Mathematics

Robin Adams

July 26, 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 say two classes $\mathbf{A}$ and $\mathbf{B}$ are *equal*, and write $\mathbf{A} = \mathbf{B}$, iff $\forall x(x \in \mathbf{A} \leftrightarrow x \in \mathbf{B})$.

The following are all valid formulas of first-order logic:

Proposition Schema 1.1.1. *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{C}$*, the following are theorems:*

1. $\mathbf{A} = \mathbf{A}$
2. *If* $\mathbf{A} = \mathbf{B}$ *then* $\mathbf{B} = \mathbf{A}$*.*
3. *If* $\mathbf{A} = \mathbf{B}$ *and* $\mathbf{B} = \mathbf{C}$ *then* $\mathbf{A} = \mathbf{C}$*.*

Definition 1.1.2 (Subclass)**.** We say a class $\mathbf{A}$ is a *subclass* of $\mathbf{B}$, or $\mathbf{B}$ is a *superclass* of $\mathbf{A}$, or $\mathbf{B}$ *includes* $\mathbf{A}$, and write $\mathbf{A} \subseteq \mathbf{B}$ or $\mathbf{B} \supseteq \mathbf{A}$, iff every element of $\mathbf{A}$ is an element of $\mathbf{B}$. Otherwise we write $\mathbf{A} \nsubseteq \mathbf{B}$ or $\mathbf{B} \nsupseteq \mathbf{A}$.

We say $\mathbf{A}$ is a *proper* subclass of $\mathbf{B}$, $\mathbf{B}$ is a *proper* superclass of $\mathbf{A}$, or $\mathbf{B}$ *properly* includes $\mathbf{A}$, and write $\mathbf{A} \subsetneq \mathbf{B}$ or $\mathbf{B} \supsetneq \mathbf{A}$, iff in addition $\mathbf{A} \neq \mathbf{B}$.

The following are all valid formulas of first-order logic:

Proposition Schema 1.1.3. *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{C}$*, the following are theorems:*

1. $\mathbf{A} \subseteq \mathbf{A}$
2. *If* $\mathbf{A} \subseteq \mathbf{B}$ *and* $\mathbf{B} \subseteq \mathbf{A}$ *then* $\mathbf{A} = \mathbf{B}$.
3. *If* $\mathbf{A} \subseteq \mathbf{B}$ *and* $\mathbf{B} \subseteq \mathbf{C}$ *then* $\mathbf{A} \subseteq \mathbf{C}$.

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

Proposition 1.1.5. *For any class* $\mathbf{A}$*, we have* $\emptyset \subseteq \mathbf{A}$.

Proof: Vacuously, every element of $\emptyset$ is an element of $\mathbf{A}$. $\square$

Definition 1.1.6 (Universal Class)**.** The *universal class* $\mathbf{V}$ is $\{x \mid \top\}$.

Proposition 1.1.7. *For any class* $\mathbf{A}$*, we have* $\mathbf{A} \subseteq \mathbf{V}$.

Proof: Trivially, every element of $\mathbf{A}$ is an element of $\mathbf{V}$. $\square$

Definition 1.1.8 (Union)**.** The *union* of two classes $\mathbf{A}$ and $\mathbf{B}$ is the class $\mathbf{A} \cup \mathbf{B} = \{x \mid x \in \mathbf{A} \vee x \in \mathbf{B}\}$.

Proposition 1.1.9. *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$*, we have*

$$\begin{aligned} \mathbf{A} \cup \mathbf{B} &= \mathbf{B} \cup \mathbf{A} \\ \mathbf{A} \cup (\mathbf{B} \cup \mathbf{C}) &= (\mathbf{A} \cup \mathbf{B}) \cup \mathbf{C} \\ \mathbf{A} \cup \emptyset &= \mathbf{A} \end{aligned}$$

Proof: These are valid formulas of first-order logic. $\square$

Definition 1.1.10 (Intersection)**.** The *intersection* of two classes $\mathbf{A}$ and $\mathbf{B}$ is the class $\{x \mid x \in \mathbf{A} \wedge x \in \mathbf{B}\}$.

Proposition 1.1.11. *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$*, we have*

$$\begin{aligned} \mathbf{A} \cap \mathbf{B} &= \mathbf{B} \cap \mathbf{A} \\ \mathbf{A} \cap (\mathbf{B} \cap \mathbf{C}) &= (\mathbf{A} \cap \mathbf{B}) \cap \mathbf{C} \\ \mathbf{A} \cap \emptyset &= \emptyset \end{aligned}$$

Proof: These are valid formulas of first-order logic. $\square$

Proposition 1.1.12 (Distributive Laws)**.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$*, we have*

$$\begin{aligned} \mathbf{A} \cup (\mathbf{B} \cap \mathbf{C}) &= (\mathbf{A} \cup \mathbf{B}) \cap (\mathbf{A} \cup \mathbf{C}) \\ \mathbf{A} \cap (\mathbf{B} \cup \mathbf{C}) &= (\mathbf{A} \cap \mathbf{B}) \cup (\mathbf{A} \cap \mathbf{C}) \end{aligned}$$

Proof: These are valid formulas of first-order logic. $\square$

Definition 1.1.13 (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 $\bigcup\{t(x) \mid P(x)\}$.

Proposition 1.1.14. *For any classes* $\mathbf{A}$ *and* $\mathbf{B}$*, if* $\mathbf{A} \subseteq \mathbf{B}$ *then* $\bigcup \mathbf{A} \subseteq \bigcup \mathbf{B}$.

PROOF: First-order logic. □

Definition 1.1.15 (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 1.1.16 (Relative Complement)**.** Let $\mathbf{A}$ and $\mathbf{B}$ be classes. The *relative complement* of $\mathbf{B}$ in $\mathbf{A}$ is the class $\mathbf{A} - \mathbf{B} = \{x \in \mathbf{A} \mid x \notin \mathbf{B}\}$.

Proposition 1.1.17 (De Morgan's Laws)**.** *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, *we have*

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

PROOF: First-order logic. □

Proposition 1.1.18. *If* $\mathbf{A} \subseteq \mathbf{B}$ *then* $\mathbf{C} - \mathbf{B} \subseteq \mathbf{C} - \mathbf{A}$.

PROOF: First-order logic. □

Definition 1.1.19 (Symmetric Difference)**.** The *symmetric difference* of classes $\mathbf{A}$ and $\mathbf{B}$ is the class $\mathbf{A} + \mathbf{B} := (\mathbf{A} - \mathbf{B}) \cup (\mathbf{B} - \mathbf{A})$.

Proposition 1.1.20. *For any classes* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, *we have*

$$\mathbf{A} \cap (\mathbf{B} + \mathbf{C}) = (\mathbf{A} \cap \mathbf{B}) + (\mathbf{A} \cap \mathbf{C})$$
$$\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$$

PROOF: First-order logic. □

1.2 Axioms

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*.

Axiom 1.2.2 (Union)**.** *The union of a set is a set.*

Axiom 1.2.3 (Power Set)**.** *For any set A, the class $\mathcal{P}A = \{x \mid x \subseteq A\}$ is a set, called the* power set *of A.*

Axiom 1.2.4 (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 1.2.5 (Choice)**.** *For any set A of pairwise disjoint, nonempty sets, there exists a set C such that, for all $x \in A$, $x \cap C$ has exactly one element.*

Axiom Schema 1.2.6 (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 1.2.7 (Regularity)**.** *For any nonempty set A, there exists $m \in A$ such that $m \cap A = \emptyset$.*

1.3 Basic Constructions on Sets

1.3.1 Consequences of the Axioms

Proposition 1.3.1. *The class $\emptyset = \{x \mid \bot\}$ is a set.*

Proof: Immediate from the Axiom of Infinity. □

Proposition 1.3.2 (Pairing)**.** *For any sets a and b, the class $\{a, b\} = \{x \mid x = a \vee x = b\}$ 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 $P(x, y)$.
  $\langle 2 \rangle 1$. Let: $x \in \mathcal{P}\mathcal{P}\emptyset$
  $\langle 2 \rangle 2$. Let: y and y' be sets.
  $\langle 2 \rangle 3$. Assume: $P(x, y)$ and $P(x, y')$
  $\langle 2 \rangle 4$. $(x = \emptyset \wedge y = a) \vee (x = \mathcal{P}\emptyset \wedge y = b)$
    Proof: From $\langle 2 \rangle 3$.
  $\langle 2 \rangle 5$. $(x = \emptyset \wedge y' = a) \vee (x = \mathcal{P}\emptyset \wedge y' = b)$
    Proof: From $\langle 2 \rangle 3$.
  $\langle 2 \rangle 6$. $\emptyset \neq \mathcal{P}\emptyset$
    Proof: Since $\emptyset \in \mathcal{P}\emptyset$ and $\emptyset \notin \emptyset$.
  $\langle 2 \rangle 7$. $y = y'$
$\langle 1 \rangle 3$. Let: A be the set $\{y \mid \exists x \in \mathcal{P}\mathcal{P}\emptyset.P(x, y)\}$.
$\langle 1 \rangle 4$. $A = \{a, b\}$
□

Proposition 1.3.3. *The union of two sets is a set.*

Proof: The union of two sets A and B is $\bigcup\{A, B\}$. □

Proposition Schema 1.3.4. *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 $\{a_1, \ldots, a_n, a_{n+1}\} = \{a_1, \ldots, a_n\} \cup \{a_{n+1}\}$. □

Proposition 1.3.5. *For any classes* $\mathbf{A}$ *and* $\mathbf{B}$*, if* $\mathbf{A} \subseteq \mathbf{B}$ *then* $\bigcup \mathbf{A} \subseteq \bigcup \mathbf{B}$*.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: $\mathbf{A} \subseteq \mathbf{B}$
$\langle 1 \rangle 2$. LET: $x \in \bigcup \mathbf{A}$
$\langle 1 \rangle 3$. PICK $A \in \mathbf{A}$ such that $x \in A$
$\langle 1 \rangle 4$. $A \in \mathbf{B}$
$\langle 1 \rangle 5$. $x \in \bigcup \mathbf{B}$
$\square$

Proposition 1.3.6. *For any sets* A *and* B*, if* $A \subseteq B$ *then* $\mathcal{P}A \subseteq \mathcal{P}B$*.*

PROOF: From Proposition 1.1.3. $\square$

Proposition 1.3.7. *For any set* A *we have* $\bigcup \mathcal{P}A = A$*.*

PROOF:
$\langle 1 \rangle 1$. $\bigcup \mathcal{P}A \subseteq A$
  $\langle 2 \rangle 1$. LET: $x \in \bigcup \mathcal{P}A$
  $\langle 2 \rangle 2$. PICK $X \in \mathcal{P}A$ such that $x \in X$
    PROOF: $\langle 2 \rangle 1$
  $\langle 2 \rangle 3$. $X \subseteq A$
    PROOF: $\langle 2 \rangle 2$
  $\langle 2 \rangle 4$. $x \in A$
    PROOF: $\langle 2 \rangle 2$, $\langle 2 \rangle 3$
$\langle 1 \rangle 2$. $A \subseteq \bigcup \mathcal{P}A$
  PROOF: For all $x \in A$ we have $x \in \{x\} \in \mathcal{P}A$.
$\langle 1 \rangle 3$. Q.E.D.
  PROOF: By Proposition 1.1.3.
$\square$

1.3.2 Comprehension

Proposition Schema 1.3.8 (Comprehension)**.** *For any predicate* $P(x)$*, the following is a theorem:*
  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 1.3.8.1. *The intersection of a set and a class is a set.*

Corollary 1.3.8.2. *The intersection of a nonempty class is a set.*

PROOF:
$\langle 1\rangle 1$. LET: $\mathbf{A}$ be a nonempty class.
$\langle 1\rangle 2$. PICK$A \in \mathbf{A}$
$\langle 1\rangle 3$. $\bigcap \mathbf{A} = \{x \in A \mid \forall X \in \mathbf{A}. x \in X\}$ which is a set.
□

Corollary 1.3.8.3. *The relative complement of a class in a set is a set.*

Corollary 1.3.8.4 (Russell's Paradox)**.** $\mathbf{V}$ *is a proper class.*

PROOF:
$\langle 1\rangle 1$. LET: $\mathbf{R} = \{x \mid x \notin x\}$
$\langle 1\rangle 2$. $\mathbf{R}$ is a proper class.
$\langle 2\rangle 1$. ASSUME: for a contradiction $\mathbf{R}$ is a set
$\langle 2\rangle 2$. $\mathbf{R} \in \mathbf{R}$ iff $\mathbf{R} \notin \mathbf{R}$
$\langle 2\rangle 3$. This is a contradiction.
$\langle 1\rangle 3$. $\mathbf{V}$ is a proper class.
PROOF: From Comprehension and $\langle 1\rangle 2$.
□

Definition 1.3.9. For any sets A and B, the *relative complement* $A - B$ is the set $\{x \in A \mid x \notin B\}$.

Proposition 1.3.10 (Distributive Laws)**.** *For any set A and class $\mathbf{B}$, we have*

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

PROOF: First-order logic. □

Proposition 1.3.11 (De Morgan's Laws)**.** *For any set C and class $\mathbf{A}$, we have*

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

PROOF: First-order logic. □

1.4 Transitive Classes

Definition 1.4.1 (Transitive Class)**.** A class $\mathbf{A}$ is a *transitive class* iff whenever $x \in y \in \mathbf{A}$ then $x \in \mathbf{A}$.

Proposition 1.4.2. *Let A be a set. Then the following are equivalent.*

1. *A is a transitive class.*
2. $\bigcup A \subseteq A$
3. *Every element of A is a subset of A.*
4. $A \subseteq \mathcal{P}A$

PROOF: Immediate from definitions. □

Proposition 1.4.3. *For any set a, we have a is a transitive set if and only if $\mathcal{P}a$ is a transitive set.*

PROOF:
⟨1⟩1. If a is a transitive set then $\mathcal{P}a$ is a transitive set.
⟨2⟩1. ASSUME: a is a transitive set.
⟨2⟩2. $a \subseteq \mathcal{P}a$
PROOF: Proposition 1.4.2, ⟨2⟩1.
⟨2⟩3. $\mathcal{P}a \subseteq \mathcal{P}\mathcal{P}a$
PROOF: Proposition 1.3.6, ⟨2⟩2.
⟨2⟩4. $\mathcal{P}a$ is a transitive set.
PROOF: Proposition 1.4.2, ⟨2⟩3.
⟨1⟩2. If $\mathcal{P}a$ is a transitive set then a is a transitive set.
⟨2⟩1. ASSUME: $\mathcal{P}a$ is a transitive set.
⟨2⟩2. $\bigcup \mathcal{P}a \subseteq \mathcal{P}a$
PROOF: Proposition 1.4.2, ⟨2⟩1.
⟨2⟩3. $a \subseteq \mathcal{P}a$
PROOF: Proposition 1.3.7, ⟨2⟩2
⟨2⟩4. a is a transitive set.
PROOF: Proposition 1.4.2, ⟨2⟩3.
□

Proposition 1.4.4. *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: ⟨1⟩1, ⟨1⟩2
⟨1⟩4. $x \in \mathbf{A}$
PROOF: ⟨1⟩1, ⟨1⟩2, ⟨1⟩3
□

Proposition 1.4.5. *If every member of* $\mathbf{A}$ *is a transitive set then* $\bigcup \mathbf{A}$ *is a transitive class.*

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

Proposition 1.4.6. *If every member of* $\mathbf{A}$ *is a transitive set then* $\bigcap \mathbf{A}$ *is a transitive class.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: Every member of $\mathbf{A}$ is a transitive set.
$\langle 1 \rangle 2$. LET: $x \in y \in \bigcap \mathbf{A}$
PROVE: $x \in \bigcap \mathbf{A}$
$\langle 1 \rangle 3$. LET: $A \in \mathbf{A}$
$\langle 1 \rangle 4$. $y \in A$
$\langle 1 \rangle 5$. $x \in A$
$\square$

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. *If A and B are sets then $A \times B$ is a set.*

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

Proposition 2.1.5. *For any classes* $\mathbf{A}$*,* $\mathbf{B}$ *and* $\mathbf{C}$*, we have* $\mathbf{A} \times (\mathbf{B} \cup \mathbf{C}) = (\mathbf{A} \times \mathbf{B}) \cup (\mathbf{A} \times \mathbf{C})$*.*

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

Proposition 2.1.6. *If* $\mathbf{A} \times \mathbf{B} = \mathbf{A} \times \mathbf{C}$ *and* $\mathbf{A}$ *is nonempty then* $\mathbf{B} = \mathbf{C}$*.*

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

Proposition 2.1.7. *For any set* A *and class* $\mathbf{B}$*, we have* $A \times \bigcup \mathbf{B} = \bigcup \{A \times X \mid X \in \mathbf{B}\}$*.*

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

2.2 Relations

Definition 2.2.1 (Relation)**.** A *relation* is a class of ordered pairs.

Definition 2.2.2 (Domain)**.** The *domain* of a class $\mathbf{R}$ is the class

$$\operatorname{dom} \mathbf{R} := \{x \mid \exists y.(x, y) \in \mathbf{R}\} \ .$$

Definition 2.2.3 (Range)**.** The *range* of a class $\mathbf{R}$ is the class

$$\operatorname{ran} \mathbf{R} := \{x \mid \exists y.(y, x) \in \mathbf{R}\} \ .$$

Definition 2.2.4 (Field)**.** The *field* of a class $\mathbf{R}$ is the class

$$\operatorname{fld} \mathbf{R} := \operatorname{dom} \mathbf{R} \cup \operatorname{ran} \mathbf{R} \ .$$

Proposition 2.2.5. *For any set* R*, the classes* $\operatorname{dom} R$*,* $\operatorname{ran} R$*,* $\operatorname{fld} R$ *are sets.*

PROOF: They are all subsets of $\bigcup \bigcup R$. □

Definition 2.2.6 (Single-Rooted)**.** A class $\mathbf{R}$ is *single-rooted* iff, for all $y \in \operatorname{ran}\mathbf{R}$, there is exactly one x such that $(x, y) \in \mathbf{R}$.

