟩2. If $(x_n)$ is a Cauchy sequence in $W$ then $(T(x_n))$ is Cauchy in $V$.
    ⟨3⟩1. ASSUME: w.l.o.g. $T \neq 0$
    ⟨3⟩2. LET: $(x_n)$ be a Cauchy sequence in $W$.
    ⟨3⟩3. PICK $B > 0$ such that $\forall x \in W.\|T(x)\| \leq B\|x\|$
    ⟨3⟩4. LET: $\epsilon > 0$
    ⟨3⟩5. PICK $N$ such that $\forall m, n \geq N.\|x_m - x_n\| < \epsilon/\|T\|$
    ⟨3⟩6. LET: $m, n \geq N$
    ⟨3⟩7. $\|T(x_m) - T(x_n)\| < \epsilon$
  ⟨2⟩3. If $(x_n)$ and $(y_n)$ are sequences in $W$ that converge to the same element in $\operatorname{cl} W$ then $(T(x_n))$ and $(T(y_n))$ have the same limit in $V$.
    ⟨3⟩1. ASSUME: w.l.o.g. $T \neq 0$
    ⟨3⟩2. ASSUME: $x_n \to l$ and $y_n \to l$ as $n \to \infty$
    ⟨3⟩3. LET: $T(x_n) \to a$ and $T(y_n) \to b$ as $n \to \infty$
    ⟨3⟩4. ASSUME: for a contradiction $a \neq b$
    ⟨3⟩5. LET: $\epsilon = \|a - b\|$
    ⟨3⟩6. PICK $N$ such that $\forall n \geq N.\|x_n - l\| < \epsilon/3\|T\|$ and $\forall n \geq N.\|y_n - l\| < \epsilon/3\|T\|$
    ⟨3⟩7. $\forall n \geq N.\|T(x_n) - T(y_n)\| < 2\epsilon/3$
    ⟨3⟩8. $\|a - b\| \leq 2\epsilon/3$
    ⟨3⟩9. This contradicts ⟨3⟩5.
⟨1⟩2. $S$ extends $T$
  ⟨2⟩1. LET: $w \in W$
  ⟨2⟩2. $w \to w$ as $n \to \infty$
  ⟨2⟩3. $T(w) \to T(w)$ as $n \to \infty$
  ⟨2⟩4. $S(w) = T(w)$
⟨1⟩3. $S$ is bounded.
  ⟨2⟩1. LET: $x \in \operatorname{cl} W$
    PROVE: $\|S(x)\| \leq \|T\|\|x\|$
  ⟨2⟩2. PICK a sequence $(x_n)$ in $W$ that converges to $x$.
  ⟨2⟩3. $\|T(x_n)\| \leq \|T\|\|x_n\|$ for all $n$.
  ⟨2⟩4. $\|S(x)\| \leq \|T\|\|x\|$
  PROOF: Taking the limit as $n \to \infty$.
⟨1⟩4. $S$ is linear.

$\langle 2 \rangle 1$. LET: $x, y \in \operatorname{cl} W$ and $\alpha, \beta \in K$

$\langle 2 \rangle 2$. PICK sequences $(x_n)$ and $(y_n)$ in $W$ that converge to $x$ and $y$.

$\langle 2 \rangle 3$. $T(\alpha x_n + \beta y_n) = \alpha T(x_n) + \beta T(y_n)$ for all $n$.

$\langle 2 \rangle 4$. $S(\alpha x + \beta y) = \alpha S(x) + \beta S(y)$

   PROOF: Taking the limit as $n \to \infty$.

$\langle 1 \rangle 5$. $S$ is unique.

$\langle 2 \rangle 1$. LET: $S'$ be a continuous linear extension of $S$ defined on $\operatorname{cl} W$.

$\langle 2 \rangle 2$. LET: $x \in W$

   PROVE:   $S(x) = S'(x)$

$\langle 2 \rangle 3$. PICK a sequence $(x_n)$ in $W$ that converges to $x$.

$\langle 2 \rangle 4$. $T(x_n) = S'(x_n) \to S'(x)$ as $n \to \infty$

$\langle 2 \rangle 5$. $S'(x) = S(x)$

☐

**Corollary 18.3.18.1.** *Let $U$ be a normed space and $V$ a Banach space. Let $W$ be a dense subspace of $U$. Let $T : W \to V$ be a continuous linear transformation. Then $T$ has a unique extension to a continuous linear transformation $U \to V$.*

**Definition 18.3.19** (Functional). Let $V$ be a normed space over $K$. A *functional* on $V$ is a bounded linear mapping $V \to K$. The *dual space* of $V$ is the space $\mathcal{B}(V, K)$ of all functionals.

**Theorem 18.3.20** (Banach-Steinhaus Theorem). *Let $\mathcal{T}$ be a family of bounded linear mappings from a Banach space $X$ into a normed space $Y$. If, for every $x \in X$, there exists a constant $M_x$ such that $\forall T \in \mathcal{T}.\|T(x)\| \leq M_x$, then there exists a constant $M > 0$ such that $\forall T \in \mathcal{T}.\|T\| \leq M$.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: for a contradiction no such $M$ exists.

$\langle 1 \rangle 2$. For $n \in \mathbb{Z}_+$, PICK $T_n \in \mathcal{T}$ such that $\|T_n\| > n2^n$.

$\langle 1 \rangle 3$. For $n \in \mathbb{Z}_+$, PICK $x_n \in X$ such that $\|x_n\| = 1$ and $\|T_n(x_n)\| > n2^n$.

$\langle 1 \rangle 4$. For $n \in \mathbb{Z}_+$,

$$\left\| \frac{1}{n} T_n \left( \frac{x_n}{2^n} \right) \right\| > 1 \ .$$

$\langle 1 \rangle 5$. For $i, j \in \mathbb{Z}_+$,

   LET: $y_{ij} = \frac{1}{i} T_i(\frac{x_j}{2^j})$.

$\langle 1 \rangle 6$. For all $j \in \mathbb{Z}_+$, $y_{ij} \to 0$ as $i \to \infty$

$\langle 2 \rangle 1$. LET: $j \in \mathbb{Z}_+$

$\langle 2 \rangle 2$. PICK $M$ such that $\forall T \in \mathcal{T}.\|T(x_j/2^j)\| \leq M$

$\langle 2 \rangle 3$. For all $i$, $\|y_{ij}\| \leq M/i$

$\langle 1 \rangle 7$. For any increasing sequence of positive integers $(p_i)$, we have $\sum_{j=1}^{\infty} y_{p_i p_j} \to 0$ as $i \to \infty$

$\langle 2 \rangle 1$. LET: $(p_i)$ be an increasing sequence of positive integers.

$\langle 2 \rangle 2$. LET: $z = \sum_{j=1}^{\infty} x_{p_j}/2^{p_j}$

   PROOF: This converges by Theorem 18.3.13.

$\langle 2 \rangle 3$. PICK $C$ such that $\forall T \in \mathcal{T}.\|T(z)\| \leq C$

$\langle 2 \rangle 4$. For all $i$, $\| \sum_{j=1}^{\infty} y_{p_i p_j} \| \leq C/p_i$.

PROOF:

$$\left\| \sum_{j=1}^{\infty} y_{p_i p_j} \right\| = \left\| \sum_{j=1}^{\infty} \frac{1}{p_i} T_{p_i} \left( \frac{x_{p_j}}{2^{p_j}} \right) \right\| \qquad (\langle 1 \rangle 5)$$

$$= \frac{1}{p_i} \left\| T_{p_i} \left( \sum_{j=1}^{\infty} \frac{x_{p_j}}{2^{p_j}} \right) \right\| \qquad (T_{p_i} \text{ continuous})$$

$$= \frac{1}{p_i} \| T_{p_i}(z) \| \qquad (\langle 2 \rangle 2)$$

$$\leq \frac{C}{p_i} \qquad (\langle 2 \rangle 3)$$

$\langle 2 \rangle 5.$ $\sum_{j=1}^{\infty} y_{p_i p_j} \to 0$ as $i \to \infty$

$\langle 1 \rangle 8.$ $y_{ii} \to 0$ as $i \to \infty$

PROOF: Diagonal Theorem, $\langle 1 \rangle 6$, $\langle 1 \rangle 7$.

$\langle 1 \rangle 9.$ Q.E.D.

PROOF: $\langle 1 \rangle 4$ and $\langle 1 \rangle 8$ form a contradiction.

□

## 18.4   Contraction Mappings

**Definition 18.4.1** (Contraction Mapping)**.** Let $E$ be a normed space over $K$. Let $A \subseteq E$. A function $f : A \to E$ is a *contraction (mapping)* iff there exists a real $\alpha$ such that $0 < \alpha < 1$ and

$$\forall x, y \in A. \| f(x) - f(y) \| \leq \alpha \| x - y \| \ .$$

**Proposition 18.4.2.** *Contraction mappings are uniformly continuous.*

PROOF:

$\langle 1 \rangle 1.$ LET: $E$ be a normed space over $K$.

$\langle 1 \rangle 2.$ LET: $A \subseteq E$

$\langle 1 \rangle 3.$ LET: $f : A \to E$ be a contraction mapping.

$\langle 1 \rangle 4.$ PICK $\alpha$ such that $0 < \alpha < 1$ and $\forall x, y \in A. \| f(x) - f(y) \| \leq \alpha \| x - y \|$.

$\langle 1 \rangle 5.$ LET: $\epsilon > 0$

$\langle 1 \rangle 6.$ LET: $\delta = \epsilon / \alpha$

$\langle 1 \rangle 7.$ For all $x, y \in A$, if $\| x - y \| < \delta$ then $\| f(x) - f(y) \| < \epsilon$.

□

**Theorem 18.4.3** (Banach Fixed Point Theorem)**.** *Let $E$ be a Banach space over $K$. Let $F$ be a nonempty closed subset of $E$. Let $f : F \to F$ be a contraction mapping. Then there exists a unique $z \in F$ such that $f(z) = z$.*

PROOF:

$\langle 1 \rangle 1.$ PICK $\alpha$ such that $0 < \alpha < 1$ and
$$\forall x, y \in F. \| f(x) - f(y) \| \leq \alpha \| x - y \| \ .$$

$\langle 1 \rangle 2.$ PICK $x_0 \in F$

$\langle 1 \rangle 3$. For $n \in \mathbb{Z}_+$,

    LET: $x_n = f^n(x_0)$.

$\langle 1 \rangle 4$. $(x_n)$ is a Cauchy sequence.

    $\langle 2 \rangle 1$. For all $n \in \mathbb{Z}_+$ we have $\|x_{n+1} - x_n\| \leq \alpha^n \|x_1 - x_0\|$.

    $\langle 2 \rangle 2$. For all $m, n \in \mathbb{Z}_+$ with $m < n$ we have $\|x_n - x_m\| < \alpha^m \|x_1 - x_0\|/(1-\alpha)$.

    PROOF:

$$\|x_n - x_m\| \leq \|x_n - x_{n-1}\| + \|x_{n-1} - x_{n-2}\| + \cdots + \|x_{m+1} - x_m\| \quad \text{(Triangle inequality)}$$

$$\leq (\alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha^m)\|x_1 - x_0\| \qquad\qquad (\langle 2 \rangle 1)$$

$$< \frac{\|x_1 - x_0\|}{1 - \alpha} \alpha^m$$

    $\langle 2 \rangle 3$. LET: $\epsilon > 0$

    $\langle 2 \rangle 4$. PICK $N$ such that $\alpha^N \|x_1 - x_0\|/(1 - \alpha) < \epsilon$

    $\langle 2 \rangle 5$. For all $m, n \geq N$, we have $\|x_n - x_m\| < \epsilon$

$\langle 1 \rangle 5$. LET: $z = \lim_{n \to \infty} x_n$

$\langle 1 \rangle 6$. $f(z) = z$

    PROOF:

$$f(z) = f\left(\lim_{n \to \infty} x_n\right)$$

$$= \lim_{n \to \infty} f(x_n) \qquad\qquad \text{(Proposition 18.4.2)}$$

$$= \lim_{n \to \infty} x_{n+1}$$

$$= z$$

$\langle 1 \rangle 7$. For any $w \in F$, if $f(w) = w$ then $w = z$.