Definition 2.2.7 (Inverse)**.** The *inverse* of a class $\mathbf{F}$ is the class

$$\mathbf{F}^{-1} := \{(x, y) \mid (y, x) \in \mathbf{F}\} \ .$$

Proposition 2.2.8. *For any class* $\mathbf{F}$*, we have* $\operatorname{dom}\mathbf{F}^{-1} = \operatorname{ran}\mathbf{F}$

PROOF:

$$\begin{aligned} y \in \operatorname{dom}\mathbf{F}^{-1} &\Leftrightarrow \exists x.(y, x) \in \mathbf{F}^{-1} \\ &\Leftrightarrow \exists x.(x, y) \in \mathbf{F} \\ &\Leftrightarrow y \in \operatorname{ran}\mathbf{F} \qquad \square \end{aligned}$$

Proposition 2.2.9. *For any class* $\mathbf{F}$*, we have* $\operatorname{ran}\mathbf{F}^{-1} = \operatorname{dom}\mathbf{F}$.

PROOF:

$$\begin{aligned} y \in \operatorname{ran}\mathbf{F}^{-1} &\Leftrightarrow \exists x.(x, y) \in \mathbf{F}^{-1} \\ &\Leftrightarrow \exists x.(y, x) \in \mathbf{F} \\ &\Leftrightarrow y \in \operatorname{dom}\mathbf{F} \qquad \square \end{aligned}$$

Proposition 2.2.10. *For any relation* $\mathbf{F}$*, we have* $(\mathbf{F}^{-1})^{-1} = \mathbf{F}$.

PROOF:

$$\begin{aligned} (x, y) \in (\mathbf{F}^{-1})^{-1} &\Leftrightarrow (y, x) \in \mathbf{F}^{-1} \\ &\Leftrightarrow (x, y) \in \mathbf{F} \qquad \square \end{aligned}$$

Definition 2.2.11 (Composition)**.** The *composition* of classes $\mathbf{F}$ and $\mathbf{G}$ is the class

$$\mathbf{F} \circ \mathbf{G} := \{(x, z) \mid \exists y.(x, y) \in \mathbf{G} \wedge (y, z) \in \mathbf{F}\} \ .$$

Proposition 2.2.12. *For any classes* $\mathbf{F}$ *and* $\mathbf{G}$*,*

$$(\mathbf{F} \circ \mathbf{G})^{-1} = \mathbf{G}^{-1} \circ \mathbf{F}^{-1} \ .$$

PROOF:

$$\begin{aligned} (z, x) \in (\mathbf{F} \circ \mathbf{G})^{-1} &\Leftrightarrow (x, z) \in \mathbf{F} \circ \mathbf{G} \\ &\Leftrightarrow \exists y.(x, y) \in \mathbf{G} \wedge (y, z) \in \mathbf{F} \\ &\Leftrightarrow \exists y.(y, x) \in \mathbf{G}^{-1} \wedge (z, y) \in \mathbf{F}^{-1} \\ &\Leftrightarrow (z, x) \in \mathbf{G}^{-1} \circ \mathbf{F}^{-1} \qquad \square \end{aligned}$$

Definition 2.2.13 (Restriction)**.** The *restriction* of the class $\mathbf{F}$ to the class $\mathbf{A}$ is the class $\mathbf{F} \restriction \mathbf{A} := \{(x, y) \mid x \in \mathbf{A}, (x, y) \in \mathbf{F}\}$.

Definition 2.2.14 (Image)**.** The *image* of the class $\mathbf{A}$ under the class $\mathbf{F}$ is the set $F(A) := \operatorname{ran}(F \restriction A) = \{y \mid \exists x \in \mathbf{A}.(x, y) \in \mathbf{F}\}$.

Proposition 2.2.15. *For any classes* $\mathbf{F}$*,* $\mathbf{A}$ *and* $\mathbf{B}$*, we have*

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

PROOF:

$$\begin{aligned} y \in \mathbf{F}(\mathbf{A} \cup \mathbf{B}) &\Leftrightarrow \exists x \in \mathbf{A} \cup \mathbf{B}.(x, y) \in \mathbf{F} \\ &\Leftrightarrow \exists x \in \mathbf{A}.(x, y) \in \mathbf{F} \vee \exists x \in \mathbf{B}.(x, y) \in \mathbf{F} \\ &\Leftrightarrow y \in \mathbf{F}(\mathbf{A}) \cup \mathbf{F}(\mathbf{B}) \end{aligned}$$

□

Proposition 2.2.16. *For any classes* $\mathbf{F}$ *and* $\mathbf{A}$ *we have* $\mathbf{F}(\bigcup \mathbf{A}) = \bigcup \{\mathbf{F}(X) \mid X \in \mathbf{A}\}$.

PROOF:

$$\begin{aligned} y \in \mathbf{F}(\bigcup \mathbf{A}) &\Leftrightarrow \exists x \in \bigcup \mathbf{A}.(x, y) \in \mathbf{F} \\ &\Leftrightarrow \exists x.\exists X.X \in \mathbf{A} \wedge x \in X \wedge (x, y) \in \mathbf{F} \\ &\Leftrightarrow \exists X \in \mathbf{F}.y \in \mathbf{F}(X) \end{aligned}$$

□

Proposition 2.2.17. *For any classes* $\mathbf{F}$*,* $\mathbf{A}$ *and* $\mathbf{B}$*, we have* $\mathbf{F}(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$*. Equality holds if* $\mathbf{F}$ *is single-rooted.*

PROOF:
⟨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 $(x, y) \in \mathbf{F}$
  ⟨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 $\mathbf{F}$ is single-rooted then $\mathbf{F}(\mathbf{A} \cap \mathbf{B}) = \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$.
  ⟨2⟩1. ASSUME: $\mathbf{F}$ is single-rooted.
  ⟨2⟩2. LET: $y \in \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$
  ⟨2⟩3. PICK $x \in \mathbf{A}$ such that $(x, y) \in \mathbf{F}$
  ⟨2⟩4. PICK $x' \in \mathbf{B}$ such that $(x', y) \in \mathbf{F}$
  ⟨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 2.2.18. *For any classes* $\mathbf{F}$ *and* $\mathbf{A}$ *we have*

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

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

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

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

Proposition 2.2.19. *For any classes* $\mathbf{F}$, $\mathbf{A}$ *and* $\mathbf{B}$, *we have*

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

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

PROOF:
⟨1⟩1. $\mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B}) \subseteq \mathbf{F}(\mathbf{A} - \mathbf{B})$
⟨2⟩1. LET: $y \in \mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B})$
⟨2⟩2. PICK $x \in \mathbf{A}$ such that $(x, y) \in \mathbf{F}$
⟨2⟩3. $x \notin \mathbf{B}$
⟨2⟩4. $x \in \mathbf{A} - \mathbf{B}$
⟨2⟩5. $y \in \mathbf{F}(\mathbf{A} - \mathbf{B})$
⟨1⟩2. If $\mathbf{F}$ is single-rooted then $\mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B}) = \mathbf{F}(\mathbf{A} - \mathbf{B})$
⟨2⟩1. ASSUME: $\mathbf{F}$ is single-rooted.
⟨2⟩2. LET: $y \in \mathbf{F}(\mathbf{A} - \mathbf{B})$
⟨2⟩3. PICK $x \in \mathbf{A} - \mathbf{B}$ such that $(x, y) \in \mathbf{F}$
⟨2⟩4. $y \in \mathbf{F}(\mathbf{A})$
⟨2⟩5. $y \notin \mathbf{F}(\mathbf{B})$
⟨3⟩1. ASSUME: for a contradiction $y \in \mathbf{F}(\mathbf{B})$
⟨3⟩2. PICK $x' \in \mathbf{B}$ such that $(x', y) \in \mathbf{F}$
⟨3⟩3. $x = x'$
PROOF: ⟨2⟩1
⟨3⟩4. $x \in \mathbf{B}$
⟨3⟩5. Q.E.D.
PROOF: This contradicts ⟨2⟩3.

□

Definition 2.2.20 (Reflexive)**.** Let $\mathbf{R}$ be a binary relation on $\mathbf{A}$. Then $\mathbf{R}$ is *reflexive* on $\mathbf{A}$ iff $\forall x \in \mathbf{A}.(x, x) \in \mathbf{R}$.

Definition 2.2.21 (Irreflexive)**.** A relation $\mathbf{R}$ is *irreflexive* iff there is no x such that $(x, x) \in \mathbf{R}$.

Definition 2.2.22 (Symmetric)**.** A relation $\mathbf{R}$ is *symmetric* iff, whenever $(x, y) \in \mathbf{R}$, then $(y, x) \in \mathbf{R}$.

Definition 2.2.23 (Transitive)**.** A relation $\mathbf{R}$ is *transitive* iff, whenever $(x, y), (y, z) \in \mathbf{R}$, then $(x, z) \in \mathbf{R}$.

Proposition 2.2.24. *If $\mathbf{R}$ is transitive then $\mathbf{R}^{-1}$ is transitive.*

Proof:
⟨1⟩1. Assume: $(x, y), (y, z) \in \mathbf{R}^{-1}$
⟨1⟩2. $(y, x), (z, y) \in \mathbf{R}$
⟨1⟩3. $(z, x) \in \mathbf{R}$
⟨1⟩4. $(x, z) \in \mathbf{R}^{-1}$
□

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* $\mathbf{A}$ is a class of ordered n-tuples all of whose components are in $\mathbf{A}$.

2.4 Equivalence Relations

Definition 2.4.1 (Equivalence Relation)**.** An *equivalence relation* on a class $\mathbf{A}$ is a relation on $\mathbf{A}$ that is reflexive on $\mathbf{A}$, symmetric and transitive.

Proposition 2.4.2. *If $\mathbf{R}$ is a symmetric and transitive relation, then $\mathbf{R}$ is an equivalence relation on* $\operatorname{fld} \mathbf{R}$*.*

Proof:
⟨1⟩1. Let: $x \in \operatorname{fld} \mathbf{R}$
Prove: $(x, x) \in \mathbf{R}$
⟨1⟩2. Pick y such that either $(x, y) \in \mathbf{R}$ or $(y, x) \in \mathbf{R}$
⟨1⟩3. $(x, y) \in \mathbf{R}$ and $(y, x) \in \mathbf{R}$
Proof: Symmetry.

⟨1⟩4. $(x, x) \in \mathbf{R}$
  PROOF: Transitivity.
□

Definition 2.4.3 (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

$$[a]_{\mathbf{R}} := \{x \mid (a, x) \in \mathbf{R}\} \ .$$

Proposition 2.4.4. *Let* $\mathbf{R}$ *be an equivalence relation on* $\mathbf{A}$ *and* $a, b \in \mathbf{A}$*. Then* $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$ *if and only if* $(a, b) \in \mathbf{R}$*.*

PROOF:
⟨1⟩1. If $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$ then $(a, b) \in \mathbf{R}$.
  ⟨2⟩1. ASSUME: $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$
  ⟨2⟩2. $(b, b) \in \mathbf{R}$
    PROOF: Reflexivity
  ⟨2⟩3. $b \in [b]_{\mathbf{R}}$
  ⟨2⟩4. $b \in [a]_{\mathbf{R}}$
  ⟨2⟩5. $(a, b) \in \mathbf{R}$
⟨1⟩2. If $(a, b) \in \mathbf{R}$ then $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$.
  ⟨2⟩1. For all $x, y \in \mathbf{A}$, if $(x, y) \in \mathbf{R}$ then $[y]_{\mathbf{R}} \subseteq [x]_{\mathbf{R}}$
    ⟨3⟩1. LET: $x, y \in \mathbf{A}$
    ⟨3⟩2. ASSUME: $(x, y) \in \mathbf{R}$
    ⟨3⟩3. LET: $t \in [y]_{\mathbf{R}}$
    ⟨3⟩4. $(y, t) \in \mathbf{R}$
      PROOF: ⟨3⟩3
    ⟨3⟩5. $(x, t) \in \mathbf{R}$
      PROOF: Transitivity, ⟨3⟩2, ⟨3⟩4.
    ⟨3⟩6. $t \in [x]_{\mathbf{R}}$
      PROOF: ⟨3⟩5
  ⟨2⟩2. ASSUME: $(a, b) \in \mathbf{R}$
  ⟨2⟩3. $[b]_{\mathbf{R}} \subseteq [a]_{\mathbf{R}}$
    PROOF: ⟨2⟩1, ⟨2⟩2.
  ⟨2⟩4. $(b, a) \in \mathbf{R}$
    PROOF: Symmetry, ⟨2⟩2.
  ⟨2⟩5. $[a]_{\mathbf{R}} \subseteq [b]_{\mathbf{R}}$
    PROOF: ⟨2⟩1, ⟨2⟩4.
  ⟨2⟩6. $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$
    PROOF: ⟨2⟩3, ⟨2⟩5.
□

Definition 2.4.5 (Partition)**.** A *partition* Π 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 Π have any common elements, and
2. each element of A is in some set in Π.

Definition 2.4.6. Let R be an equivalence relation on a set A. The *quotient set* A/R is the set of all equivalence classes.

Proposition 2.4.7. *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. $(a, c) \in R$
    PROOF: $\langle 2 \rangle$2
  $\langle 2 \rangle$4. $(b, c) \in R$
    PROOF: $\langle 2 \rangle$2
  $\langle 2 \rangle$5. $(c, b) \in R$
    PROOF: Symmetry, $\langle 2 \rangle$4
  $\langle 2 \rangle$6. $(a, b) \in R$
    PROOF: Transitivity, $\langle 2 \rangle$3, $\langle 2 \rangle$5
  $\langle 2 \rangle$7. $[a]_R = [b]_R$
    PROOF: Proposition 2.4.4, $\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.
□

2.5 Ordering Relations

2.5.1 Structures

Definition 2.5.1 (Structure)**.** A *structure* is a pair (A, R) where A is a set and R is a binary relation on A.

2.5.2 Partial Orders

Definition 2.5.2 (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 $x \leq y \wedge x \neq y$.

Definition 2.5.3 (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 $(A, \leq)$.

Proposition 2.5.4. *If $\mathbf{R}$ is a partial order on $\mathbf{A}$ then so is $\mathbf{R}^{-1}$.*

PROOF: Easy. □

Proposition 2.5.5. *Let* $\mathbf{R}$ *be a partial order on* $\mathbf{A}$ *and* $\mathbf{B} \subseteq \mathbf{A}$*. Then* $\mathbf{R} \cap \mathbf{B}^2$ *is a partial order on* $\mathbf{B}$*.*

PROOF: Easy. □

Definition 2.5.6 (Minimal)**.** Let A be a poset. An element $m \in A$ is *minimal* iff there is no $x \in A$ such that $x < m$.

Definition 2.5.7 (Maximal)**.** Let A be a poset. An element $m \in A$ is *maximal* iff there is no $x \in A$ such that $m < x$.

Definition 2.5.8 (Least)**.** Let A be a poset. An element $m \in A$ is *least* iff for all $x \in A$ we have $m \leq x$.

Proposition 2.5.9. *A poset 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 2.5.10 (Greatst)**.** Let A be a poset. An element $m \in A$ is *greatest* iff for all $x \in A$ we have $x \leq m$.

Proposition 2.5.11. *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 2.5.12 (Upper Bound)**.** Let $\mathbf{R}$ be a partial ordering on $\mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{A}$. Let $u \in \mathbf{A}$. Then u is an *upper bound* for $\mathbf{B}$ iff $\forall x \in \mathbf{B}. x \leq u$.

Definition 2.5.13 (Lower Bound)**.** Let $\mathbf{R}$ be a partial ordering on $\mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{A}$. Let $l \in \mathbf{A}$. Then l is a *lower bound* for $\mathbf{B}$ iff $\forall x \in \mathbf{B}. l \leq x$.

Definition 2.5.14 (Bounded Above)**.** Let $\mathbf{R}$ be a partial ordering on $\mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{A}$. Then $\mathbf{B}$ is *bounded above* iff it has an upper bound.

Definition 2.5.15 (Bounded Below)**.** Let $\mathbf{R}$ be a partial ordering on $\mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{A}$. Then $\mathbf{B}$ is *bounded below* iff it has a lower bound.

Definition 2.5.16 (Least Upper Bound)**.** Let $\mathbf{R}$ be a partial ordering on $\mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{A}$. Let $s \in \mathbf{A}$. Then s is the *least upper bound* or *supremum* of $\mathbf{B}$ iff s is an upper bound for $\mathbf{B}$ and, for every upper bound u for $\mathbf{B}$, we have $s \leq u$.

Definition 2.5.17 (Greatest Lower Bound)**.** Let $\mathbf{R}$ be a partial ordering on $\mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{A}$. Let $i \in \mathbf{A}$. Then i is the *greatest lower bound* or *infimum* of $\mathbf{B}$ iff i is a lower bound for $\mathbf{B}$ and, for every lower bound l for $\mathbf{B}$, we have $i \leq l$.

Definition 2.5.18 (Complete)**.** A poset is *complete* iff every nonempty subset bounded above has a supremum, and every nonempty subset bounded below has an infimum.