    $\langle 2 \rangle 1$. LET: $w \in F$

    $\langle 2 \rangle 2$. ASSUME: $f(w) = w$

    $\langle 2 \rangle 3$. $\|z - w\| \leq \alpha \|z - w\|$

      PROOF: $\|z - w\| = \|f(z) - f(w)\| \leq \alpha \|z - w\|$

    $\langle 2 \rangle 4$. $\|z - w\| = 0$

    $\langle 2 \rangle 5$. $z = w$

$\blacksquare$

# Chapter 19

# Inner Product Spaces

**Definition 19.0.1** (Inner Product Space)**.** Let $E$ be a complex vector space. An *inner product* on $E$ is a function $\langle \ , \ \rangle : E^2 \to \mathbb{C}$ such that, for all $x, y, z \in E$ and $\alpha, \beta \in \mathbb{C}$, we have:

1. $\langle x, y \rangle = \overline{\langle y, x \rangle}$

2. $\langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle$

3. $\langle x, x \rangle \geq 0$

4. If $\langle x, x \rangle = 0$ then $x = 0$

An *inner product space* consists of a complex vector space $V$ and an inner product on $V$.

**Proposition 19.0.2.** *Let $E$ be an inner product space. For any $x \in E$, we have $\langle x, x \rangle$ is real.*

Proof: Since $\langle x, x \rangle = \overline{\langle x, x \rangle}$. $\square$

**Proposition 19.0.3.**

$$\langle x, \alpha y + \beta z \rangle = \overline{\alpha} \langle x, y \rangle + \overline{\beta} \langle x, z \rangle$$

**Proposition 19.0.4.**

$$\langle 0, y \rangle = \langle x, 0 \rangle = 0$$

**Proposition 19.0.5.** *The function $\langle \vec{x}, \vec{y} \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$ is an inner product on $\mathbb{C}^n$.*

**Proposition 19.0.6.** *The function $\langle (x_n), (y_n) \rangle = \sum_{i=1}^{\infty} x_i \overline{y_i}$ is an inner product on $l^2$.*

**Proposition 19.0.7.** *The function $\langle f, g \rangle = \int_a^b f(x) \overline{g(x)} dx$ is an inner product on $\mathcal{C}([a, b])$.*

175

**Proposition 19.0.8.** *Let $p > 1$ and $\Omega \subseteq \mathbb{R}^N$. Let $L^p(\Omega)$ be the set of all functions $f : \Omega \to \mathbb{C}$ such that $|f|^p$ is Lebesgue integrable.*

*The function $\langle f, g \rangle = \int_\Omega f(x)\overline{g(x)}dx$ is an inner product on $L^2(\Omega)$.*

**Proposition 19.0.9.** *Let $E_1$ and $E_2$ be inner product spaces. Then the function $\langle (e_1, e_2), (e_1', e_2') \rangle = \langle e_1, e_1' \rangle + \langle e_2, e_2' \rangle$ is an inner product on $E_1 \times E_2$.*

**Definition 19.0.10** (Norm)**.** In an inner product space, define $\|x\| = \sqrt{\langle x, x \rangle}$.

**Proposition 19.0.11** (Schwarz's Inequality)**.** *In any inner product space,*

$$|\langle x, y \rangle| \leq \|x\|\|y\| \ .$$

*Equality holds iff $x$ and $y$ are linearly dependent.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: w.l.o.g. $y \neq 0$
$\langle 1 \rangle 2.$ $|\langle x, y \rangle| \leq \|x\|\|y\|$
  $\langle 2 \rangle 1.$ For all $\alpha \in \mathbb{C}$ we have $\langle x, x \rangle + \overline{\alpha}\langle x, y \rangle + \alpha\langle y, x \rangle + |\alpha|^2 \langle y, y \rangle$
    PROOF: The right-hand side is $\langle x + \alpha y, x + \alpha y \rangle$.
  $\langle 2 \rangle 2.$ $\langle x, x \rangle \langle y, y \rangle - |\langle x, y \rangle|^2 \geq 0$
    PROOF: Taking $\alpha = -\langle x, x \rangle / \langle y, y \rangle$ in $\langle 2 \rangle 1$.
$\langle 1 \rangle 3.$ If $|\langle x, y \rangle| = \|x\|\|y\|$ then $x$ and $y$ are linearly dependent.
  $\langle 2 \rangle 1.$ ASSUME: $|\langle x, y \rangle| = \|x\|\|y\|$
  $\langle 2 \rangle 2.$ $\langle x, y \rangle \langle y, x \rangle = \langle x, x \rangle \langle y, y \rangle$
  $\langle 2 \rangle 3.$ $\langle y, y \rangle x - \langle x, x \rangle y = 0$
    PROOF:
    $$\langle \langle y, y \rangle x - \langle x, y \rangle y, \langle y, y \rangle x - \langle x, y \rangle y \rangle = \langle y, y \rangle^2 \langle x, x \rangle - \langle y, y \rangle \langle y, x \rangle \langle x, y \rangle - \langle x, y \rangle \langle y, y \rangle \langle y, x \rangle + \langle x, y \rangle \langle y, x \rangle$$
    $$= 0$$
$\langle 1 \rangle 4.$ If $x$ and $y$ are linearly dependent then $|\langle x, y \rangle| = \|x\|\|y\|$
  $\langle 2 \rangle 1.$ ASSUME: $x$ and $y$ are linearly dependent.
  $\langle 2 \rangle 2.$ LET: $y = \alpha x$
  $\langle 2 \rangle 3.$ $|\langle x, y \rangle| = \|x\|\|y\|$
    PROOF:
    $$|\langle x, y \rangle| = |\langle x, \alpha x \rangle|$$
    $$= |\alpha||\langle x, x \rangle|$$
    $$= |\alpha|\|x\|^2$$
    $$= \|x\|\|\alpha x\|$$
    $$= \|x\|\|y\|$$

☐

**Corollary 19.0.11.1** (Triangle Inequality)**.** *In any inner product space,*

$$\|x + y\| \leq \|x\| + \|y\|$$

PROOF:

$$\begin{aligned}
\|x + y\|^2 &= \langle x + y, x + y \rangle \\
&= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\
&\leq \langle x, x \rangle + 2|\langle x, y \rangle| + \langle y, y \rangle \\
&\leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 \qquad \text{(Schwarz's Inequality)} \\
&= (\|x\| + \|y\|)^2 \qquad\qquad\qquad \square
\end{aligned}$$

**Corollary 19.0.11.2.** *The norm in an inner product space is a norm.*

**Theorem 19.0.12** (Parallelogram Law)**.** *In any inner product space,*

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

PROOF:

$\langle 1 \rangle 1. \ \|x + y\|^2 = \|x\|^2 + \langle x, y \rangle + \langle y, x \rangle + \|y\|^2$

$\langle 1 \rangle 2. \ \|x - y\|^2 = \|x\|^2 - \langle x, y \rangle - \langle y, x \rangle + \|y\|^2$

$\langle 1 \rangle 3.$ Q.E.D.

   PROOF: Add $\langle 1 \rangle 1$ and $\langle 1 \rangle 2$.

$\square$

**Proposition 19.0.13.** *Let $E$ be a normed space over $\mathbb{C}$. Then there exists an inner product on $E$ that induces the norm of $E$ iff $E$ satisfies the Parallelogram Law.*

PROOF: If $E$ satisfies the parallelogram law, define

$$\langle x, y \rangle = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2 + i\|x + iy\|^2 - i\|x - iy\|^2) \ .$$

**Definition 19.0.14** (Orthogonal)**.** Vectors $x$ and $y$ in an inner product space are *orthogonal*, $x \perp y$, iff $\langle x, y \rangle = 0$.

**Theorem 19.0.15** (Pythagorean Formula)**.** *If $x$ and $y$ are orthogonal then*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 \ .$$

**Definition 19.0.16** (Weak Convergence)**.** Let $E$ be an inner product space. Let $(x_n)$ be a sequence in $E$ and $l \in E$. Then $(x_n)$ *weakly converges* to $l$, $x_n \xrightarrow{w} l$ as $n \to \infty$, iff $\forall y \in E. \langle x_n, y \rangle \to \langle l, y \rangle$ as $n \to \infty$.

**Proposition 19.0.17.** *In any inner product space $E$, the inner product $\langle \ , \ \rangle : E^2 \to \mathbb{C}$ is continuous.*

PROOF:

$\langle 1 \rangle 1.$ LET: $x_n \to x$ and $y_n \to y$ in $E$.

$\langle 1 \rangle 2. \ \langle x_n, y_n \rangle \to \langle x, y \rangle$

   PROOF:

$$\begin{aligned}
|\langle x_n, y_n \rangle - \langle x, y \rangle| &\leq |\langle x_n, y_n \rangle - \langle x_n, y \rangle| + |\langle x_n, y \rangle - \langle x, y \rangle| \\
&= |\langle x_n, y_n - y \rangle| + |\langle x_n - x, y \rangle| \\
&\leq \|x_n\|\|y_n - y\| + \|x_n - x\|\|y\| \qquad \text{(Schwarz's Inequality)} \\
&\to 0
\end{aligned}$$

   using the fact that $(x_n)$ is bounded.

□

**Theorem 19.0.18.** *$x_n \to l$ if and only if $x_n \overset{w}{\to} l$ and $\|x_n\| \to \|x\|$.*

PROOF:

$\langle 1 \rangle 1$. If $x_n \to l$ then $x_n \overset{w}{\to} l$ and $\|x_n\| \to \|l\|$.

PROOF: Easy using the fact that the inner product is continuous.

$\langle 1 \rangle 2$. If $x_n \overset{w}{\to} l$ and $\|x_n\| \to \|l\|$ then $x_n \to l$.

  $\langle 2 \rangle 1$. ASSUME: $x_n \overset{w}{\to} l$ and $\|x_n\| \to \|l\|$

  $\langle 2 \rangle 2$. $\langle x_n, l \rangle \to \|l\|^2$

  $\langle 2 \rangle 3$. $\|x_n - l\| \to 0$

    PROOF:

$$
\begin{aligned}
\|x_n - l\|^2 &= \langle x_n - l, x_n - l \rangle \\
&= \langle x_n, x_n \rangle - \langle x_n, l \rangle - \langle l, x_n \rangle + \langle l, l \rangle \\
&= \|x_n\|^2 - \langle x_n, l \rangle - \overline{\langle x_n, l \rangle} + \|l\|^2 \\
&\to \|l\|^2 - 2\|l\|^2 + \|l\|^2 \\
&= 0
\end{aligned}
$$

□

**Theorem 19.0.19.** *Let $S$ be a subset of an inner product space $E$ such that span $S$ is dense in $E$. If $(x_n)$ is a bounded sequence in $E$ and, for all $y \in S$, we have $\langle x_n, y \rangle \to \langle x, y \rangle$ then $x_n \overset{w}{\to} x$.*

PROOF:

$\langle 1 \rangle 1$. For all $y \in \operatorname{span} S$, we have $\langle x_n, y \rangle \to \langle x, y \rangle$

$\langle 1 \rangle 2$. LET: $z \in E$

    PROVE:   $\langle x_n, z \rangle \to \langle x, z \rangle$

$\langle 1 \rangle 3$. LET: $\epsilon > 0$

    PROVE:   There exists $n_0$ such that $\forall n \geq n_0.|\langle x_n, z \rangle - \langle x, z \rangle| < \epsilon$

$\langle 1 \rangle 4$. PICK $M > 0$ such that $\|x\| \leq M$ and $\forall n \in \mathbb{Z}_+.\|x_n\| \leq M$.

$\langle 1 \rangle 5$. PICK $y_0 \in \operatorname{span} S$ such that $\|z - y_0\| < \epsilon/3M$

$\langle 1 \rangle 6$. PICK $n_0 \in \mathbb{Z}_+$ such that, for all $n \geq n_0$, we have $|\langle x_n, y_0 \rangle - \langle x, y_0 \rangle| < \epsilon/3$

$\langle 1 \rangle 7$. LET: $n \geq n_0$

$\langle 1 \rangle 8$. $|\langle x_n, z \rangle - \langle x, z \rangle| < \epsilon$

  PROOF:

$$
\begin{aligned}
|\langle x_n, z \rangle - \langle x, z \rangle| &\leq |\langle x_n, z \rangle - \langle x_n, y_0 \rangle| + |\langle x_n, y_0 \rangle - \langle x, y_0 \rangle| + |\langle x, y_0 \rangle - \langle x, z \rangle| \\
&< \|x_n\|\|z - y_0\| + \epsilon/3 + \|x\|\|y_0 - z\| \\
&< M(\epsilon/3M) + \epsilon/3 + M(\epsilon/3M) \\
&= \epsilon
\end{aligned}
$$

□

## 19.1   Orthonormal Bases

**Definition 19.1.1** (Orthogonal)**.** Let $V$ be an inner product space and $S \subseteq V$. Then $S$ is *orthogonal* iff any two distinct elements of $S$ are orthogonal.

**Definition 19.1.2** (Orthonormal)**.** Let $V$ be an inner product space and $S \subseteq V$.
Then $S$ is *orthonormal* iff it is orthogonal and $\forall x \in S.\|x\| = 1$.