Definition 2.5.19 (Dense)**.** Let A be a poset 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 2.5.20. *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.
$\langle 1 \rangle 4$. $\sup S(a) \leq a$
$\langle 1 \rangle 5$. $\sup S(a) = a$
$\langle 2 \rangle 1$. 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 $b \leq \theta(a)$
$\langle 2 \rangle 1$. LET: $b \in S(a)$
$\langle 2 \rangle 2$. $b < a$
$\langle 2 \rangle 3$. $\theta(b) \leq \theta(a)$
$\langle 2 \rangle 4$. $b \leq \theta(a)$
PROOF: $\theta(b) = b$
$\langle 1 \rangle 7$. $a \leq \theta(a)$
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 $a < b < \theta(a)$
$\langle 2 \rangle 3$. $\theta(a) \leq \theta(b) = b$
$\langle 2 \rangle 4$. Q.E.D.
PROOF: This contradicts the fact that $b < \theta(a)$.
$\langle 1 \rangle 9$. $\theta(a) = a$
□

Theorem 2.5.21. *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 $B \cong Q$ 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.
⟨3⟩2. PICK $b \in B$ such that $a_1 < b < a$.
⟨3⟩3. $\phi(b) \in \phi(S(a))$
⟨2⟩2. $\phi(S(a))$ is bounded above.
⟨3⟩1. PICK $a_2 > a$
PROOF: Since a is not greatest.
⟨3⟩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 ϕ.
⟨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 ψ
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 2.5.20.
⟨1⟩10. $\overline{\phi} \circ \overline{\psi} = \mathrm{id}_B$
PROOF: Proposition 2.5.20.
⟨1⟩11. If $\phi^* : A \cong P$ is any order isomorphism that extends ϕ 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.
□

Theorem 2.5.22 (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: $b \in B$
$\langle 2 \rangle 2.$ $b \leq \phi(b)$
$\langle 2 \rangle 3.$ $b \leq a$
$\langle 2 \rangle 4.$ $\phi(b) \leq \phi(a)$
$\langle 2 \rangle 5.$ $b \leq \phi(a)$
$\langle 1 \rangle 4.$ $a \leq \phi(a)$
$\langle 1 \rangle 5.$ $\phi(a) \leq \phi(\phi(a))$
$\langle 1 \rangle 6.$ $\phi(a) \in B$
$\langle 1 \rangle 7.$ $\phi(a) \leq a$
$\langle 1 \rangle 8.$ $\phi(a) = a$
□

Definition 2.5.23 (Initial Segment)**.** Let A be a poset and $t \in A$. The *initial segment* up to t is
$$\operatorname{seg} t := \{x \in A \mid x < t\} \enspace .$$

2.5.3 Linear Orders

Definition 2.5.24 (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 2.5.25 (Trichotomy)**.** *Let $\leq$ 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 2.5.26. *Let $<$ be an irreflexive 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: Easy. □

Proposition 2.5.27. *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 transitive.
  PROOF: Proposition 2.2.24.
$\langle 1\rangle 2$. $\mathbf{R}^{-1}$ satisfies trichotomy.
  $\langle 2\rangle 1$. LET: $x, y \in \mathbf{A}$
  $\langle 2\rangle 2$. Exactly one of $(x, y) \in \mathbf{R}$, $(y, x) \in \mathbf{R}$, $x = y$ holds.
  $\langle 2\rangle 3$. Exactly one of $(y, x) \in \mathbf{R}^{-1}$, $(x, y) \in \mathbf{R}^{-1}$, $x = y$ holds.
□

Proposition 2.5.28. *Let* $\mathbf{R}$ *be a linear order on* $\mathbf{A}$ *and* $\mathbf{B} \subseteq \mathbf{A}$. *Then* $\mathbf{R} \cap \mathbf{B}^2$ *is a linear order on* $\mathbf{B}$.

PROOF: Easy. □

Definition 2.5.29 (Lexicographic Ordering)**.** Let A and B be linearly ordered sets. The *lexicographic ordering* $<$ on $A \times B$ is defined by:

$$(a, b) < (a', b') \Leftrightarrow a < a' \vee (a = a' \wedge b < b') \ .$$

Proposition 2.5.30. *Let* A *and* B *be linearly ordered sets. Then the lexicographic ordering on* $A \times B$ *is a linear ordering.*

PROOF:
$\langle 1\rangle 1$. $<$ is transitive.
  $\langle 2\rangle 1$. LET: $(a_1, b_1) < (a_2, b_2) < (a_3, b_3)$
      PROVE: $(a_1, b_1) < (a_3, b_3)$
  $\langle 2\rangle 2$. CASE: $a_1 < a_2$
    $\langle 3\rangle 1$. $a_2 < a_3$ or $a_2 = a_3$
      PROOF: $\langle 2\rangle 1$
    $\langle 3\rangle 2$. $a_1 < a_3$
      PROOF: Transitivity
    $\langle 3\rangle 3$. $(a_1, b_1) < (a_3, b_3)$
  $\langle 2\rangle 3$. CASE: $a_1 = a_2$ and $b_1 < b_2$ and $a_2 < a_3$
    PROOF: We have $a_1 < a_3$ so $(a_1, b_1) < (a_3, b_3)$.
  $\langle 2\rangle 4$. CASE: $a_1 = a_2$ and $b_1 < b_2$ and $a_2 = a_3$ and $b_2 < b_3$
    PROOF: We have $a_1 = a_3$ and $b_1 < b_3$ so $(a_1, b_1) < (a_3, b_3)$.
$\langle 1\rangle 2$. $<$ satisfies trichotomy.
  $\langle 2\rangle 1$. LET: $(a_1, b_1), (a_2, b_2) \in A \times B$
  $\langle 2\rangle 2$. Exactly one of $a_1 < a_2$, $a_1 = a_2$, $a_2 < a_1$ holds.
  $\langle 2\rangle 3$. CASE: $a_1 < a_2$
    PROOF: We have $(a_1, b_1) < (a_2, b_2)$, $(a_1, b_1) \neq (a_2, b_2)$, and $(a_2, b_2) \not< (a_1, b_1)$.
  $\langle 2\rangle 4$. CASE: $a_1 = a_2$
    $\langle 3\rangle 1$. Exactly one of $b_1 < b_2$, $b_1 = b_2$, $b_2 < b_1$ holds.
    $\langle 3\rangle 2$. Exactly one of $(a_1, b_1) < (a_2, b_2)$, $(a_1, b_1) = (a_2, b_2)$, $(a_2, b_2) < (a_1, b_1)$ holds.

⟨2⟩5. CASE: $a_2 < a_1$
PROOF: We have $(a_2, b_2) < (a_1, b_1)$, $(a_2, b_2) \neq (a_1, b_1)$, and $(a_1, b_1) \not< (a_2, b_2)$.

2.5.4 Well Orderings

Definition 2.5.31 (Well Ordering)**.** A *well ordering* on a set A is a linear ordering on A such that every nonempty subset has a least element.

Proposition 2.5.32. *Let* $\mathbf{R}$ *be a well ordering on* $\mathbf{A}$ *and* $\mathbf{B} \subseteq \mathbf{A}$. *Then* $\mathbf{R} \cap \mathbf{B}^2$ *is a well ordering on* $\mathbf{B}$.

PROOF: Easy. □

Theorem 2.5.33 (Transfinite Induction Principle)**.** *Let $<$ be a well ordering on A. Let $B \subseteq A$. Assume that, for all $t \in A$,*

$$\operatorname{seg} t \subseteq B \Rightarrow t \in B \ .$$

Then $B = A$.

PROOF:
⟨1⟩1. ASSUME: for a contradiction $B \neq A$
⟨1⟩2. LET: m be the least element of $A - B$
⟨1⟩3. $\operatorname{seg} m \subseteq B$
PROOF: By leastness of m.
⟨1⟩4. $m \in B$
⟨1⟩5. Q.E.D.
PROOF: This is a contradiction.
□

Theorem 2.5.34. *Let $<$ 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 $<$ 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.
□

Chapter 3

Functions

3.1 Functions

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

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

Proposition 3.1.2. *For any class* $\mathbf{F}$*,* $\mathbf{F}^{-1}$ *is a function if and only if* $\mathbf{F}$ *is single-rooted.*

Proof: Immediate from definitions. $\square$

Proposition 3.1.3. *For any relation* $\mathbf{F}$*,* $\mathbf{F}$ *is a function if and only if* $\mathbf{F}^{-1}$ *is single-rooted.*

Proof: Immediate from definitions. $\square$

Proposition 3.1.4. *Let* $\mathbf{F}$ *and* $\mathbf{G}$ *be functions. Then* $\mathbf{F} \circ \mathbf{G}$ *is a function, its domain is*

$$\{x \in \operatorname{dom} \mathbf{G} \mid \mathbf{G}(x) \in \operatorname{dom} \mathbf{F}\} \enspace ,$$

and for x *in this domain,* $(\mathbf{F} \circ \mathbf{G})(x) = \mathbf{F}(\mathbf{G}(x))$*.*

Proof:
$\langle 1 \rangle 1.$ $\mathbf{F} \circ \mathbf{G}$ is a function.
  $\langle 2 \rangle 1.$ Let: $(x, z), (x, z') \in \mathbf{F} \circ \mathbf{G}$
  $\langle 2 \rangle 2.$ Pick y, y' such that $(x, y) \in \mathbf{G}$, $(y, z) \in \mathbf{F}$, $(x, y') \in \mathbf{G}$, $(y', z') \in \mathbf{F}$
  $\langle 2 \rangle 3.$ $y = y'$
    Proof: $\mathbf{G}$ is a function.
  $\langle 2 \rangle 4.$ $z = z'$
    Proof: $\mathbf{F}$ is a function.
$\langle 1 \rangle 2.$ $\operatorname{dom}(\mathbf{F} \circ \mathbf{G}) = \{x \in \operatorname{dom} \mathbf{G} \mid \mathbf{G}(x) \in \operatorname{dom} \mathbf{F}\}$

PROOF:

$$\begin{aligned} x \in \mathrm{dom}(\mathbf{F} \circ \mathbf{G}) &\Leftrightarrow \exists z.(x, z) \in \mathbf{F} \circ \mathbf{G} \\ &\Leftrightarrow \exists y, z((x, y) \in \mathbf{G} \wedge (y, z) \in \mathbf{F}) \\ &\Leftrightarrow \exists y((x, y) \in \mathbf{G} \wedge y \in \mathrm{dom}\,\mathbf{F}) \\ &\Leftrightarrow x \in \mathrm{dom}\,\mathbf{G} \wedge \mathbf{G}(y) \in \mathrm{dom}\,\mathbf{F} \end{aligned}$$

⟨1⟩3. $\forall x \in \mathrm{dom}(\mathbf{F} \circ \mathbf{G}).(\mathbf{F} \circ \mathbf{G})(x) = \mathbf{F}(\mathbf{G}(x))$
PROOF:
⟨2⟩1. LET: $x \in \mathrm{dom}(\mathbf{F} \circ \mathbf{G})$
⟨2⟩2. $(x, (\mathbf{F} \circ \mathbf{G})(x)) \in \mathbf{F} \circ \mathbf{G}$
⟨2⟩3. PICK y such that $(x, y) \in \mathbf{G}$ and $(y, (\mathbf{F} \circ \mathbf{G})(x)) \in \mathbf{F}$
⟨2⟩4. $y = \mathbf{G}(x)$
⟨2⟩5. $\mathbf{F}(\mathbf{G}(x)) = (\mathbf{F} \circ \mathbf{G})(x)$
□

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. $\mathrm{dom}\,F = \mathcal{P}A - \{\emptyset\}$
PROOF:

$$\begin{aligned} B \in \mathrm{dom}\,F &\Leftrightarrow \exists b.(B, b) \in F \\ &\Leftrightarrow \exists b.((B, b) \in \bigcup \mathcal{A} \wedge (B, b) \in C) \\ &\Leftrightarrow \exists b. \exists B' \in \mathcal{P}A - \{\emptyset\}.((B, b) \in \{B'\} \times B' \wedge (B, b) \in C) \\ &\Leftrightarrow B \in \mathcal{P}A - \{\emptyset\} \wedge \exists b \in B.(B, b) \in C \\ &\Leftrightarrow B \in \mathcal{P}A - \{\emptyset\} && (\langle 1 \rangle 5) \end{aligned}$$

⟨2⟩3. $\mathrm{ran}\,F \subseteq A$
⟨1⟩8. For every nonempty $B \subseteq A$ we have $F(B) \in B$
□

Proposition 3.1.6. *For any relation R there exists a function $H \subseteq R$ with* $\operatorname{dom} H = \operatorname{dom} R$*.*

Proof:
$\langle 1 \rangle 1$. Let: R be a relation.
$\langle 1 \rangle 2$. Pick a choice function G for $\operatorname{ran} R$.
$\langle 1 \rangle 3$. Define $H : domR \to \operatorname{ran} R$ by $H(x) = G(\{y \mid xRy\})$
$\langle 1 \rangle 4$. $H \subseteq R$
□

Proposition 3.1.7. *For any function* $\mathbf{G}$ *and nonempty class* $\mathbf{A}$*, we have*

$$\mathbf{G}^{-1}\left(\bigcap \mathbf{A}\right) = \bigcap \{\mathbf{G}^{-1}(X) \mid X \in \mathbf{A}\} \enspace .$$

Proof: Propositions 2.2.18 and 3.1.3. □

Proposition 3.1.8. *For any function* $\mathbf{G}$ *and classes* $\mathbf{A}$ *and* $\mathbf{B}$*, we have*

$$\mathbf{G}^{-1}(\mathbf{A} - \mathbf{B}) = \mathbf{G}^{-1}(\mathbf{A}) - \mathbf{G}^{-1}(\mathbf{B}) \enspace .$$

Proof: Proposition 2.2.19 and 3.1.3. □

Definition 3.1.9 (Identity Function)**.** For any class $\mathbf{A}$, the *identity function* on $\mathbf{A}$ is $\mathbf{I_A} = \{(x, x) \mid x \in \mathbf{A}\}$.

Definition 3.1.10 (Injective)**.** A function is *one-to-one*, *injective* or an *injection* iff it is single-rooted.

Proposition 3.1.11. *Let* $\mathbf{F}$ *be a one-to-one function. Let* $x \in \operatorname{dom} \mathbf{F}$*. Then* $\mathbf{F}^{-1}(\mathbf{F}(x)) = x$*.*

Proof:
$\langle 1 \rangle 1$. $\mathbf{F}^{-1}$ is a function.
Proof: Proposition 3.1.2.
$\langle 1 \rangle 2$. $(x, \mathbf{F}(x)) \in \mathbf{F}$
$\langle 1 \rangle 3$. $(\mathbf{F}(x), x) \in \mathbf{F}^{-1}$
□

Proposition 3.1.12. *Let* $\mathbf{F}$ *be a one-to-one function. Let* $y \in \operatorname{ran} \mathbf{F}$*. Then* $\mathbf{F}(\mathbf{F}^{-1}(y)) = y$*.*

Proof:
$\langle 1 \rangle 1$. $\mathbf{F}^{-1}$ is a function.
Proof: Proposition 3.1.2.
$\langle 1 \rangle 2$. $y \in \operatorname{dom} \mathbf{F}^{-1}$
Proof: Proposition 2.2.8.
$\langle 1 \rangle 3$. $(y, \mathbf{F}^{-1}(y)) \in \mathbf{F}^{-1}$
$\langle 1 \rangle 4$. $(\mathbf{F}^{-1}(y), y) \in \mathbf{F}$
□

Proposition 3.1.13. *Let $F : A \to B$ where A is nonempty. There exists $G : B \to A$ (a* left inverse*) such that $G \circ F = I_A$ if and only if F is one-to-one.*

PROOF:
⟨1⟩1. If there exists $G : B \to A$ such that $G \circ F = I_A$ then F is one-to-one.
  ⟨2⟩1. ASSUME: $G : B \to A$ 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 $G : B \to A$ such that $G \circ F = I_A$.
  ⟨2⟩1. ASSUME: F is one-to-one.
  ⟨2⟩2. PICK $a \in A$
  ⟨2⟩3. LET: $G : B \to A$ be the function defined by: $G(b) = F^{-1}(b)$ if $b \in \operatorname{ran} F$, $G(b) = a$ otherwise.
    PROVE: $G \circ F = I_A$
  ⟨2⟩4. LET: $x \in A$
  ⟨2⟩5. $G(F(x)) = x$
□

Definition 3.1.14 (Surjective)**.** Let $F : A \to B$. 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 3.1.15. *Let $F : A \to B$. There exists $H : B \to A$ (a* right inverse*) such that $F \circ H = I_B$ 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 such that $H \subseteq F^{-1}$ and $\operatorname{dom} H = \operatorname{dom} F^{-1} = B$
  ⟨2⟩3. $H : B \to A$
  ⟨2⟩4. $F \circ H = I_B$
    ⟨3⟩1. LET: $y \in B$
    ⟨3⟩2. $(y, H(y)) \in F^{-1}$
    ⟨3⟩3. $F(H(y)) = y$
□

Definition 3.1.16 (Function Set)**.** Given a set A and a class $\mathbf{B}$, we write $\mathbf{B}^A$ for the class of all functions $A \to \mathbf{B}$.

Proposition 3.1.17. *If A and B are sets then A^B is a set.*

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

Definition 3.1.18 (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 $[a]_R$.

Definition 3.1.19 (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 $\mathbf{F}(x) = \mathbf{F}(y)$.