**Proposition 19.1.3.** *Orthonormal sets are linearly independent.*

Proof:
$\langle 1 \rangle 1$. Let: $S$ be orthonormal
$\langle 1 \rangle 2$. Assume: $\alpha_1 e_1 + \cdots + \alpha_n e_n = 0$ where $e_1, \ldots, e_n \in S$
$\langle 1 \rangle 3$. $|\alpha_1|^2 + \cdots |\alpha_n|^2 = 0$
  Proof:

$$0 = \sum_{m=1}^{n} \langle 0, \alpha_m e_m \rangle$$
$$= \sum_{m=1}^{n} \langle \sum_{k=1}^{n} \alpha_k e_k, \alpha_m e_m \rangle$$
$$= \sum_{m=1}^{n} \sum_{k=1}^{n} \alpha_k \overline{\alpha_m} \langle e_k, e_m \rangle$$
$$= \sum_{k=1}^{n} |\alpha_k|^2$$

$\langle 1 \rangle 4$. $\alpha_1 = \cdots = \alpha_n = 0$
$\square$

**Proposition 19.1.4.** *In $l^2$, let $e_n$ be the sequence whose nth element is 1 and whose other elements are 0. Then $\{e_n \mid n \in \mathbb{Z}_+\}$ is orthonormal.*

**Proposition 19.1.5.** *In $L^2([-\pi, \pi])$, let $\phi_n(x) = e^{inx}/\sqrt{2\pi}$ for $n \in \mathbb{Z}$. Then $\{\phi_n \mid n \in \mathbb{Z}\}$ is orthonormal.*

**Definition 19.1.6** (Legendre Polynomials)**.** The *Legendre polynomials $P_n \in \mathbb{Q}[x]$* for $n \in \mathbb{N}$ are defined by

$$P_0 = 1$$
$$P_n = \frac{1}{2^n n!} \frac{d^n}{dx^n}(x^2 - 1)^n$$

**Proposition 19.1.7.** *Let $P_n$ be the nth Legendre polynomial. Then $\{P_n \mid n \in \mathbb{N}\}$ is orthogonal in $L^2([-1, 1])$.*

**Definition 19.1.8** (Hermite Polynomial)**.** The *Hermite polynomials $H_n \in \mathbb{R}[x]$* for $n \in \mathbb{N}$ are defined by

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2} \ .$$

**Proposition 19.1.9.** *Let $H_n$ be the nth Hermite polynomial. Then $\{e^{-x^2/2} H_n(x) \mid n \in \mathbb{N}\}$ is orthogonal in $L^2(\mathbb{R})$.*

**Theorem 19.1.10.** *Let $V$ be an inner product space. If $x_1, \ldots, x_n \in V$ are orthogonal then*

$$\left\| \sum_{i=1}^{n} x_i \right\|^2 = \sum_{i=1}^{n} \|x_i\|^2 \ .$$

**Theorem 19.1.11** (Bessel's Equality)**.** *Let $V$ be an inner product space. Let $x_1, \ldots, x_n \in V$ be orthonormal. Let $x \in V$. Then*

$$\left\| x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\|^2 = \|x\|^2 - \sum_{k=1}^{n} |\langle x, x_k \rangle|^2 \ .$$

PROOF:

$$\left\| x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\|^2 = \left\langle x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k, x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\rangle$$

$$= \langle x, x \rangle - \left\langle x, \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\rangle - \left\langle \sum_{k=1}^{n} \langle x, x_k \rangle x_k, x \right\rangle$$

$$+ \left\langle \sum_{k=1}^{n} \langle x, x_k \rangle x_k, \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\rangle$$

$$= \langle x, x \rangle - 2 \sum_{k=1}^{n} \langle x, x_k \rangle \langle x_k, x \rangle + \sum_{i=1}^{n} \sum_{j=1}^{n} \langle x, x_i \rangle \langle x_j, x \rangle \langle x_i, x_j \rangle$$

$$= \|x\|^2 - 2 \sum_{k=1}^{n} |\langle x, x_k \rangle|^2 + \sum_{i=1}^{n} \langle x, x_i \rangle \langle x_i, x \rangle$$

$$= \|x\|^2 - \sum_{k=1}^{n} |\langle x, x_k \rangle|^2 \qquad\qquad \square$$

**Corollary 19.1.11.1** (Bessel's Inequality)**.** *Let $V$ be an inner product space. Let $x_1, \ldots, x_n \in V$ be orthonormal. Let $x \in E$. Then*

$$\sum_{k=1}^{n} |\langle x, x_k \rangle|^2 \leq \|x\|^2 \ .$$

**Corollary 19.1.11.2.** *Orthonormal sequences are weakly convergent to 0.*

PROOF: Let $(x_n)$ be an orthonormal sequence. Taking the limit in Bessel's inequality we have $\sum_{k=1}^{\infty} |\langle x, x_k \rangle|^2 \leq \|x\|^2 < \infty$ and so $\langle x, x_k \rangle \to 0$ as $k \to \infty$. $\square$

**Corollary 19.1.11.3** (Generalized Fourier Series)**.** *Let $V$ be an inner product space. Let $(e_n)$ be an orthonormal sequence in $V$. For any $x \in V$, the* generalized Fourier series *of $x$ is*

$$\sum_{n=1}^{\infty} \langle x, e_n \rangle e_n \ ,$$

*and $\langle x, e_n \rangle$ is called the nth* generalized Fourier coefficient *of $x$ with respect to* $(e_n)$. *We have* $(\langle x, e_n \rangle e_n)_n \in l^2$.