Theorem 3.1.20. *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:
⟨1⟩1. If F respects R then there exists $\hat{F} : A/R \to \mathbf{B}$ such that $\forall a \in A.\hat{F}([a]_R) = F(a)$.
  ⟨2⟩1. ASSUME: F respects R.
  ⟨2⟩2. LET: $\hat{F} = \{([a]_R, F(a)) \mid a \in A\}$
  ⟨2⟩3. $\hat{F}$ is a function.
    ⟨3⟩1. ASSUME: $a, a' \in A$ and $[a]_R = [a']_R$
      PROVE: $F(a) = F(a')$
    ⟨3⟩2. $(a, a') \in R$
      PROOF: Proposition 2.4.4.
    ⟨3⟩3. $F(a) = F(a')$
      PROOF: ⟨2⟩1
  ⟨2⟩4. $\operatorname{dom} \hat{F} = A/R$
  ⟨2⟩5. $\operatorname{ran} \hat{F} \subseteq \mathbf{B}$
  ⟨2⟩6. $\forall a \in A.\hat{F}([a]_R) = F(a)$
⟨1⟩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.
  ⟨2⟩1. ASSUME: $\hat{F} : A/R \to \mathbf{B}$ and $\forall a \in A.\hat{F}([a]_R) = F(a)$
  ⟨2⟩2. LET: $a, a' \in A$
  ⟨2⟩3. ASSUME: $(a, a') \in R$
  ⟨2⟩4. $[a]_R = [a']_R$
    PROOF: Proposition 2.4.4.
  ⟨2⟩5. $F(a) = F(a')$
    PROOF: ⟨2⟩1
⟨1⟩3. If $G, H : A/R \to \mathbf{B}$ and $\forall a \in A.G([a]_R) = H([a]_R)$ then $G = H$.
□

Definition 3.1.21 (Strictly Monotone)**.** Let $(A, <_A)$ and $(B, <_B)$ be linearly ordered sets. A function $f : A \to B$ is *strictly monotone* iff, whenever $x <_A y$, then $f(x) <_B f(y)$.

Proposition 3.1.22. *A strictly monotone function is injective.*

PROOF:
⟨1⟩1. LET: $(A, <_A)$ and $(B, <_B)$ be linearly ordered sets.

$\langle 1\rangle 2.$ LET: $f : A \to B$ be strictly monotone.
$\langle 1\rangle 3.$ LET: $x, y \in A$
$\langle 1\rangle 4.$ ASSUME: $f(x) = f(y)$
$\langle 1\rangle 5.$ $f(x) \not< f(y)$ and $f(y) \not< f(x)$
PROOF: Trichotomy.
$\langle 1\rangle 6.$ $x \not< y$ and $y \not< x$
$\langle 1\rangle 7.$ $x = y$
PROOF: Trichotomy.
$\square$

Proposition 3.1.23. *Let A and B be linearly ordered sets. Let $f : A \to B$. Let $x, y \in A$. If f is strictly monotone and $f(x) < f(y)$ then $x < y$.*

PROOF:
$\langle 1\rangle 1.$ $f(x) \neq f(y)$ and $f(y) \not< f(x)$
PROOF: Trichotomy.
$\langle 1\rangle 2.$ $x \neq y$ and $y \not< x$
$\langle 1\rangle 3.$ $x < y$
PROOF: Trichotomy.
$\square$

Definition 3.1.24 (Closed)**.** Let $\mathbf{F}$ be a function and $\mathbf{A} \subseteq \operatorname{dom} \mathbf{F}$. Then $\mathbf{A}$ is *closed* under $\mathbf{F}$ iff $\forall x \in \mathbf{A}.\mathbf{F}(x) \in \mathbf{A}$.

Definition 3.1.25 (Binary Operation)**.** A *binary operation* on a set A is a function from $A \times A$ into A.

3.2 Dependent Product Sets

Definition 3.2.1. 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 with $\operatorname{dom} f = I$ and $\forall i \in I.f(i) \in \mathbf{H}(i)$.

Proposition 3.2.2. *If I is a set and $H(i)$ is a set for all $i \in I$, then $\prod_{i \in I} H(i)$ is a set.*

PROOF:
$\langle 1\rangle 1.$ $\{H(i) \mid i \in I\}$ is a set.
PROOF: Axiom of Replacement.
$\langle 1\rangle 2.$ $\prod_{i \in I} H(i) \subseteq \bigcup \{H(i) \mid i \in I\}^I$
$\square$

Proposition 3.2.3. *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 $f \subseteq R$ such that $\operatorname{dom} f = \operatorname{dom} R$
$\langle 1\rangle 4.$ $f \in \prod_{i \in I} H(i)$
$\square$

3.3 Equinumerosity

Definition 3.3.1 (Equinumerous)**.** Sets A and B are *equinumerous*, $A \approx B$, iff there exists a bijection between A and B.

Proposition 3.3.2. *Equinumerosity is an equivalence relation on the class of all sets.*

PROOF:
$\langle 1 \rangle 1$. For any set A we have $A \approx A$.
PROOF: We have id_A is a bijection between A and A.
$\langle 1 \rangle 2$. If $A \approx B$ then $B \approx A$.
PROOF: If $f : A \approx B$ then $f^{-1} : B \approx A$.
$\langle 1 \rangle 3$. If $A \approx B$ and $B \approx C$ then $A \approx C$.
PROOF: If $f : A \approx B$ and $g : B \approx C$ then $g \circ f : A \approx C$.
□

Proposition 3.3.3. *Let* $2 = \{\emptyset, \{\emptyset\}\}$*. 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. □

Theorem 3.3.4 (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.
□

Definition 3.3.5 (Dominate)**.** A set A is *dominated* by a set B, $A \preccurlyeq B$, iff there exists an injection $A \to B$.

3.4 Transfinite Recursion

Theorem Schema 3.4.1 (Transfinite Recursion Theorem Schema)**.** *For any property* $G(x, y)$*, the following is a theorem:*

Assume that $<$ *is a well ordering on a set* A*. Assume that, for any* f*, there exists a unique* y *such that* $G(f, y)$*. Then there exists a unique function* F *such that* $\mathrm{dom}\, F = A$ *and*

$$\forall t \in A. G(F \restriction \mathrm{seg}\, t, F(t)) \enspace .$$

PROOF:
$\langle 1 \rangle 1$. For $t \in A$, let us say that a function v is *G-constructed up to t* iff $\mathrm{dom}\, v = \{x \in A \mid x \leq t\}$ and

$$\forall x \in \mathrm{dom}\, v. G(v \restriction \mathrm{seg}\, x, v(x)) \enspace .$$

$\langle 1 \rangle 2$. For all $t_1, t_2 \in A$ with $t_1 \leq t_2$, if v_1 is G-constructed up to t_1 and v_2 is G-constructed up to t_2, then $\forall x \leq t_1 . v_1(x) = v_2(x)$.
- $\langle 2 \rangle 1$. Let: $x \in A$
- $\langle 2 \rangle 2$. Assume: $\forall y < x . (y \leq t_1 \Rightarrow v_1(y) = v_2(y))$
- $\langle 2 \rangle 3$. Assume: $x \leq t_1$
- $\langle 2 \rangle 4$. $G(v_1 \upharpoonright \operatorname{seg} x, v_1(x))$
- $\langle 2 \rangle 5$. $G(v_2 \upharpoonright \operatorname{seg} x, v_2(x))$
- $\langle 2 \rangle 6$. $v_1 \upharpoonright \operatorname{seg} x = v_2 \upharpoonright \operatorname{seg} x$
- $\langle 2 \rangle 7$. $v_1(x) = v_2(x)$
- $\langle 2 \rangle 8$. Q.E.D.

  Proof: By transfinite induction.

$\langle 1 \rangle 3$. Let $\mathcal{K}$ be the set of all functions v such that there exists $t \in A$ such that v is G-constructed up to t.

Proof: By an Axiom of Replacement using $\langle 1 \rangle 2$.

$\langle 1 \rangle 4$. Let: $F = \bigcup \mathcal{K}$

$\langle 1 \rangle 5$. F is a function.
- $\langle 2 \rangle 1$. Let: $(x, y_1), (x, y_2) \in F$
- $\langle 2 \rangle 2$. Pick $v_1, v_2 \in \mathcal{K}$ such that $v_1(x) = y_1$ and $v_2(x) = y_2$.
- $\langle 2 \rangle 3$. Pick $t_1, t_2 \in A$ such that v_1 is G-constructed up to t_1 and v_2 is G-constructed up to t_2.
- $\langle 2 \rangle 4$. Assume: w.l.o.g. $t_1 \leq t_2$
- $\langle 2 \rangle 5$. $v_1(x) = v_2(x)$

  Proof: $\langle 1 \rangle 2$.
- $\langle 2 \rangle 6$. $y_1 = y_2$

$\langle 1 \rangle 6$. $\forall x \in \operatorname{dom} F . G(F \upharpoonright \operatorname{seg} x, F(x))$
- $\langle 2 \rangle 1$. Let: $x \in \operatorname{dom} F$
- $\langle 2 \rangle 2$. Pick $v \in \mathcal{K}$ such that $v(x) = F(x)$
- $\langle 2 \rangle 3$. Pick t such that v is G-constructed up to t.
- $\langle 2 \rangle 4$. $G(v \upharpoonright \operatorname{seg} x, v(x))$
- $\langle 2 \rangle 5$. $v \upharpoonright \operatorname{seg} x = F \upharpoonright \operatorname{seg} x$
  - $\langle 3 \rangle 1$. Let: $y < x$

    Prove: $v(y) = F(y)$
  - $\langle 3 \rangle 2$. $y \in \operatorname{dom} F$

    Proof: Since $y \in \operatorname{dom} v$ and $v \in \mathcal{K}$.
  - $\langle 3 \rangle 3$. Pick $u \in \mathcal{K}$ such that $u(y) = F(y)$
  - $\langle 3 \rangle 4$. $u(y) = v(y)$

    Proof: $\langle 1 \rangle 2$.
  - $\langle 3 \rangle 5$. $v(y) = F(y)$
- $\langle 2 \rangle 6$. $G(F \upharpoonright \operatorname{seg} x, F(x))$

$\langle 1 \rangle 7$. $\operatorname{dom} F = A$
- $\langle 2 \rangle 1$. Assume: $\operatorname{dom} F \neq A$
- $\langle 2 \rangle 2$. Let: t be least in $A - \operatorname{dom} F$
- $\langle 2 \rangle 3$. $\operatorname{seg} t = \operatorname{dom} F$
- $\langle 2 \rangle 4$. Let: y be the unique object such that $G(F, y)$
- $\langle 2 \rangle 5$. Let: $v = F \cup \{(t, y)\}$
- $\langle 2 \rangle 6$. v is G-constructed up to t.

⟨2⟩7. $t \in \operatorname{dom} F$
⟨2⟩8. Q.E.D.
PROOF: This is a contradiction.
⟨1⟩8. F is unique.
PROOF: If F' also satisfies the theorem, prove $F(x) = F'(x)$ by transfinite induction on x.
□

3.5 Structure Isomorphisms

Definition 3.5.1 (Isomorphism)**.** Let (A, R) and (B, S) be structures. An *isomorphism* between (A, R) and (B, S) is a bijection $f : A \cong B$ such that, for all $x, y \in A$, we have $(x, y) \in R$ if and only if $(f(x), f(y)) \in S$. We write $f : (A, R) \cong (B, S)$.

We say (A, R) and (B, S) are *isomorphic* iff there exists an isomorphism between them.

Theorem 3.5.2. *Isomorphism is an equivalence relation on the class of structures.*

PROOF:
⟨1⟩1. $\mathrm{id}_A : (A, R) \cong (A, R)$
⟨1⟩2. If $f : (A, R) \cong (B, S)$ then $f^{-1} : (B, S) \cong (A, R)$.
⟨1⟩3. If $f : (A, R) \cong (B, S)$ and $g : (B, S) \cong (C, T)$ then $g \circ f : (A, R) \cong (C, T)$.
□

Proposition 3.5.3. *Let B be a poset, A a set, and $f : A \to B$ an injection. Define $\leq$ on A by $x \leq y$ iff $f(x) \leq f(y)$.*

1. *$\leq$ is a partial order on A.*
2. *If B is a linearly ordered set then $\leq$ is a linear order on A.*
3. *If B is a well ordered set then $\leq$ is a well ordering on A.*

PROOF: Easy. □

Proposition 3.5.4. *There is at most one isomorphism between two well ordered sets.*

PROOF:
⟨1⟩1. LET: A and B be well ordered sets.
⟨1⟩2. LET: $f, g : A \cong B$ be isomorphisms.
⟨1⟩3. $\forall x \in A. f(x) = g(x)$
PROOF: Transfinite induction on x.
□

Theorem 3.5.5. *Let A and B be well ordered sets. Then one of the following holds: $A \cong B$; there exists $b \in B$ such that $A \cong \operatorname{seg} b$; there exists $a \in A$ such that $\operatorname{seg} a \cong B$.*

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:

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

$\langle 1 \rangle 3$. CASE: $e \in \operatorname{ran} F$
$\langle 2 \rangle 1$. LET: t be least such that $F(t) = e$
$\langle 2 \rangle 2$. $F \upharpoonright \operatorname{seg} t : \operatorname{seg} t \cong B$
$\langle 1 \rangle 4$. CASE: $\operatorname{ran} F = B$
PROOF: We have $F : A \cong B$
$\langle 1 \rangle 5$. CASE: $\operatorname{ran} F \subsetneq B$
$\langle 2 \rangle 1$. LET: b be the least element of $B - \operatorname{ran} F$
$\langle 2 \rangle 2$. $F : A \cong \operatorname{seg} b$
$\square$

Chapter 4

Ordinal Numbers

Definition 4.0.1 (Ordinal Number)**.** Let A be a well ordered set. Define the function E on A by transfinite recursion by:

$$E(t) = \{E(x) \mid x < t\} \ .$$

The *ordinal number* of A is $\alpha := \operatorname{ran} E$.

Proposition 4.0.2. *E is a bijection between A and α.*

PROOF: If $s < t$ then $E(s) \in E(t)$ so $E(s) \neq E(t)$. ☐

Proposition 4.0.3. *For all $s, t \in A$, we have $s < t$ if and only if $E(s) \in E(t)$.*

PROOF:
⟨1⟩1. If $s < t$ then $E(s) \in E(t)$.
  PROOF: By definition of $E(t)$.
⟨1⟩2. If $E(s) \in E(t)$ then $s < t$.
  ⟨2⟩1. ASSUME: $E(s) \in E(t)$
  ⟨2⟩2. PICK $s' < t$ such that $E(s) = E(s')$
  ⟨2⟩3. $s = s'$
    PROOF: Proposition 4.0.2.
  ⟨2⟩4. $s < t$
☐

Corollary 4.0.3.1. *$(A, \leq)$ is isomorphic to α ordered by $\in$.*

Corollary 4.0.3.2. *α is well ordered by $\in$.*

Corollary 4.0.3.3. *Two well-ordered sets are isomorphic if and only if they have the same ordinal number.*

Proposition 4.0.4. *α is a transitive set.*

PROOF:
⟨1⟩1. LET: $y \in z \in \alpha$

$\langle 1\rangle 2$. PICK $a \in A$ such that $z = E(a)$
$\langle 1\rangle 3$. PICK $b < a$ such that $y = E(b)$
$\langle 1\rangle 4$. $y \in \alpha$
□

Theorem 4.0.5. *A set α is an ordinal number if and only if it is a transitive set well-ordered by $\in$.*

PROOF:
$\langle 1\rangle 1$. Every ordinal number is a transitive set.
PROOF: Proposition 4.0.4.
$\langle 1\rangle 2$. Every ordinal number is well-ordered by $\in$.
PROOF: Corollary 4.0.3.2.
$\langle 1\rangle 3$. Every transitive set well-ordered by $\in$ is an ordinal number.
$\langle 2\rangle 1$. LET: α be a transitive set well-ordered by $\in$
$\langle 2\rangle 2$. LET: $E : (\alpha, \in) \cong (\beta, \in)$ be the isomorphism between $(\alpha, \in)$ and its ordinal number.
$\langle 2\rangle 3$. $\forall x \in \alpha . E(x) = x$
PROOF: By transfinite induction on x.
$\langle 2\rangle 4$. $\beta = \alpha$
□

Proposition 4.0.6. *Every element of an ordinal number is an ordinal number.*

PROOF:
$\langle 1\rangle 1$. LET: α be an ordinal number.
$\langle 1\rangle 2$. LET: $\beta \in \alpha$
$\langle 1\rangle 3$. β is a transitive set.
$\langle 2\rangle 1$. LET: $x \in y \in \beta$
$\langle 2\rangle 2$. $y \in \alpha$
PROOF: Since α is a transitive set.
$\langle 2\rangle 3$. $x \in \alpha$
PROOF: Since α is a transitive set.
$\langle 2\rangle 4$. $x \in \beta$
PROOF: Since α is well-ordered by $\in$.
$\langle 1\rangle 4$. β is well-ordered by $\in$.
PROOF: Since $\beta \subseteq \alpha$.
□

Proposition 4.0.7. *Given two ordinal numbers α, β, exactly one of $\alpha \in \beta$, $\alpha = \beta$, $\beta \in \alpha$ holds.*

PROOF:
$\langle 1\rangle 1$. At most one holds.
PROOF: Since 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 $\alpha = \beta$ as isomorphic well-ordered sets have the same ordinal number.
$\langle 2\rangle 3$. CASE: There exists $t \in \beta$ such that $\alpha \cong \operatorname{seg} t$
PROOF: t is an ordinal number and $\alpha = t$, so $\alpha \in \beta$.
$\langle 2\rangle 4$. CASE: There exists $t \in \alpha$ such that $\operatorname{seg} t \cong \beta$
PROOF: t is an ordinal number and $t = \beta$, so $\beta \in \alpha$.
□

Proposition 4.0.8. *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 β 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.
□

Proposition 4.0.9. *Any transitive set of ordinal numbers is an ordinal number.*

PROOF: It is well-ordered by $\in$ by the above propositions. □

Proposition 4.0.10. *$\emptyset$ is an ordinal number.*

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

Definition 4.0.11. We define $0 = \emptyset$.

Definition 4.0.12 (Successor)**.** The *successor* of a set a is the set $a^+ := a \cup \{a\}$.

Proposition 4.0.13. *A set a is a transitive set if and only if*

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

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: $x \in a$
$\langle 3\rangle 2$. 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 $a \in a^+$.

⟨1⟩2. If $\bigcup(a^+) = a$ then a is a transitive set.
⟨2⟩1. Assume: $\bigcup(a^+) = a$
⟨2⟩2. $\bigcup a \subseteq a$
Proof:

$$\begin{aligned}\bigcup a &\subseteq \bigcup(a^+) && \text{(Proposition 1.3.5)} \\ &= a && (\langle 2\rangle 1)\end{aligned}$$

⟨2⟩3. a is a transitive set.
Proof: Proposition 1.4.2.
□

Proposition 4.0.14. *For any set a, we have a is a transitive set if and only if a^+ is a transitive set.*

Proof:
⟨1⟩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 4.0.13 and so a^+ is a transitive set.
⟨1⟩2. If a^+ is a transitive set then a is a transitive set.
⟨2⟩1. Assume: a^+ is a transitive set.
⟨2⟩2. Let: $x \in y \in a$
⟨2⟩3. $x \in y \in a^+$
⟨2⟩4. $x \in a^+$
Proof: ⟨2⟩1
⟨2⟩5. $x \neq a$
Proof: From ⟨2⟩2 and the Axiom of Regularity.
⟨2⟩6. $x \in a$
□

Definition 4.0.15. We write 0 for $\emptyset$, 1 for $\emptyset^+$, 2 for $\emptyset^{++}$, etc.

Proposition 4.0.16. *For any ordinal number α we have α^+ is an ordinal number.*

Proof:
⟨1⟩1. α^+ is a transitive set.
Proof: Proposition 4.0.14.
⟨1⟩2. α^+ is well-ordered by $\in$.
⟨2⟩1. For all $x, y, z \in \alpha^+$, if $x \in y \in z$ then $x \in z$
⟨3⟩1. Case: $z = \alpha$
Proof: Then $x \in \alpha$ since α is a transitive set.
⟨3⟩2. Case: $z \in \alpha$
Proof: Then $x \in z$ since α is well-ordered by $\in$.
⟨2⟩2. For all $x, y \in \alpha^+$ we have $x \in y$ or $x = y$ or $y \in x$
⟨3⟩1. Case: $x, y \in \alpha$
Proof: The result follows because α is well-ordered by $\in$.
⟨3⟩2. Case: $x \in \alpha$, $y = \alpha$
Proof: Then $x \in y$.

⟨3⟩3. CASE: $x = \alpha$, $y \in \alpha$
PROOF: Then $y \in x$.
⟨3⟩4. CASE: $x = \alpha$, $y = \alpha$
PROOF: Then $x = y$.
⟨2⟩3. Every nonempty subset of α^+ has an $\in$-least element.
⟨3⟩1. LET: $S \subseteq \alpha^+$ be nonempty
⟨3⟩2. CASE: $S = \{\alpha\}$
PROOF: α is least in S.
⟨3⟩3. CASE: $S \neq \{\alpha\}$
⟨4⟩1. $S - \{\alpha\}$ is a nonempty subset of α
⟨4⟩2. LET: β be least in $S - \{\alpha\}$
⟨4⟩3. β is least in S.
□

Proposition 4.0.17. *If A is a set of ordinal numbers then $\bigcup A$ is an ordinal number.*

PROOF:
⟨1⟩1. $\bigcup A$ is a transitive set.
PROOF: Proposition 1.4.4.
⟨1⟩2. $\bigcup A$ is a set of ordinals.
□

Theorem 4.0.18 (Burali-Forti)**.** *The class of ordinal numbers is a proper class.*

PROOF: If it is a set then it is a transitive set of ordinal numbers, hence an ordinal number, hence a member of itself, which is impossible. □

Theorem 4.0.19 (Hartogs)**.** *For any set A, there exists an ordinal not dominated by A.*

PROOF:
⟨1⟩1. LET: α be the class of all ordinals β such that $\beta \preccurlyeq A$
PROVE: α is a set.
⟨1⟩2. LET: $W = \{(B, R) \mid B \subseteq A, R \text{ is a well ordering on } B\}$
⟨1⟩3. α 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 α.
⟨3⟩1. LET: $(B, R) \in W$
⟨3⟩2. LET: β 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 β 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 $\operatorname{ran} f$ by $f(x) \leq f(y)$ iff $x \leq y$

⟨3⟩4. $(\operatorname{ran} f, \leq) \in W$
⟨3⟩5. β is the ordinal number of $(\operatorname{ran} f, \leq)$
⟨1⟩4. α is a set.
PROOF: By an Axiom of Replacement.
⟨1⟩5. α is an ordinal.
PROOF: It is a transitive set of ordinals.
⟨1⟩6. $\alpha \not\preccurlyeq A$
PROOF: Since $\alpha \notin \alpha$.
□

Theorem 4.0.20 (Numeration Theorem). *Every set is equinumerous with some ordinal.*

PROOF:
⟨1⟩1. LET: A be any set.
⟨1⟩2. PICK an ordinal α 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: δ be least such that $F(\delta) = e$
⟨1⟩8. $F \restriction \delta : \delta \approx A$

Theorem 4.0.21 (Well-Ordering Theorem). *Any set can be well ordered.*

PROOF:
⟨1⟩1. PICK an ordinal δ 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.
□

Chapter 5

Cardinal Numbers

5.1 Cardinal Numbers

Definition 5.1.1 (Cardinality)**.** For any set A, the *cardinality* $|A|$ of A is the least ordinal equinumerous with A.

Proposition 5.1.2. *For any sets A and B, we have $A \approx B$ iff $|A| = |B|$.*

PROOF: Easy. $\square$

Definition 5.1.3 (Addition)**.** Given cardinal numbers κ and λ, we define $\kappa + \lambda$ to be $|A \cup B|$ where A and B are disjoint sets of cardinality κ and λ respectively.

We prove this is well-defined.

PROOF:
$\langle 1 \rangle 1$. ASSUME: $A \approx A'$, $B \approx B'$, and $A \cap B = A' \cap B' = \emptyset$
$\langle 1 \rangle 2$. PICK bijections $f : A \approx A'$ and $g : B \approx B'$
$\langle 1 \rangle 3$. 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.
$\square$

Proposition 5.1.4. *For any cardinal number κ, we have $\kappa + 0 = \kappa$.*

PROOF: Let A and B be disjoint sets of cardinality κ and 0. Then $B = \emptyset$ so $A \cup B = A$ and so $|A \cup B| = \kappa$. $\square$

Theorem 5.1.5 (Associative Law for Addition)**.** *For any cardinal numbers κ, λ, μ we have $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$.*

PROOF: Since $A \cup (B \cup C) = (A \cup B) \cup C$. $\square$

Proposition 5.1.6. *For any cardinal numbers κ and λ we have $\kappa + \lambda = \lambda + \kappa$.*

PROOF: Since $A \cup B = B \cup A$. $\square$

Definition 5.1.7 (Multiplication)**.** For κ and λ 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 $A \times B \approx A' \times B'$. □

Proposition 5.1.8. *For any cardinal number κ we have $\kappa \cdot 0 = 0$.*

PROOF: Since $A \times \emptyset = \emptyset$. □

Proposition 5.1.9. *For any cardinal number κ we have $\kappa \cdot 1 = \kappa$.*

PROOF: The function that maps (a, e) to a is a bijection $A \times \{e\} \approx A$. □

Theorem 5.1.10 (Distributive Law)**.** *For any cardinal numbers κ, λ and μ, we have $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$.*

PROOF: Since $A \times (B \cup C) = (A \times B) \cup (A \times C)$. □

Theorem 5.1.11 (Associative Law for Multiplication)**.** *For any cardinal numbers κ, λ and μ, we have $\kappa(\lambda\mu) = (\kappa\lambda)\mu$.*

PROOF: Since $A \times (B \times C) \approx (A \times B) \times C$. □

Theorem 5.1.12 (Commutative Law for Multiplication)**.** *For any cardinal numbers κ and λ, we have $\kappa\lambda = \lambda\kappa$.*

PROOF: Since $A \times B \approx B \times A$. □

Theorem 5.1.13. *For any cardinal numbers κ and λ, if $\kappa\lambda = 0$ then $\kappa = 0$ or $\lambda = 0$.*

PROOF: if $A \times B = \emptyset$ then $A = \emptyset$ or $B = \emptyset$. □

Definition 5.1.14 (Exponentiation)**.** Given cardinal numbers κ and λ, we define κ^λ 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 $A^B \approx A'^{B'}$. □

Proposition 5.1.15. *For any cardinal numbers κ, λ and μ,*

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

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 $A^{B \times C} \approx (A^B)^C$. □

Proposition 5.1.16. *For any cardinal numbers κ, λ and μ,*

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

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 5.1.17. *For any cardinal numbers κ, λ and μ, 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 5.1.18. *For any cardinal number κ, we have $\kappa^0 = 1$.*

PROOF: For any set A, we have $A^\emptyset = \{\emptyset\}$. $\square$

Proposition 5.1.19. *For any cardinal number κ, 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 5.1.20. *For any non-zero cardinal number κ we have $0^\kappa = 0$.*

PROOF: If A is nonempty then there is no function $A \to \emptyset$. $\square$

Proposition 5.1.21. *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 5.1.21.1. *For any cardinal number κ we have $2^\kappa \neq \kappa$.*

PROOF: By Cantor's Theorem. $\square$

5.2 Ordering on Cardinal Numbers

Definition 5.2.1 (Domination)**.** A set A is *dominated* by a set B, $A \preccurlyeq B$, iff there exists an injection $A \to B$.

Definition 5.2.2. Given cardinal numbers κ and λ, we write $\kappa \leq \lambda$ iff $A \preccurlyeq B$ where $|A| = \kappa$ and $|B| = \lambda$.

We prove this is well-defined.

PROOF: If $f : A \approx A'$, $g : B \approx B'$, and $h : A \to B$ is an injection, then $g \circ h \circ f^{-1}$ is an injection $A' \to B'$. $\square$

Chapter 6

Natural Numbers

6.1 Inductive Sets

Definition 6.1.1 (Inductive)**.** A set I is *inductive* iff $\emptyset \in I$ and $\forall x \in I.x^+ \in I$.

Definition 6.1.2 (Natural Number)**.** A *natural number* is a set that belongs to every inductive set.

Theorem 6.1.3. *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 6.1.4. $\mathbb{N}$ *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 6.1.4.1 (Induction Principle for $\mathbb{N}$)**.** *Any inductive subset of* $\mathbb{N}$ *coincides with* $\mathbb{N}$*.*

Theorem 6.1.5. *Every natural number except 0 is the successor of some natural number.*

Proof: Trivially by induction. ∎

Proposition 6.1.6. *Every natural number is a transitive set.*

Proof:
$\langle 1 \rangle 1$. 0 is a transitive set.
  Proof: Vacuously, if $x \in y \in 0$ then $x \in 0$.
$\langle 1 \rangle 2$. For every natural number n, if n is a transitive set then n^+ is a transitive set.
  Proof: Proposition 4.0.14.
∎

Proposition 6.1.7. *For natural numbers m and n, if $m^+ = n^+$ then $m = n$.*

Proof: If $m^+ = n^+$ then

$$\begin{aligned} m &= \bigcup(m^+) && \text{(Proposition 4.0.13)} \\ &= \bigcup(n^+) \\ &= n && \text{(Proposition 4.0.13)} \end{aligned}$$

Proposition 6.1.8. $\mathbb{N}$ *is a transitive set.*

Proof:
$\langle 1 \rangle 1$. $0 \subseteq \mathbb{N}$
$\langle 1 \rangle 2$. $\forall n \in \mathbb{N}. n \subseteq \mathbb{N} \Rightarrow n^+ \subseteq \mathbb{N}$
$\langle 1 \rangle 3$. $\forall n \in \mathbb{N}. n \subseteq \mathbb{N}$
  Proof: From $\langle 1 \rangle 1$ and $\langle 1 \rangle 2$ by induction.
∎

6.2 Ordering on $\mathbb{N}$

Definition 6.2.1. Given natural numbers m and n, we write $m < n$ iff $m \in n$. We write $m \leq n$ iff $m < n$ or $m = n$.

Proposition 6.2.2. *For any natural numbers m and n, we have $m < n$ if and only if $m^+ < n^+$.*

Proof:
$\langle 1 \rangle 1$. For any natural numbers m and n, if $m < n$ then $m^+ < n^+$.
  $\langle 2 \rangle 1$. For any natural number m, if $m < 0$ then $m^+ < 0^+$
    Proof: Vacuous.
  $\langle 2 \rangle 2$. For any natural number n, if $\forall m < n. m^+ < n^+$ then $\forall m < n^+. m^+ < n^{++}$

⟨3⟩1. LET: $m < n^+$
⟨3⟩2. $m < n$ or $m = n$
⟨3⟩3. CASE: $m < n$
⟨4⟩1. $m^+ < n^+$
PROOF: Induction hypothesis.
⟨4⟩2. $m^+ < n^{++}$
⟨3⟩4. CASE: $m = n$
PROOF: $m^+ = n^+ < n^{++}$.
⟨1⟩2. For any natural numbers m and n, if $m^+ < n^+$ then $m < n$.
⟨2⟩1. We never have $m^+ < 0^+$.
⟨3⟩1. $m^+ \not< 0$
⟨3⟩2. $m^+ \neq 0$
⟨3⟩3. $m^+ \not< 0^+$
⟨2⟩2. For any natural number n, if $\forall m.m^+ < n^+ \Rightarrow m < n$, then $\forall m.m^+ < n^{++} \Rightarrow m < n^+$.
⟨3⟩1. LET: n be a natural number.
⟨3⟩2. ASSUME: $\forall m.m^+ < n^+ \Rightarrow m < n$
⟨3⟩3. LET: m be a natural number.
⟨3⟩4. ASSUME: $m^+ < n^{++}$
⟨3⟩5. $m^+ < n^+$ or $m^+ = n^+$
⟨3⟩6. CASE: $m^+ < n^+$
⟨4⟩1. $m < n$
PROOF: Induction hypothesis.
⟨4⟩2. $m < n^+$
⟨3⟩7. CASE: $m^+ = n^+$
PROOF: $m = n < n^+$ by Proposition 6.1.7.
□

Theorem 6.2.3 (Trichotomy Law for $\mathbb{N}$)**.** *For any natural numbers m and n, exactly one of $m < n$, $n < m$, $m = n$ holds.*

PROOF:
⟨1⟩1. For all m and n, at most one of $m < n$, $n < m$, $m = n$ holds.
⟨2⟩1. We do not have $m < n$ and $m = n$.
PROOF: This would imply $n < n$ contradicting the Axiom of Regularity.
⟨2⟩2. We do not have $m < n$ and $n < m$.
PROOF: This would imply $n < n$ by Proposition 6.1.6, contradicting the Axiom of Regularity.
⟨1⟩2. For all m and n, either $m < n$ or $n < m$ or $m = n$.
⟨2⟩1. For all m, either $m = 0$ or $0 < m$.
⟨3⟩1. $0 = 0$
⟨3⟩2. For any natural number m, we have $0 < m^+$.
⟨4⟩1. $0 < 0^+$
⟨4⟩2. For any natural number m, if $0 < m^+$ then $0 < m^{++}$.
⟨2⟩2. For any natural number n, if $\forall m(m < n \vee n < m \vee m = n)$ then $\forall m(m < n^+ \vee n^+ < m \vee m = n^+)$.
⟨3⟩1. LET: n be a natural number.

⟨3⟩2. ASSUME: $\forall m(m < n \vee n < m \vee m = n)$
⟨3⟩3. LET: m be a natural number.
⟨3⟩4. CASE: $m < n$
PROOF: Then $m < n^+$.
⟨3⟩5. CASE: $n < m$
⟨4⟩1. $m \neq 0$
⟨4⟩2. PICK p such that $m = p^+$
⟨4⟩3. $n < p$ or $n = p$
⟨4⟩4. CASE: $n < p$
PROOF: Then $n^+ < p^+ = m$ by Proposition 6.2.2.
⟨4⟩5. CASE: $n = p$
PROOF: Then $n^+ = p^+ = m$.
⟨3⟩6. CASE: $m = n$
PROOF: Then $m < n^+$.
□

Corollary 6.2.3.1. *For natural numbers m and n, we have $m \leq n$ if and only if $m \subseteq n$.*

PROOF:
⟨1⟩1. If $m \leq n$ then $m \subseteq n$
⟨2⟩1. ASSUME: $m \leq n$
⟨2⟩2. LET: $p \in m$
⟨2⟩3. CASE: $m < n$
PROOF: Then $p \in n$ by Proposition 6.1.6.
⟨2⟩4. CASE: $m = n$
PROOF: Then $p \in n$ immediately.
⟨1⟩2. If $m \subseteq n$ then $m \leq n$
⟨2⟩1. ASSUME: $m \subseteq n$
⟨2⟩2. $n \not< m$
PROOF: If $n < m$ then $n \in n$ contradicting the Axiom of Regularity.
⟨2⟩3. $m \leq n$
PROOF: By trichotomy.
□

Theorem 6.2.4 (Well-Ordering of $\mathbb{N}$)**.** *Every nonempty subset of $\mathbb{N}$ has a least element.*

PROOF:
⟨1⟩1. LET: $A \subseteq \mathbb{N}$
⟨1⟩2. ASSUME: A has no least element.
PROVE: $A = \emptyset$
⟨1⟩3. $\forall n.\forall m < n.m \notin A$
⟨2⟩1. $\forall m < 0.m \notin A$
PROOF: Vacuous.
⟨2⟩2. For any natural number n, if $\forall m < n.m \notin A$, then $\forall m < n^+.m \notin A$.
⟨3⟩1. LET: n be a natural number.