**Definition 19.1.12** (Complete Orthonormal Sequence)**.** Let $E$ be an inner product space. Let $(x_n)$ be an orthonormal sequence in $E$. Then $(x_n)$ is *complete* iff, for all $x \in E$, we have

$$\sum_{n=1}^{\infty} \langle x, x_n \rangle x_n = x \ .$$

# Chapter 20

# Hilbert Spaces

**Definition 20.0.1** (Hilbert Space)**.** A *Hilbert space* is a complete inner product space.

**Proposition 20.0.2.** *For $n \in \mathbb{N}$, $\mathbb{C}^n$ is a Hilbert space.*

**Proposition 20.0.3.** *$l^2$ is a Hilbert space.*

**Proposition 20.0.4.** *$L^2(\mathbb{R})$ is a Hilbert space.*

**Proposition 20.0.5.** *$L^2([a, b])$ is a Hilbert space.*

**Proposition 20.0.6.** *Let $\rho$ be a measurable function on $[a, b]$ such that $\rho(x) > 0$ almost everywhere. Let $L^{2\rho}([a, b])$ be the set of all measurable functions $f : [a, b] \to \mathbb{C}$ such that*

$$\int_a^b |f(x)|^2 \rho(x) dx < \infty \ .$$

*Define an inner product on $L^{2\rho}([a, b])$ by*

$$\langle f, g \rangle = \int_a^b f(x)\overline{g(x)}\rho(x)dx \ .$$

*Then $L^{2\rho}([a, b])$ is a Hilbert space.*

**Proposition 20.0.7.** *Let $m$ and $N$ be positive integers. Let $\Omega$ be an open set in $\mathbb{R}^N$. Let $\tilde{H}^m(\Omega)$ be the set of all $f \in \mathcal{C}^m(\Omega)$ such that, for every $\alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbb{Z}_+^N$ with $|\alpha| := \alpha_1 + \cdots + \alpha_N \leq m$, we have*

$$D^\alpha f := \frac{\partial^{|\alpha|} f}{\partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \cdots \partial x_N^{\alpha_N}} \in L^2(\Omega) \ .$$

*Define an inner product on $\tilde{H}^m(\Omega)$ by*

$$\langle f, g \rangle := \int_\Omega \sum_\alpha D^\alpha f \overline{D^\alpha g} \ .$$

*Let $H^m(\Omega)$ be the completion of $\tilde{H}^m(\Omega)$. Then $H^m(\Omega)$ is a Hilbert space.*

**Theorem 20.0.8.** *Weakly convergent sequences in a Hilbert space are bounded.*

PROOF:
$\langle 1\rangle 1$. LET: $H$ be a Hilbert space.
$\langle 1\rangle 2$. LET: $(x_n)$ be a weakly convergent sequence in $H$.
$\langle 1\rangle 3$. For $n \in \mathbb{Z}_+$,
    LET: $f_n : H \to \mathbb{C}$, $f_n(x) = \langle x, x_n \rangle$
$\langle 1\rangle 4$. For $n \in \mathbb{Z}_+$, $f_n$ is a bounded linear functional.
$\langle 1\rangle 5$. For every $x \in H$, the sequence $(f_n(x))$ is bounded.
  PROOF: Since it converges.
$\langle 1\rangle 6$. PICK $M > 0$ such that, for all $n \in \mathbb{Z}_+$, we have $\|f_n\| \le M$.
  PROOF: Banach-Steinhaus Theorem, $\langle 1\rangle 4$, $\langle 1\rangle 5$.
$\langle 1\rangle 7$. $\forall n \in \mathbb{Z}_+.\|f_n\| = \|x_n\|$
  $\langle 2\rangle 1$. LET: $n \in \mathbb{Z}_+$
  $\langle 2\rangle 2$. $\|f_n\| \le \|x_n\|$
  PROOF: Since for all $x \in H$ we have $|f_n(x)| = |\langle x, x_n \rangle| \le \|x\|\|x_n\|$ by
  Schwarz's Inequality.
  $\langle 2\rangle 3$. $\|x_n\| \le \|f_n\|$
  PROOF: Since $\|x_n\|^2 = |\langle x_n, x_n \rangle| = |f_n(x_n)| \le \|f_n\|\|x_n\|$.
$\langle 1\rangle 8$. $\forall n \in \mathbb{Z}_+.\|x_n\| \le M$
  PROOF: $\langle 1\rangle 6$, $\langle 1\rangle 7$
$\square$

**Theorem 20.0.9.** *Let $H$ be a Hilbert space. Let $(x_n)$ be an orthonormal sequence in $H$ and let $(\alpha_n)$ be a sequence of complex numbers. Then the series $\sum_{n=1}^{\infty} \alpha_n x_n$ converges in $H$ if and only if $\sum_{n=1}^{\infty} |\alpha_n|$ converges in $\mathbb{R}$, in which case*

$$\left\|\sum_{n=1}^{\infty} \alpha_n x_n\right\|^2 = \sum_{n=1}^{\infty} |\alpha_n|^2 \ .$$

PROOF:
$\langle 1\rangle 1$. For $m > k > 0$ we have

$$\left\|\sum_{n=k}^{m} \alpha_n x_n\right\|^2 = \sum_{n=k}^{m} |\alpha_n|^2 \ .$$

  PROOF: Theorem 19.1.10.
$\langle 1\rangle 2$. If $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$ then $\sum_{n=1}^{\infty} \alpha_n x_n$ converges.
  $\langle 2\rangle 1$. ASSUME: $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$
  $\langle 2\rangle 2$. $(\sum_{n=1}^{m} \alpha_n x_n)_m$ is Cauchy.
  PROOF: From $\langle 1\rangle 1$.
  $\langle 2\rangle 3$. $\sum_{n=1}^{\infty} \alpha_n x_n$ converges.
$\langle 1\rangle 3$. If $\sum_{n=1}^{\infty} \alpha_n x_n$ converges then $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$.
  PROOF: From $\langle 1\rangle 1$.
$\langle 1\rangle 4$. If $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$ then

$$\left\|\sum_{n=1}^{\infty} \alpha_n x_n\right\|^2 = \sum_{n=1}^{\infty} |\alpha_n|^2 \ .$$

PROOF: From $\langle 1 \rangle 1$.

□

**Proposition 20.0.10.** *Every complete orthonormal sequence in a Hilbert space is a basis.*

PROOF:
$\langle 1 \rangle 1$. LET: $E$ be an inner product space.
$\langle 1 \rangle 2$. LET: $(e_n)$ be a complete orthonormal sequence in $E$.
$\langle 1 \rangle 3$. For all $x \in E$, there exists a sequence $(\alpha_n)$ in $\mathbb{C}$ such that $x = \sum_n \alpha_n e_n$.
  PROOF: Immediate from $\langle 1 \rangle 2$.
$\langle 1 \rangle 4$. If $\sum_n \alpha_n e_n = \sum_n \beta_n e_n$ then $\alpha_n = \beta_n$ for all $n$.
  $\langle 2 \rangle 1$. LET: $x = \sum_n \alpha_n e_n = \sum_n \beta_n e_n$
  $\langle 2 \rangle 2$. $\sum_n |\alpha_n - \beta_n|^2 = 0$
    PROOF:

$$
\begin{aligned}
0 = \|x - x\|^2 & \\
&= \left\| \sum_{n=1}^{\infty} \alpha_n e_n - \sum_{n=1}^{\infty} \beta_n e_n \right\|^2 \qquad\qquad (\langle 2 \rangle 1) \\
&= \left\| \sum_{n=1}^{\infty} (\alpha_n - \beta_n) e_n \right\|^2 \\
&= \sum_{n=1}^{\infty} |\alpha_n - \beta_n|^2 \qquad\qquad (\text{Theorem } 20.0.9)
\end{aligned}
$$

  $\langle 2 \rangle 3$. $\alpha_n = \beta_n$ for all $n$.