$\langle 3\rangle 2$. ASSUME: $\forall m < n.m \notin A$
$\langle 3\rangle 3$. $n \notin A$
PROOF: If $n \in A$ then n is the least element in A.
$\langle 3\rangle 4$. $\forall m < n^+.m \notin A$
$\langle 1\rangle 4$. $A = \emptyset$
□

Corollary 6.2.4.1. *There is no function $f : \mathbb{N} \to \mathbb{N}$ such that $\forall n \in \mathbb{N}.f(n+1) < f(n)$.*

Theorem 6.2.5 (Strong Induction Principle for $\mathbb{N}$)**.** *Let $A \subseteq \mathbb{N}$. Assume that, for every $n \in \mathbb{N}$, if $\forall m < n.m \in A$ then $n \in A$. Then $A = \mathbb{N}$.*

PROOF:
$\langle 1\rangle 1$. ASSUME: for a contradiction $A \neq \mathbb{N}$
$\langle 1\rangle 2$. LET: n be the least element of $\mathbb{N} - A$
PROOF: Since $\mathbb{N}$ is well ordered.
$\langle 1\rangle 3$. $\forall m < n.m \in A$
$\langle 1\rangle 4$. $n \notin A$
$\langle 1\rangle 5$. Q.E.D.
PROOF: This contradicts the hypothesis of the theorem.
□

6.3 Recursion

Theorem 6.3.1. *Let $<$ be a linear ordering on A. Then $<$ is a well ordering on A if and only if there does not exist a function $f : \mathbb{N} \to A$ such that $\forall n \in \mathbb{N}.f(n+1) < f(n)$.*

PROOF:
$\langle 1\rangle 1$. If there exists a function $f : \mathbb{N} \to A$ such that $\forall n \in \mathbb{N}.f(n+1) < f(n)$ then $<$ is not a well ordering on A.
PROOF: $\operatorname{ran} f$ is a nonempty subset of A with no least element.
$\langle 1\rangle 2$. If $<$ is not a well ordering on A then there exists a function $f : \mathbb{N} \to A$ such that $\forall n \in \mathbb{N}.f(n+1) < f(n)$.
$\langle 2\rangle 1$. ASSUME: $<$ is not a well ordering on A.
$\langle 2\rangle 2$. PICK a nonempty subset $B \subseteq A$ that has no least element.
$\langle 2\rangle 3$. $\forall x \in B.\exists y \in B.y < x$
$\langle 2\rangle 4$. Choose a function $g : B \to B$ such that $\forall x \in B.g(x) < x$
$\langle 2\rangle 5$. PICK $b \in B$
$\langle 2\rangle 6$. Define $f : \mathbb{N} \to A$ recursively by $f(0) = b$ and $\forall n \in \mathbb{N}.f(n+1) = g(f(n))$
$\langle 2\rangle 7$. $\forall n \in \mathbb{N}.f(n+1) < f(n)$
□

6.4 Cardinality

Definition 6.4.1 (Finite)**.** A set is *finite* iff it is equinumerous to some natural number; otherwise it is *infinite*.

Theorem 6.4.2 (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: $n \notin ranf$
$\langle 3\rangle 1.$ $f \restriction n : n \to n$
$\langle 3\rangle 2.$ $\mathrm{ran}(f \restriction n) = n$
$\langle 3\rangle 3.$ $f(n) = n$
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

$$\hat{f}(p) = f(n)$$
$$\hat{f}(x) = f(x) \qquad (x \neq p)$$

$\langle 3\rangle 3.$ $\hat{f}$ 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 6.4.2.1. *No finite set is equinumerous to a proper subset of itself.*

Corollary 6.4.2.2. *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 6.4.2.3. $\mathbb{N}$ *is infinite.*

PROOF: The function that maps n to $n+1$ is a bijection between $\mathbb{N}$ and $\mathbb{N} - \{0\}$. $\square$

Proposition 6.4.3. *If C is a proper subset of a natural number n, then there exists $m < n$ such that $C \approx m$.*

PROOF:
$\langle 1\rangle 1$. LET: $P(n)$ be the property: for every proper subset C of n, there exists a natural number m such that $C \approx m$.
$\langle 1\rangle 2$. $P(0)$
PROOF: Vacuous.
$\langle 1\rangle 3$. For every natural number n, if $P(n)$ then $P(n+1)$.
$\langle 2\rangle 1$. LET: n be a natural number.
$\langle 2\rangle 2$. ASSUME: $P(n)$
$\langle 2\rangle 3$. LET: C be a proper subset of $n+1$
$\langle 2\rangle 4$. CASE: $C = n$
PROOF: $C \approx n < n+1$
$\langle 2\rangle 5$. CASE: $C \subsetneq n$
PROOF: There exists $m < n$ such that $C \approx m$ by $\langle 2\rangle 2$.
$\langle 2\rangle 6$. CASE: $n \in C$
$\langle 3\rangle 1$. $C - \{n\} \subsetneq n$
$\langle 3\rangle 2$. PICK $m < n$ such that $C - \{n\} \approx m$
$\langle 3\rangle 3$. $C \approx m+1$
$\langle 1\rangle 4$. For every natural number n, $P(n)$.
□

Corollary 6.4.3.1. *Any subset of a finite set is finite.*

Proposition 6.4.4. *For any natural numbers m and n we have $m + n^+ = (m+n)^+$.*

PROOF:
$\langle 1\rangle 1$. PICK disjoint sets A and B of cardinalities m and n.
$\langle 1\rangle 2$. PICK an element $e \notin A \cup B$
$\langle 1\rangle 3$. $A \cup B \cup \{e\} \approx m + n^+$
$\langle 1\rangle 4$. $A \cup B \cup \{e\} \approx (m+n)^+$
□

Proposition 6.4.5. *For any natural numbers m and n we have $m+n$ is a natural number.*

PROOF: Induction on n. □

Proposition 6.4.6. *For any natural numbers m and n we have $m \cdot n^+ = mn + m$.*

PROOF:
$\langle 1\rangle 1$. PICK sets A and B of cardinality m and n respectively.
$\langle 1\rangle 2$. PICK $e \notin B$
$\langle 1\rangle 3$. $A \times (B \cup \{e\}) = (A \times B) \cup (A \times \{e\})$
□

Corollary 6.4.6.1. *For any natural numbers m and n, we have mn is a natural number.*

Corollary 6.4.6.2. *If A and B are finite sets then $A \times B$ is finite.*

Proposition 6.4.7. *The union of a finite set of finite sets is finite.*

PROOF: By induction on the number of elements. □

Proposition 6.4.8. $\mathbb{N}^2 \approx \mathbb{N}$

PROOF: The function $J : \mathbb{N}^2 \to \mathbb{N}$ defined by $J(m, n) = ((m + n)^2 + 3m + n)/2$ is a bijection. □

Corollary 6.4.8.1. *For any natural numbers m and n, we have m^n is a natural number.*

PROOF: By induction on n since $m^0 = 1$ and $m^{n+1} = m^n m$. □

Corollary 6.4.8.2. *If A and B are finite sets then A^B are finite.*

6.5 Arithmetic

Definition 6.5.1 (Even)**.** A natural number n is *even* iff there exists $m \in \mathbb{N}$ such that $n = 2m$.

Definition 6.5.2 (Odd)**.** A natural number n is *odd* iff there exists $p \in \mathbb{N}$ such that $n = 2p + 1$.

Proposition 6.5.3 (Division Algorithm)**.** *Let m be a natural number and d a nonzero natural number. Then there exist natural numbers q and r such that $m = dq + r$ and $r < d$.*

PROOF:
⟨1⟩1. LET: d be a nonzero natural number.
⟨1⟩2. $\exists q, r.0 = dq + r \wedge r < d$
  PROOF: Take $q = r = 0$.
⟨1⟩3. For any natural number m, if $\exists q, r.m = dq + r \wedge r < d$ then $\exists q, r.m^+ = dq + r \wedge r < d$
  ⟨2⟩1. LET: m be a natural number.
  ⟨2⟩2. ASSUME: $m = dq + r$ and $r < d$
  ⟨2⟩3. $r^+ \leq d$
  ⟨2⟩4. CASE: $r^+ < d$
    PROOF: In this case we have $m^+ = dq + r^+$.
  ⟨2⟩5. CASE: $r^+ = d$
    PROOF: In this case we have $m^+ = dq^+ + 0$.
□

Proposition 6.5.4. *Every natural number is either even or odd.*

PROOF:
⟨1⟩1. 0 is even.
  PROOF: $0 = 2 \times 0$.
⟨1⟩2. For any natural number n, if n is either even or odd then n^+ is either even or odd.

PROOF:
⟨2⟩1. LET: $n \in \mathbb{N}$
⟨2⟩2. If n is even then n^+ is odd.
PROOF: If $n = 2p$ then $n^+ = 2p + 1$.
⟨2⟩3. If n is odd then n^+ is even.
PROOF: If $n = 2p + 1$ then $n^+ = 2(p + 1)$.
□

Proposition 6.5.5. *No natural number is both even and odd.*

PROOF:
⟨1⟩1. 0 is not odd.
PROOF: For any p we have $2p + 1 = (2p)^+ \neq 0$.
⟨1⟩2. For any natural number n, if n is not both even and odd, then n^+ is not both even and odd.
⟨2⟩1. LET: n be a natural number.
⟨2⟩2. If n^+ is even then n is odd.
⟨3⟩1. ASSUME: n^+ is even.
⟨3⟩2. PICK p such that $n^+ = 2p$
⟨3⟩3. $p \neq 0$
PROOF: Since $n^+ \neq 0$.
⟨3⟩4. PICK q such that $p = q^+$
PROOF: Theorem 6.1.5.
⟨3⟩5. $n^+ = 2q + 2$
PROOF: ⟨3⟩2, ⟨3⟩4.
⟨3⟩6. $n = 2q + 1$
PROOF: Proposition 6.1.7, ⟨3⟩5
⟨3⟩7. n is odd.
⟨2⟩3. If n^+ is odd then n is even.
⟨3⟩1. ASSUME: n^+ is odd.
⟨3⟩2. PICK p such that $n^+ = 2p + 1$
⟨3⟩3. $n = 2p$
PROOF: Proposition 6.1.7, ⟨3⟩2
⟨3⟩4. n is even.
□

Proposition 6.5.6. *For any natural numbers m and n, we have $m < n$ if and only if there exists $p \in \mathbb{N}$ such that $n = m + p^+$.*

PROOF:
⟨1⟩1. For any natural numbers m and p we have $m < m + p^+$.
⟨2⟩1. $\forall m. m < m + 0^+$
PROOF: Since $m \in m^+ = m + 0^+$.
⟨2⟩2. For any natural number p, if $\forall m. m < m + p^+$ then $\forall m. m < m + p^{++}$
PROOF: If $m \in m + p^+$ then $m \in (m + p^+)^+ = m + p^{++}$.
⟨1⟩2. For any natural numbers m and n, if $m < n$ then there exists p such that $n = m + p^+$.

⟨2⟩1. $\forall m < 0.\exists p.0 = m + p^+$
PROOF: Vacuous.
⟨2⟩2. For any natural number n, if $\forall m < n.\exists p.n = m + p^+$, then $\forall m < n^+.\exists p.n^+ = m + p^+$.
⟨3⟩1. LET: n be a natural number.
⟨3⟩2. ASSUME: $\forall m < n.\exists p.n = m + p^+$
⟨3⟩3. LET: $m < n^+$
⟨3⟩4. $m < n$ or $m = n$
⟨3⟩5. CASE: $m < n$
⟨4⟩1. PICK p such that $n = m + p^+$
⟨4⟩2. $n^+ = m + p^{++}$
⟨3⟩6. CASE: $m = n$
PROOF: Then $n^+ = m + 0^+$.

□

Theorem 6.5.7. *For natural numbers m, n and p, we have $m < n$ iff $m + p < n + p$.*

PROOF:
⟨1⟩1. $\forall m, n.m < n \Leftrightarrow p + 0 < n + 0$
⟨1⟩2. For any natural number p, if $\forall m, n.m < n \Leftrightarrow m+p < n+p$ then $\forall m, n.m < n \Leftrightarrow m + p^+ < n + p^+$
PROOF: Proposition 6.2.2.

□

Corollary 6.5.7.1. *For natural numbers m, n and p, if $m + p = n + p$ then $m = n$.*

PROOF: By trichotomy. □

Theorem 6.5.8. *For natural numbers m, n and p, if $m < n$ and $p \neq 0$ then $mp < np$.*

PROOF:
⟨1⟩1. LET: m and n be natural numbers.
⟨1⟩2. ASSUME: $m < n$
PROVE: $\forall p.mp^+ < np^+$
⟨1⟩3. $m0^+ < n0^+$
PROOF: Proposition **??**.
⟨1⟩4. For any natural number p, if $mp < np$ then $mp^+ < np^+$
PROOF:

$$\begin{aligned} mp^+ &= mp + m \\ &< np + m && \text{(induction hypothesis. Theorem 6.5.7)} \\ &< np + n && \text{(⟨1⟩2, Theorem 6.5.7)} \\ &= np^+ \end{aligned}$$

□

Corollary 6.5.8.1. *For natural numbers m, n and p, if $p \neq 0$ then $m < n$ if and only if $mp < np$.*

PROOF: Proposition 3.1.23. ∎

Corollary 6.5.8.2. *For natural numbers m, n and p, if $mp = np$ and $p \neq 0$ then $m = n$.*

PROOF: By trichotomy. ∎

Proposition 6.5.9. *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 $m + n < p + q$.
$\langle 1 \rangle 2$. If $q < n$ then $m < p$.
  PROOF: Similar.
∎

Proposition 6.5.10. *Let m, n, p and q be natural numbers. Assume $n < m$ and $q < p$. Then*

$$mq + np < mp + nq \ .$$

PROOF:
$\langle 1 \rangle 1$. PICK positive natural numbers a and b such that $m = n+a$ and $p = q+b$.
$\langle 1 \rangle 2$. $mp + nq > mq + np$
  PROOF:

$$\begin{aligned} mp + nq &= (n+a)(q+b) + nq \\ &= 2nq + nb + aq + ab \\ mq + np &= (n+a)q + n(q+b) \\ &= 2nq + aq + nb \\ \therefore mp + nq &= mq + np + ab \\ &> mq + np \end{aligned}$$

∎

Chapter 7

Group Theory

7.1 Groups

Definition 7.1.1 (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 7.1.2. *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:

$$\begin{aligned} b &= be \\ &= bab' \\ &= eb' \\ &= b' \end{aligned}$$

∎

Definition 7.1.3. We write x^{-1} for the inverse of x.

Proposition 7.1.4. *In any group, if $ab = ac$ then $b = c$.*

Proof:

$$\begin{aligned} b &= eb \\ &= a^{-1}ab \\ &= a^{-1}ac \\ &= ec \\ &= c \end{aligned}$$

∎

7.2 Abelian Groups

Definition 7.2.1 (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 8

Ring Theory

8.1 Rings

Definition 8.1.1 (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 8.1.2. *In any commutative ring,* $0x = 0$*.*

PROOF:

$$\begin{aligned} (0+0)x &= 0x \\ \therefore 0x + 0x &= 0x + 0 \\ \therefore 0x &= 0 \qquad \text{(Proposition 7.1.4)} \square \end{aligned}$$

Proposition 8.1.3. *In any commutative ring,* $(-a)b = -(ab)$*.*

PROOF:

$$\begin{aligned} ab + (-a)b &= (a + (-a))b \\ &= 0b \\ &= 0 \qquad \text{(Proposition 8.1.2)} \square \end{aligned}$$

8.2 Ordered Rings

Definition 8.2.1 (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 8.2.2. *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 8.2.3. *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 $z = (x + y)/2$. □

8.3 Integral Domains

Definition 8.3.1 (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 8.3.2. *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 8.3.3 (Ordered Integral Domain)**.** An *ordered integral domain* is an ordered commutative ring that is an integral domain.

Chapter 9

Field Theory

9.1 Fields

Definition 9.1.1 (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 9.1.2. *Every field is an integral domain.*

PROOF: If $ab = 0$ and $a \neq 0$ then $b = a^{-1}ab = 0$. $\square$

Proposition 9.1.3. *In any field F, we have $F - \{0\}$ is an Abelian group under multiplication.*

PROOF: Immediate from the definition. $\square$

Definition 9.1.4 (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. $\sim$ 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 8.3.2.
□
⟨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:

$$\begin{aligned}(ad + bc)b'd' &= ab'dd' + bb'cd' \\ &= a'bdd' + bb'c'd \\ &= (a'd' + b'c')bd\end{aligned}$$

□
⟨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:

$$\begin{aligned}[(a, b)] + ([(c, d)] + [(e, f)]) &= [(a, b)] + [(cf + de, df)] \\ &= [(adf + bcf + bde, bdf)] \\ &= [(ad + bc, bd)] + [(e, f)] \\ &= ([(a, b)] + [(c, d)]) + [(e, f)]\end{aligned}$$ □

⟨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. $[(a, b)][(b, a)] = [(1, 1)]$
□
□

Definition 9.1.5. 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 9.1.6 (Characteristic Zero)**.** A field F has *characteristic 0* iff $0 \notin N(F)$.

Proposition 9.1.7. *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 $\operatorname{ran} n$ is a subset of F that includes 1 and is closed under $+1$.
□

Definition 9.1.8. In any field F, let

$$I(F) = N(F) \cup \{0\} \cup \{-x \mid x \in N(F)\}$$

Definition 9.1.9. In any field F, let

$$Q(F) = \{x/y \mid x, y \in I(F), y \neq 0\}$$

Proposition 9.1.10. *$Q(F)$ 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 $Q(F)$. □

Theorem 9.1.11. *Let F and G be fields of characteristic 0. Then there exists a unique field isomorphism between $Q(F)$ and $Q(G)$.*

PROOF:

$\langle 1\rangle 1$. LET: $\phi : N(F) \to N(G)$ be the unique function such that $\phi(1) = 1$ and $\forall x \in N(F).\phi(x+1) = \phi(x) + 1$.