□

**Theorem 20.0.11.** *An orthonormal sequence $(x_n)$ in a Hilbert space $H$ is complete if and only if, for all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$ then $x = 0$.*

PROOF:
$\langle 1 \rangle 1$. If $(x_n)$ is complete then, for all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$ then $x = 0$.
  $\langle 2 \rangle 1$. ASSUME: $(x_n)$ is complete.
  $\langle 2 \rangle 2$. LET: $x \in H$
  $\langle 2 \rangle 3$. ASSUME: $\forall n. \langle x, x_n \rangle = 0$
  $\langle 2 \rangle 4$. $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n = 0$
$\langle 1 \rangle 2$. If, for all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$ then $x = 0$, then $(x_n)$ is complete.
  $\langle 2 \rangle 1$. ASSUME: For all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$, then $x = 0$.
  $\langle 2 \rangle 2$. LET: $y = x - \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$
  $\langle 2 \rangle 3$. For all $n$, $\langle y, x_n \rangle = 0$
    $\langle 3 \rangle 1$. LET: $n \in \mathbb{Z}_+$
    $\langle 3 \rangle 2$. $\langle y, x_n \rangle = 0$

PROOF:

$$\langle y, x_n \rangle = \left\langle x - \sum_{m=1}^{\infty} \langle x, x_m \rangle x_m, x_n \right\rangle$$

$$= \langle x, x_n \rangle - \sum_{m=1}^{\infty} \langle x, x_m \rangle \langle x_m, x_n \rangle$$

$$= \langle x, x_n \rangle - \langle x, x_n \rangle$$

$$= 0$$

$\langle 2 \rangle 4.$  $y = 0$
$\langle 2 \rangle 5.$  $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

□

**Theorem 20.0.12** (Parseval's Formula)**.** *Let $H$ be a Hilbert space. Let $(x_n)$ be an orthonormal sequence in $H$. Then $(x_n)$ is complete if and only if, for all $x \in H$,*

$$\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2 \ .$$

PROOF:
$\langle 1 \rangle 1.$ If $(x_n)$ is complete then for all $x \in H$ we have $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$.
  $\langle 2 \rangle 1.$ ASSUME: $(x_n)$ is complete.
  $\langle 2 \rangle 2.$ LET: $x \in H$
  $\langle 2 \rangle 3.$ $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$
    PROOF:

$$\|x\|^2 = \left\| \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n \right\|^2 \qquad\qquad (\langle 2 \rangle 1)$$

$$= \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2 \qquad\qquad \text{(Theorem 20.0.9)}$$

$\langle 1 \rangle 2.$ If, for all $x \in H$, we have $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$, then $(x_n)$ is complete.
  $\langle 2 \rangle 1.$ ASSUME: For all $x \in H$, we have $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$
  $\langle 2 \rangle 2.$ LET: $x \in H$
  $\langle 2 \rangle 3.$ $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

□

**Proposition 20.0.13.** *For $n \in \mathbb{Z}$, let $\pi_n(x) = e^{inx}/\sqrt{2\pi}$. Then $\{\pi_n \mid n \in \mathbb{Z}\}$ is a complete orthonormal set in $L^2([-\pi, \pi])$.*

TODO

**Proposition 20.0.14.** $B = \{1/\sqrt{2\pi}\} \cup \{\cos nx/\sqrt{\pi} \mid n \in \mathbb{Z}_+\} \cup \{\sin nx/\sqrt{\pi} \mid n \in \mathbb{Z}_+\}$ *is a complete orthonormal set in $L^2([-\pi, \pi])$.*

PROOF:
$\langle 1 \rangle 1.$ For all $f \in B$ we have $\|f\| = 1$
  $\langle 2 \rangle 1.$ $\|1/\sqrt{2\pi}\| = 1$

PROOF:

$$\|1/\sqrt{2\pi}\| = \int_{-\pi}^{\pi} dx/2\pi$$

$$= 1$$

$\langle 2 \rangle 2.$ For all $n \in \mathbb{Z}_+$ we have $\|\cos nx/\sqrt{\pi}\| = 1$

PROOF:

$$\|\cos nx/\sqrt{\pi}\| = 1/\pi \int_{-\pi}^{\pi} \cos^2 nx \, dx$$

$$= 1/2\pi \int_{-\pi}^{\pi} (\cos 2nx + 1) dx$$

$$= 1/2\pi \left[ 1/2n \sin 2nx + x \right]_{-\pi}^{\pi}$$

$$= (1/2\pi)(2\pi)$$

$$= 1$$

$\langle 2 \rangle 3.$ For all $n \in \mathbb{Z}_+$ we have $\|\sin nx/\sqrt{\pi}\| = 1$

PROOF:

$$\|\sin nx/\sqrt{\pi}\| = 1/\pi \int_{-\pi}^{\pi} \sin^2 nx \, dx$$

$$= -1/2\pi \int_{-\pi}^{\pi} (\cos 2nx - 1) dx$$

$$= -1/2\pi \left[ 1/2n \sin 2nx - x \right]_{-\pi}^{\pi}$$

$$= (-1/2\pi)(-2\pi)$$

$$= 1$$

$\langle 1 \rangle 2.$ For all $f, g \in B$ with $f \neq g$ we have $\langle f, g \rangle = 0$