$\langle 1\rangle 2$. ϕ is a bijection.

PROOF: Similar to Proposition 9.1.7.

$\langle 1\rangle 3$. $\forall x, y \in N(F).\phi(x+y) = \phi(x) + \phi(y)$

PROOF: Induction on y.

$\langle 1\rangle 4$. $\forall x, y \in N(F).\phi(xy) = \phi(x)\phi(y)$

PROOF: Induction on y.

$\langle 1\rangle 5$. Extend ϕ to a bijection $I(F) \cong I(G)$ such that $\forall x, y \in I(F).\phi(x+y) = \phi(x) + \phi(y)$ and $\forall x, y \in I(F).\phi(xy) = \phi(x)\phi(y)$

$\langle 2\rangle 1$. Define $\phi(0) = 0$ and $\phi(-x) = -\phi(x)$ for $x \in N(F)$

$\langle 3\rangle 1$. $0 \notin N(F)$

$\langle 3\rangle 2$. For all $x \in N(F)$ we have $-x \notin N(F)$

PROOF: Then we would have $x + -x = 0 \in N(F)$.

$\langle 3\rangle 3$. For all $x \in N(F)$ we have $-x \neq 0$

$\langle 2\rangle 2$. For all $x, y \in I(F)$ we have $\phi(x+y) = \phi(x) + \phi(y)$

PROOF: Case analysis on x and y.

$\langle 2\rangle 3$. For all $x, y \in I(F)$ we have $\phi(xy) = \phi(x)\phi(y)$

PROOF: Case analysis on x and y.

$\langle 1\rangle 6$. Extend ϕ to a bijection $Q(F) \cong Q(G)$ such that $\forall x, y \in Q(F).\phi(x+y) = \phi(x) + \phi(y)$ and $\forall x, y \in Q(F).\phi(xy) = \phi(x)\phi(y)$

$\langle 2\rangle 1$. Define $\phi(x/y) = \phi(x)/\phi(y)$

$\langle 1\rangle 7$. ϕ is unique.

$\langle 2\rangle 1$. LET: θ satisfy the theorem.

$\langle 2\rangle 2$. For all $x \in N(F)$ we have $\theta(x) = \phi(x)$

$\langle 2\rangle 3$. For all $x \in I(F)$ we have $\theta(x) = \phi(x)$

$\langle 2\rangle 4$. For all $x \in Q(F)$ we have $\theta(x) = \phi(x)$

□

9.2 Ordered Fields

Definition 9.2.1 (Ordered Field)**.** An *ordered field* is an ordered commutative ring that is a field.

Proposition 9.2.2. *Every ordered field F has characteristic 0.*

PROOF: We have $0 < n$ for all $n \in N(F)$. □

Proposition 9.2.3. *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 9.2.3.1. *Let F and G be ordered fields. Let ϕ be the unique field isomorphism between $Q(F)$ and $Q(G)$. Then ϕ is an ordered field isomorphism.*

Definition 9.2.4 (Archimedean)**.** An ordered field F is *Archimedean* iff

$$\forall x \in F.\exists n \in N(F).n > x \ .$$

Proposition 9.2.5. *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 $n > y/x$. □

Proposition 9.2.6. *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 9.2.5.
⟨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 9.2.7 (Complete)**.** An ordered field F is *complete* iff every nonempty subset of F bounded above has a least upper bound.

Proposition 9.2.8. *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.
□

Proposition 9.2.9. *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. ϕ is strictly monotone.
⟨2⟩1. LET: $0 \leq x < y \leq 1 + a$
⟨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 9.2.10 (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 9.2.3.1.
⟨1⟩2. $Q(F)$ intersects every interval in F.
PROOF: Proposition 9.2.6.
⟨1⟩3. $Q(G)$ intersects every interval in G.
PROOF: Proposition 9.2.6.
⟨1⟩4. PICK an order isomorphism $\psi : F \cong G$ that extends ϕ.
PROOF: Theorem 2.5.21.
⟨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. $x < r$

$\langle 3\rangle 11.$ $y < s$
$\langle 3\rangle 12.$ $x + y > r + s$
$\langle 3\rangle 13.$ Q.E.D.
Proof: This is a contradiction.
$\langle 2\rangle 3.$ $\psi(x + y) \not< \psi(x) + \psi(y)$
Proof: Similar.
$\langle 1\rangle 6.$ $\forall x, y \in F.\psi(xy) = \psi(x)\psi(y)$
$\langle 2\rangle 1.$ Let: $x, y \in F$
$\langle 2\rangle 2.$ Case: x and y are positive.
$\langle 3\rangle 1.$ $\psi(x)\psi(y) \not< \psi(xy)$
$\langle 4\rangle 1.$ Assume: for a contradiction $\psi(x)\psi(y) < \psi(xy)$
$\langle 4\rangle 2.$ Pick $r' \in Q(G)$ such that $\psi(x) < r' < \psi(xy)/\psi(y)$
$\langle 4\rangle 3.$ Pick $s' \in Q(G)$ such that $\psi(y) < s' < \psi(xy)/r'$
$\langle 4\rangle 4.$ $r's' < \psi(xy)$
$\langle 4\rangle 5.$ Pick $r, s \in Q(F)$ such that $\phi(r) = r'$ and $\phi(s) = s'$
$\langle 4\rangle 6.$ $\phi(rs) = r's'$
$\langle 4\rangle 7.$ $x < r$, $y < s$ and $rs < xy$
$\langle 4\rangle 8.$ Q.E.D.
Proof: This is a contradiction.
$\langle 3\rangle 2.$ $\psi(xy) \not< \psi(x)\psi(y)$
Proof: Similar.
$\langle 2\rangle 3.$ Case: x and y are not both positive.
Proof: Follows from $\langle 2\rangle 2$ since $\psi(-x) = -\psi(x)$ by $\langle 1\rangle 5$.
$\langle 1\rangle 7.$ For any field isomorphism $\theta : F \cong G$, we have $\theta = \psi$.
$\langle 2\rangle 1.$ $\theta \restriction Q(F) = \phi$
Proof: Theorem 9.1.11.
$\langle 2\rangle 2.$ θ is strictly monotone.
$\langle 3\rangle 1.$ Let: $x, y \in F$ with $x < y$
$\langle 3\rangle 2.$ $y - x > 0$
$\langle 3\rangle 3.$ Pick $z \in F$ such that $z^2 = y - x$
$\langle 3\rangle 4.$ $\theta(z)^2 = \theta(y) - \theta(x)$
$\langle 3\rangle 5.$ $\theta(y) - \theta(x) > 0$
$\langle 3\rangle 6.$ $\theta(x) < \theta(y)$
$\langle 2\rangle 3.$ $\theta = \psi$
Proof: By the uniqueness of ψ.
$\square$

Chapter 10

Number Systems

10.1 The Integers

Definition 10.1.1. 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:
⟨1⟩1. $\sim$ is reflexive.
PROOF: For all $m,n \in \mathbb{N}$ we have $m+n = n+m$.
⟨1⟩2. $\sim$ is symmetric.
PROOF: If $m+q = n+p$ then $p+n = q+m$.
⟨1⟩3. $\sim$ is transitive.
⟨2⟩1. ASSUME: $(m,n) \sim (p,q) \sim (r,s)$
⟨2⟩2. $m+q = n+p$ and $p+s = q+r$
⟨2⟩3. $m+q+s = n+q+r$
⟨2⟩4. $m+s = n+r$
PROOF: Corollary 6.5.7.1.
□

Definition 10.1.2 (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 10.1.3. *Addition on $\mathbb{Z}$ is commutative.*

PROOF: $[(m,n)]+[(p,q)] = [(m+p, n+q)] = [(p+m, q+n)] = [(p,q)]+[(m,n)]$.
□

Proposition 10.1.4. *Addition on $\mathbb{Z}$ is associative.*

PROOF: $[(m,n)] + ([(p,q)] + [(r,s)]) = [(m+p+r, n+q+s)] = ([(m,n)] + [(p,q)]) + [(r,s)]$. □

Proposition 10.1.5. *Given natural numbers m and n, we have $[(m,0)] = [(n,0)]$ iff $m = n$.*

PROOF: Immediate from definitions. □

Definition 10.1.6. We identify any natural number n with the integer $[(n,0)]$.

Proposition 10.1.7. *Addition on integers agrees with addition on natural numbers.*

PROOF: Since $[(m,0)] + [(n,0)] = [(m+n,0)]$. □

Proposition 10.1.8. *For all $a \in \mathbb{Z}$ we have $a + 0 = a$.*

PROOF: $[(m,n)] + [(0,0)] = [(m+0, n+0)] = [(m,n)]$. □

Proposition 10.1.9. *For all $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0$.*

PROOF: $[(m,n)] + [(n,m)] = [(m+n, m+n)] = [(0,0)]$ □

Proposition 10.1.10. *The integers form an Abelian group under addition.*

PROOF: Proposition 10.1.3, 10.1.4, 10.1.8, 10.1.9. □

Definition 10.1.11. Define multiplication $\cdot$ on $\mathbb{Z}$ by: $[(m,n)][(p,q)] = [(mp + nq, mq + np)]$.

We prove this is well defined.

PROOF:
⟨1⟩1. ASSUME: $m + n' = n + m'$ and $p + q' = q + p'$
PROVE: $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$
⟨1⟩2. $mp + n'p = np + m'p$
⟨1⟩3. $nq + m'q = mq + n'q$
⟨1⟩4. $m'p + m'q' = m'q + m'p'$
⟨1⟩5. $n'q + n'p' = n'p + n'q'$
⟨1⟩6. $mp + n'p + nq + m'q + m'p + m'q' + n'q + n'p' = np + m'p + mq + n'q + m'q + m'p' + n'p + n'q'$
⟨1⟩7. $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$
PROOF: Corollary 6.5.7.1.
□

Proposition 10.1.12. *Multiplication on integers agrees with multiplication on natural numbers.*

PROOF: Since $[(m,0)][(n,0)] = [(mn + 0, m0 + n0)] = [(mn,0)]$. □

Proposition 10.1.13. *Multiplication on $\mathbb{Z}$ is commutative.*

PROOF: $[(m,n)][(p,q)] = [(mp + nq, mq + np)] = [(pm + qn, pn + qm)] = [(p,q)][(m,n)]$. □

Proposition 10.1.14. *Multiplication on $\mathbb{Z}$ is associative.*

PROOF:

$$\begin{aligned}[(m,n)]([(p,q)][(r,s)]) &= [(m,n)][(pr+qs, ps+qr)] \\ &= [(mpr+mqs+nps+nqr, mps+mqr+npr+nqs)] \\ &= [(mp+nq, mq+np)][(r,s)] \\ &= ([(m,n)][(p,q)])[(r,s)]\end{aligned}$$

∎

Proposition 10.1.15. *Multiplication distributes over addition.*

PROOF:

$$\begin{aligned}[(m,n)]([(p,q)]+[(r,s)]) &= [(m,n)][(p+r, q+s)] \\ &= [(mp+mr+nq+ns, np+nr+mq+ms)] \\ [(m,n)][(p,q)]+[(m,n)][(r,s)] &= [(mp+nq, mq+np)]+[(mr+ns, ms+nr)] \\ &= [(mp+nq+mr+ns, mq+np+ms+nr)]\end{aligned}$$

∎

Proposition 10.1.16. *For any integer a we have $a1 = a$.*

PROOF: Since $[(m,n)][(1,0)] = [(m1+n0, m0+n1)] = [(m,n)]$. ∎

Proposition 10.1.17. *For any integeres a and b, if $ab = 0$ then $a = 0$ or $b = 0$.*

PROOF:
⟨1⟩1. ASSUME: $[(m,n)][(p,q)] = [(0,0)]$
⟨1⟩2. $mp + nq = mq + np$
⟨1⟩3. ASSUME: $[(m,n)] \neq [(0,0)]$
⟨1⟩4. $m \neq n$
PROVE: $p = q$
⟨1⟩5. CASE: $m < n$
⟨2⟩1. $p \nless q$
PROOF: If $p < q$ then $mq + np < mp + nq$ by Proposition 6.5.10.
⟨2⟩2. $q \nless p$
PROOF: If $q < p$ then $mp + nq < mq + np$ by Proposition 6.5.10.
⟨2⟩3. $p = q$
PROOF: By trichotomy.
⟨1⟩6. CASE: $n < m$
PROOF: Similar.
∎

Proposition 10.1.18. *The integers $\mathbb{Z}$ form an integral domain.*

PROOF: Propositions 10.1.13, 10.1.14, 10.1.15, 10.1.16, 10.1.17, 10.1.10. ∎

Definition 10.1.19. 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:

$$\begin{aligned}
m + q < n + p &\Leftrightarrow m + n' + q < n + n' + p && \text{(Theorem 6.5.7)} \\
&\Leftrightarrow m' + n + q < n + n' + p \\
&\Leftrightarrow m' + q < n' + p && \text{(Theorem 6.5.7)} \\
&\Leftrightarrow m' + q + p' < n' + p + p' && \text{(Theorem 6.5.7)} \\
&\Leftrightarrow m' + q' + p < n' + p + p' \\
&\Leftrightarrow m' + q' < n' + p' && \text{(Theorem 6.5.7)}\square
\end{aligned}$$

Proposition 10.1.20. *The ordering on the integers agrees with the ordering on the natural numbers.*

PROOF: We have $[(m, 0)] < [(n, 0)]$ iff $m < n$. □

Proposition 10.1.21. $<$ *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: Theorem 6.5.7.
⟨1⟩3. $<$ is total.
PROOF: Given natural numbers m, n, p and q, either $m + q < n + p$, or $m + q = n + p$, or $n + p < m + q$.
□

Definition 10.1.22 (Positive)**.** An integer a is *positive* iff $a > 0$.

Theorem 10.1.23. *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. $a + c < b + c$

⟨1⟩2. If $a + c < b + c$ then $a < b$.
PROOF: From ⟨1⟩1 and Proposition 3.1.23.
□

Proposition 10.1.24. *Let a, b and c be integers. If $0 < c$, then $a < b$ if and only if $ac < bc$.*

PROOF:
⟨1⟩1. LET: $c = [(r, s)]$
⟨1⟩2. ASSUME: $0 < c$
⟨1⟩3. $s < r$
⟨1⟩4. For all integers a and b, if $a < b$ then $ac < bc$
⟨2⟩1. LET: $a = [(m, n)]$, $b = [(p, q)]$.
⟨2⟩2. ASSUME: $a < b$
⟨2⟩3. $m + q < n + p$
⟨2⟩4. $(m + q)r + (p + n)s < (m + q)s + (p + n)r$
PROOF: Proposition 6.5.10, ⟨1⟩3, ⟨2⟩3.
⟨2⟩5. $mr + ns + ps + qr < ms + nr + pr + qs$
⟨2⟩6. $[(mr + ns, ms + nr)] < [(pr + qs, ps + qr)]$
⟨2⟩7. $ac < bc$
⟨1⟩5. For all integers a and b, if $ac < bc$ then $a < b$
PROOF: From ⟨1⟩4 and Proposition 3.1.23.
□

Proposition 10.1.25. *Let a be a positive integer. For any integer b, there exists $k \in \mathbb{N}$ such that $b < ak$.*

PROOF:
⟨1⟩1. CASE: $b \leq 0$
PROOF: Take $k = 1$.
⟨1⟩2. CASE: $b > 0$
PROOF: Take $k = b + 1$.
□

10.2 The Rationals

Definition 10.2.1 (Rational Numbers)**.** The set $\mathbb{Q}$ of *rational numbers* is the field of fractions over the integers.

Proposition 10.2.2. *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 10.2.3. *Addition on the rationals agrees with addition on the integers.*

PROOF: $[(a,1)] + [(b,1)] = [(a \cdot 1 + b \cdot 1, 1 \cdot 1)] = [(a+b,1)]$. ∎

Proposition 10.2.4. *Multiplication on the rationals agrees with multiplication on the integers.*

PROOF: $[(a,1)][(b,1)] = [(ab,1)]$ ∎

Definition 10.2.5. 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.
∎

Proposition 10.2.6. *The ordering on the rationals agrees with the ordering on the integers.*

PROOF: We have $[(a,1)] < [(b,1)]$ if and only if $a < b$. ∎

Proposition 10.2.7. *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 10.2.8. *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:

$$\begin{aligned}[(a,b)] + [(e,f)] < [(c,d)] + [(e,f)] &\Leftrightarrow [(af + be, bf)] < [(cf + de, df)] \\ &\Leftrightarrow (af + be)df < (cf + de)bf \\ &\Leftrightarrow afdf + bedf < cfbf + debf \\ &\Leftrightarrow afdf < cfbf \\ &\Leftrightarrow ad < bc \\ &\Leftrightarrow [(a,b)] < [(c,d)]\end{aligned}$$

∎

Corollary 10.2.8.1. *For any rational r, we have $r < 0$ if and only if $0 < -r$.*

Definition 10.2.9 (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 10.2.10. *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:

$$\begin{aligned}rt < st &\Leftrightarrow [(ae, bf)] < [(ce, df)] \\ &\Leftrightarrow aedf < cebf \\ &\Leftrightarrow ad < bc \\ &\Leftrightarrow r < s\end{aligned}$$

∎

Corollary 10.2.10.1. *The rationals form an ordered field.*

Proposition 10.2.11. *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 10.1.25.
$\langle 1\rangle 3$. $r < pk$
□

Proposition 10.2.12. $\mathbb{Q} \approx \mathbb{N}$

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. □

10.3 The Real Numbers

Definition 10.3.1 (Cauchy Sequence)**.** A *Cauchy sequence* is a sequence (q_n) of rationals such that, for every positive rational ϵ, there exists $k \in \mathbb{N}$ such that $\forall m, n > k. |q_m - q_n| < \epsilon$.