$\langle 2 \rangle 1.$ $\langle 1, \cos nx \rangle = 0$

PROOF:

$$\int_{-\pi}^{\pi} \cos nx \, dx = \left[ 1/n \sin nx \right]_{-\pi}^{\pi}$$

$$= 0$$

$\langle 2 \rangle 2.$ $\langle 1, \sin nx \rangle = 0$

PROOF:

$$\int_{-\pi}^{\pi} \sin nx \, dx = \left[ -1/n \cos nx \right]_{-\pi}^{\pi}$$

$$= -1/n \cos n\pi + 1/n \cos n\pi$$

$$= 0$$

$\langle 2 \rangle 3.$ If $m \neq n$ then $\langle \cos mx, \cos nx \rangle = 0$

PROOF:

$$\int_{-\pi}^{\pi} \cos mx \cos nx \, dx = 1/2 \int_{-\pi}^{\pi} (\cos(n+m)x - \cos(n-m)x) dx$$

$$= 1/2 \left[ \frac{1}{n+m} \sin(n+m)x - \frac{1}{n-m} \sin(n-m)x \right]_{-\pi}^{\pi}$$

$$= 0$$

$\langle 2 \rangle 4.$ $\langle \cos mx, \sin nx \rangle = 0$

PROOF:
$$\int_{-\pi}^{\pi} \cos mx \sin nx \, dx = 1/2 \int_{-\pi}^{\pi} (\sin(n+m)x - \sin(n-m)x)dx$$
$$= 1/2 \left[ -\frac{1}{n+m} \cos(n+m)x + \frac{1}{n-m} \cos(n-m)x \right]_{-\pi}^{\pi}$$
$$= 0 \qquad\qquad\qquad (\cos \text{ is odd})$$

$\langle 2 \rangle 5$. If $m \neq n$ then $\langle \sin mx, \sin nx \rangle = 0$

PROOF:
$$\int_{-\pi}^{\pi} \sin mx \sin nx \, dx = 1/2 \int_{-\pi}^{\pi} (\cos(n-m)x - \cos(n+m)x)dx$$
$$= 1/2 \left[ \frac{1}{n-m} \sin(n-m)x - \frac{1}{n+m} \sin(n+m)x \right]_{-\pi}^{\pi}$$
$$= 0$$

$\langle 1 \rangle 3$. For all $f \in L^2([-\pi,\pi])$, if $\forall g \in B.\langle f,g \rangle = 0$ then $f = 0$

$\quad \langle 2 \rangle 1$. LET: $f \in L^2([-\pi,\pi])$

$\quad \langle 2 \rangle 2$. ASSUME: $\forall g \in B.\langle f,g \rangle = 0$

$\quad \langle 2 \rangle 3$. For all $n \in \mathbb{Z}$, $\langle f, e^{inx} \rangle = 0$

$\quad$ PROOF: Since $e^{inx} = \cos nx + i \sin nx$.

$\quad \langle 2 \rangle 4$. $f = 0$

$\quad$ PROOF: From Proposition 20.0.13.

$\square$

**Proposition 20.0.15.** $\{\frac{1}{\sqrt{\pi}}\} \cup \{\sqrt{\frac{2}{\pi}} \cos nx \mid n \in \mathbb{Z}_+\}$ *is a complete orthonormal set in* $L^2([0,\pi])$.

**Proposition 20.0.16.** $\{\sqrt{\frac{2}{\pi}} \sin nx \mid n \in \mathbb{Z}_+\}$ *is a complete orthonormal set in* $L^2([0,\pi])$.

**Definition 20.0.17** (Signum)**.** The *signum* function sgn $: \mathbb{R} \to \mathbb{R}$ is defined by

$$\text{sgn}\, x = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

**Definition 20.0.18** (Rademacher Functions)**.** The *Rademarcher functions* $R : \mathbb{N} \times [0,1] \to \{-1,0,1\}$ are defined by

$$R(m,x) = \text{sgn}(\sin(2^m \pi x)) \ .$$

**Proposition 20.0.19.** *The Rademacher functios* $\{R(m,-) \mid m \in \mathbb{N}\}$ *are orthonormal in* $L^2([0,1])$.

PROOF:

$\langle 1 \rangle 1$. $\forall m \in \mathbb{N}.\|R(m,-)\| = 1$

$\quad$ PROOF: $\int_0^1 \text{sgn}(\sin(2^m \pi x))^2 dx = 1$ since the integrand is 1 except for finitely many points in $[0,1]$.

⟨1⟩2. Given natural numbers $m \neq n$, we have $\langle R(m, -), R(n, -) \rangle = 0$

 ⟨2⟩1. Given reals $a$, $b$ and a natural number $m$, we have $\int_a^b R(m, x) dx = 0$ whenever $2^m(b - a)$ is an even integer.

 PROOF: If $m > 0$, or if $m = 0$ and $b - a$ is an even integer, then the regions where $R(m, x) = 1$ are isometric with the regions where $R(m, x) = -1$.

 ⟨2⟩2. LET: $m$ and $n$ be natural numbers with $n < m$.

 ⟨2⟩3. $\langle R(m, -), R(n, -) \rangle = 0$

 PROOF:

$$\int_0^1 R(m, x) R(n, x) dx = \sum_{k=1}^{2^n} \int_{\frac{k-1}{2^n}}^{\frac{k}{2^n}} R(m, x) R(n, x) dx$$

$$= \sum_{k=1}^{2^n} (-i)^{k+1} \int_{\frac{k-1}{2^n}}^{\frac{k}{2^n}} R(m, x) dx$$

$$= 0 \qquad\qquad \left( \langle 2 \rangle 1, \; 2^m \left( \frac{k}{2^n} - \frac{k-1}{2^n} \right) = 2^{m-n} \text{ is an even integer} \right)$$

☐

**Proposition 20.0.20.** *The set of Rademacher functions is not complete.*

PROOF:
⟨1⟩1. Define $f : [0, 1] \to \mathbb{C}$ by $f(x) = 0$ if $0 \leq x < 1/4$, $f(x) = 1$ if $1/4 \leq x \leq 3/4$, $f(x) = 0$ if $3/4 < x \leq 1$.

⟨1⟩2. $f \in L^2([0, 1])$

⟨1⟩3. $\langle R(0, -), f \rangle = 1/2$

⟨1⟩4. $\langle R(m, -), f \rangle = 0$ for $m \geq 1$

⟨1⟩5. $f \neq 1/2 R(0, -)$

☐

**Definition 20.0.21** (Walsh Functions)**.** Define the *Walsh functions* $W : \mathbb{N} \times [0, 1] \to \{-1, 0, 1\}$ as follows. Given $m \in \mathbb{N}$, let $m = \sum_{k=1}^n 2^{k-1} a_k$ where each $a_k$ is either 0 or 1. Then

$$W(m, x) = \prod_{k=1}^n R(k, x)^{a_k} \ .$$

**Proposition 20.0.22.** *The set of Walsh functions $\{W(m, -) \mid m \in \mathbb{N}\}$ is a compete orthonormal set.*

TODO