Definition 10.3.2 (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 10.3.3. *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 $r < (q + r)/2 \in q \downarrow$.
□

Proposition 10.3.4. *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 $q \notin q\downarrow$.
□

Henceforth we identify a rational q with the real number $\{r \in \mathbb{Q} \mid r < q\}$.

Definition 10.3.5. Define the ordering $<$ on $\mathbb{R}$ by: $x < y$ iff $x \subsetneq y$.

Proposition 10.3.6. *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 10.3.4.
$\langle 1\rangle 5$. 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 $s \notin q\downarrow$
  $\langle 2\rangle 3$. $q \leq s < r$
□

Proposition 10.3.7. *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 10.3.8. *Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound.*

PROOF:
$\langle 1 \rangle 1$. LET: A be a bounded nonempty subset of $\mathbb{R}$.
$\langle 1 \rangle 2$. $\bigcup A$ is a Dedekind cut.
  $\langle 2 \rangle 1$. $\bigcup A \neq \emptyset$
    $\langle 3 \rangle 1$. PICK$x \in A$
    $\langle 3 \rangle 2$. PICK $q \in x$
    $\langle 3 \rangle 3$. $q \in \bigcup A$
  $\langle 2 \rangle 2$. $\bigcup A \neq \mathbb{Q}$
    $\langle 3 \rangle 1$. PICK an upper bound u for A
    $\langle 3 \rangle 2$. PICK $q \notin u$
      PROVE: $q \notin \bigcup A$
    $\langle 3 \rangle 3$. ASSUME: for a contradiction $q \in \bigcup A$
    $\langle 3 \rangle 4$. PICK $x \in A$ such that $q \in x$
    $\langle 3 \rangle 5$. $x \leq u$
    $\langle 3 \rangle 6$. $q \in u$
    $\langle 3 \rangle 7$. Q.E.D.
      PROOF: This is a contradiction.
  $\langle 2 \rangle 3$. $\bigcup A$ is closed downwards.
    $\langle 3 \rangle 1$. LET: $q \in \bigcup A$ and $r < q$
    $\langle 3 \rangle 2$. PICK $x \in A$ such that $q \in x$
    $\langle 3 \rangle 3$. $r \in x$
    $\langle 3 \rangle 4$. $r \in \bigcup A$
  $\langle 2 \rangle 4$. $\bigcup A$ has no greatest element.
    $\langle 3 \rangle 1$. LET: $q \in \bigcup A$
    $\langle 3 \rangle 2$. PICK $x \in A$ such that $q \in x$
    $\langle 3 \rangle 3$. PICK $r \in x$ such that $q < r$
    $\langle 3 \rangle 4$. $r \in \bigcup A$
$\langle 1 \rangle 3$. $\bigcup A$ is an upper bound for A.
  PROOF: For all $x \in A$ we have $x \subseteq \bigcup A$.
$\langle 1 \rangle 4$. 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 10.3.9 (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:
$\langle 1 \rangle 1$. 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 $r < r'$
$\langle 2 \rangle 3.$ $q + r < q' + r' \in x + y$
$\square$

Proposition 10.3.10. *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 $s - r < t < q$
$\langle 2 \rangle 4.$ $s - t < r$
$\langle 2 \rangle 5.$ $s = t + (s - t) \in q \downarrow + r \downarrow$
$\square$

Proposition 10.3.11. *Addition is associative.*

PROOF:
$$\begin{aligned} x + (y + z) &= \{q + r \mid q \in x, r \in y + z\} \\ &= \{q + s_1 + s_2 \mid q \in x, s_1 \in y, s_2 \in z\} \\ &= \{r + s_2 \mid r \in x + y, s_2 \in z\} \\ &= (x + y) + z \end{aligned}$$
$\square$

Proposition 10.3.12. *Addition is commutative.*

PROOF:
$$\begin{aligned} x + y &= \{q + r \mid q \in x, r \in y\} \\ &= \{r + q \mid r \in y, q \in x\} \\ &= y + x \end{aligned}$$
∎

Proposition 10.3.13. *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.
$\langle 2 \rangle 3.$ $q - r < 0$
$\langle 2 \rangle 4.$ $q = r + (q - r) \in x + 0$
∎

Definition 10.3.14. For $x \in \mathbb{R}$, define $-x := \{q \in \mathbb{Q} \mid \exists r > q. -r \notin x\}$.

Proposition 10.3.15. *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 $q < s < r$
$\langle 2 \rangle 4.$ $s \in -x$
∎

Lemma 10.3.16. *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:
$\langle 1\rangle 1$. PICK $q_0 \in x$
$\langle 1\rangle 2$. There exists $k \in \mathbb{N}$ such that $q_0 + kp \notin x$
$\langle 2\rangle 1$. PICK $q_1 \notin x$
$\langle 2\rangle 2$. PICK $k \in \mathbb{N}$ such that $q_1 - q_0 < pk$
PROOF: Proposition 10.2.11.
$\langle 2\rangle 3$. $q_1 < q_0 + kp$
$\langle 2\rangle 4$. $q_0 + kp \notin x$
$\langle 1\rangle 3$. LET: k be the least natural number such that $q_0 + kp \notin x$
$\langle 1\rangle 4$. $k \neq 0$
PROOF: $\langle 1\rangle 1$
$\langle 1\rangle 5$. LET: $q = q_0 + (k-1)p$
$\langle 1\rangle 6$. $q \in x$ and $q + p \notin x$.
□

Proposition 10.3.17. *For every real x we have $x + (-x) = 0$.*

PROOF:
$\langle 1\rangle 1$. LET: x be a real number.
$\langle 1\rangle 2$. $x + (-x) \subseteq 0$
$\langle 2\rangle 1$. LET: $q_1 \in x$ and $q_2 \in -x$
$\langle 2\rangle 2$. PICK $r > q_2$ such that $-r \notin x$
$\langle 2\rangle 3$. $q_1 < -r$
$\langle 2\rangle 4$. $r < -q_1$
$\langle 2\rangle 5$. $q_2 < -q_1$
$\langle 2\rangle 6$. $q_1 + q_2 < 0$
$\langle 1\rangle 3$. $0 \subseteq x + (-x)$
$\langle 2\rangle 1$. LET: $p < 0$
$\langle 2\rangle 2$. $0 < -p$
$\langle 2\rangle 3$. PICK $q \in x$ such that $q - p/2 \notin x$
PROOF: Lemma 10.3.16.
$\langle 2\rangle 4$. LET: $s = p/2 - q$
$\langle 2\rangle 5$. $-s \notin x$
$\langle 2\rangle 6$. $p - q < s$
$\langle 2\rangle 7$. $p - q \in -x$
$\langle 2\rangle 8$. $p \in x + (-x)$
□

Corollary 10.3.17.1. *The reals form an Abelian group under addition.*

Proposition 10.3.18. *For any reals x, y and z, we have $x < y$ if and only if $x + z < y + z$.*

PROOF:
$\langle 1\rangle 1$. $\forall x, y, z \in \mathbb{R}. x \leq y \Rightarrow x + z \leq y + z$
$\langle 2\rangle 1$. LET: $x, y, z \in \mathbb{R}$
$\langle 2\rangle 2$. ASSUME: $x \leq y$
$\langle 2\rangle 3$. 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 7.1.4.
$\langle 1\rangle 3.$ $\forall x, y, z \in \mathbb{R}. x < y \Rightarrow x + z < y + z$
$\langle 1\rangle 4.$ Q.E.D.
PROOF: Proposition 3.1.23.
□

Definition 10.3.19 (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 10.3.20 (Multiplication)**.** Define *multiplication* $\cdot$ on $\mathbb{R}$ as follows:

- If x and y are non-negative then
$$xy = 0 \cup \{rs \mid 0 \leq r \in x \wedge 0 \leq s \in y\} \ .$$
- 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 $r < q$

⟨2⟩2. CASE: $q \in 0$
PROOF: Then $r < q < 0$ so $r \in xy$
⟨2⟩3. CASE: $q = s_1 s_2$ where $0 \leq s_1 \in x$ and $0 \leq s_2 \in y$
⟨3⟩1. ASSUME: w.l.o.g. $0 \leq r$
⟨3⟩2. $0 < s_1$ and $0 < s_2$
⟨3⟩3. $r/s_2 < s_1$
⟨3⟩4. $r/s_2 \in x$
⟨3⟩5. $r = (r/s_2)s_2 \in xy$
⟨1⟩5. xy has no greatest element.
⟨2⟩1. LET: $q \in xy$
⟨2⟩2. CASE: $q \in 0$
PROOF: $q < q/2 \in 0$
⟨2⟩3. CASE: $q = rs$ where $0 \leq r \in x$ and $0 \leq s \in y$
⟨3⟩1. PICK r' and s' with $r < r' \in x$ and $s < s' \in y$
⟨3⟩2. $q < r's' \in xy$
□

Proposition 10.3.21. *Multiplication is commutative.*

PROOF: Immediate from definition. □

Proposition 10.3.22. *Multiplication is associative.*

PROOF:
⟨1⟩1. For non-negative reals x, y and z, we have $x(yz) = (xy)z$
PROOF: It computes to $0 \cup \{qrs \mid 0 \leq q \in x, 0 \leq r \in y, 0 \leq s \in z\}$.
⟨1⟩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 10.3.23. *Multiplication distributes over addition.*

PROOF:
⟨1⟩1. For all non-negative reals x, y and z, we have $x(y+z) = xy + xz$
⟨2⟩1. LET: x, y and z be non-negative reals.
⟨2⟩2. $x(y+z) \subseteq xy + xz$
⟨3⟩1. LET: $q \in x(y+z)$
⟨3⟩2. CASE: $q < 0$
PROOF: Then we have $q/2 \in xy$ and $q/2 \in xz$ so $q \in xy + xz$.
⟨3⟩3. CASE: $q = rs$ where $0 \leq r \in x$ and $0 \leq s \in y + z$
⟨4⟩1. PICK $s_1 \in y$ and $s_2 \in z$ such that $s = s_1 + s_2$
⟨4⟩2. $rs_1 \in xy$
PROOF: If $s_1 < 0$ then $rs_1 < 0$ so $rs_1 \in xy$. If $0 \leq s_1$ then we also have $rs_1 \in xy$.
⟨4⟩3. $rs_2 \in xz$
PROOF: Similar.
⟨4⟩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 $r = r_1r_2$ 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 $q + r = s_1s_2$

$\langle 4\rangle 5.$ $s_2 \in y + z$
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: $q = q_1q_2$ where $0 \leq q_1 \in x$ and $0 \leq q_2 \in y$ and $r < 0$
PROOF: Similar.

$\langle 3\rangle 5.$ CASE: $q = q_1q_2$ where $0 \leq q_1 \in x$ and $0 \leq q_2 \in y$ and $r = r_1r_2$ 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:

$$\begin{aligned} x(y + z) = -(-x)(y + z) &= -((-x)y + (-x)z) && (\langle 1\rangle 1) \\ &= -((-x)y) - ((-x)z) \\ &= xy + xz \end{aligned}$$

$\langle 1\rangle 3.$ 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:

$$\begin{aligned} xy + xz &= xy + x(-y + y + z) \\ &= -(x(-y)) + x(-y + y + z) \\ &= -(x(-y)) + x(-y) + x(y + z) && (\langle 1\rangle 1) \\ &= x(y + z) \end{aligned}$$

$\langle 2\rangle 3.$ 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:

$$\begin{aligned} xy + xz &= -(x(-y)) + xz \\ &= -(x(z - y - z)) + xz \\ &= -(xz + x(-y - z)) + xz && (\langle 1\rangle 1) \\ &= -xy - x(-y - z) + xz \\ &= -x(-y - z) \\ &= x(y + z) \end{aligned}$$

$\langle 1\rangle$4. For any non-negative real x and negative reals y and z, we have $x(y+z) = xy + xz$

PROOF:

$$\begin{aligned} x(y + z) &= -x(-y - z) \\ &= -(x(-y) + x(-z)) && (\langle 1\rangle 1) \\ &= -x(-y) - x(-z) \\ &= xy + xz \end{aligned}$$

$\langle 1\rangle$5. For any negative real x and reals y and z with one negative and one non-negative, we have $x(y + z) = xy + xz$

$\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:

$$\begin{aligned} x(y + z) &= -((-x)(y + z)) \\ &= -((-x)y + (-x)z) && (\langle 1\rangle 3) \\ &= -((-x)y) - ((-x)z) \\ &= (-x)(-y) - ((-x)z) \\ &= xy + xz \end{aligned}$$

$\langle 2\rangle$3. CASE: $y + z < 0$

PROOF:

$$\begin{aligned} x(y + z) &= (-x)(-y - z) \\ &= (-x)(-y) + (-x)(-z) && (\langle 1\rangle 3) \\ &= xy + xz \end{aligned}$$

$\langle 1\rangle$6. For any negative reals x, y and z, we have $x(y + z) = xy + xz$

PROOF:

$$\begin{aligned} x(y + z) &= (-x)(-y - z) \\ &= (-x)(-y) + (-x)(-z) && (\langle 1\rangle 1) \\ &= xy + xz \end{aligned}$$

$\square$

Proposition 10.3.24. *For any real x we have $x1 = x$.*

PROOF:

$\langle 1\rangle$1. CASE: $0 \leq x$

$\langle 2\rangle$1. $x1 \subseteq x$

$\langle 3\rangle$1. LET: $q \in x1$

$\langle 3\rangle 2$. CASE: $q < 0$

PROOF: Then $q \in x$ because $0 \leq x$.

$\langle 3\rangle 3$. $q = rs$ where $0 \leq r \in x$ and $0 \leq s < 1$

PROOF: Then $q < r$ so $q \in x$.

$\langle 2\rangle 2$. $x \subseteq x1$

$\langle 3\rangle 1$. LET: $q \in x$

$\langle 3\rangle 2$. ASSUME: w.l.o.g. $0 \leq q$

$\langle 3\rangle 3$. PICK r such that $q < r \in x$

$\langle 3\rangle 4$. $0 \leq q/r < 1$

$\langle 3\rangle 5$. $q = r(q/r) \in x1$

$\langle 1\rangle 2$. CASE: $x < 0$

PROOF:

$$\begin{aligned} x1 &= -((-x)1) \\ &= -(-x) && (\langle 1\rangle 1) \\ &= x \end{aligned}$$

□

Lemma 10.3.25. *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:

$\langle 1\rangle 1$. PICK $a_1 \in x$ such that if x has a rational supremum s then $a_1 > s - c$

$\langle 1\rangle 2$. There exists a natural number n such that $a_1 + nc$ is an upper bound for x.

$\langle 2\rangle 1$. PICK a non-least upper bound b_1 for x.

$\langle 2\rangle 2$. PICK a natural number n such that $nc > b_1 - a_1$

PROOF: Proposition 10.2.11.

$\langle 2\rangle 3$. $a_1 + nc > b_1$

$\langle 2\rangle 4$. $a_1 + nc$ is an upper bound for x.

$\langle 1\rangle 3$. LET: k be the least natural number such that $a_1 + kc$ is an upper bound for x.

$\langle 1\rangle 4$. $a_1 + (k-1)c \in x$

$\langle 1\rangle 5$. $a_1 + kc$ is not the supremum of x.

$\langle 2\rangle 1$. ASSUME: for a contradiction $a_1 + kc$ is the supremum of x.

$\langle 2\rangle 2$. $a_1 > a_1 + (k-1)c$

PROOF: $\langle 1\rangle 1$

$\langle 2\rangle 3$. Q.E.D.

PROOF: This is a contradiction.

$\langle 1\rangle 6$. LET: $a = a_1 + (k-1)c$

$\langle 1\rangle 7$. LET: $b = a_1 + kc$

$\langle 1\rangle 8$. $b - a = c$

□

Proposition 10.3.26. *For any non-zero real x, there exists a real y such that $xy = 1$.*

PROOF:

⟨1⟩1. CASE: $0 < x$
⟨2⟩1. LET: $y = \{q \in \mathbb{Q} \mid q \leq 0\} \cup \{u^{-1} \mid u \text{ is an upper bound for } x \text{ but not the supremum of } x\}$
⟨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 10.3.25.
⟨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

⟨3⟩10. $q/a \in y$
⟨3⟩11. $q \in xy$
⟨1⟩2. CASE: $x < 0$
⟨2⟩1. PICK y such that $(-x)y = 1$
PROOF: ⟨1⟩1
⟨2⟩2. $x(-y) = 1$
□

Proposition 10.3.27. *For real numbers x, y and z, if $0 < z$ then $x < y$ if and only if $xz < yz$.*

PROOF:
⟨1⟩1. For any real numbers x, y and z, if $0 < z$ and $x < y$ then $xz < yz$
⟨2⟩1. LET: x, y and z be real numbers.
⟨2⟩2. ASSUME: $0 < z$ and $x < y$.
⟨2⟩3. $y = x + (y - x)$
⟨2⟩4. $y - x > 0$
⟨2⟩5. $(y - x)z > 0$
⟨2⟩6. $yz > xz$
PROOF:

$$\begin{aligned} yz &= (x + (y - x))z \\ &= xz + (y - x)z \\ &> xz \end{aligned}$$

⟨1⟩2. For any real numbers x, y and z, if $0 < z$ and $xz < yz$ then $x < y$
PROOF: Proposition 3.1.23.
□

Corollary 10.3.27.1. *The real numbers form a complete ordered field.*

Proposition 10.3.28.

$$(0, 1) \approx \mathbb{R}$$

PROOF: The function $f(x) = (2x - 1)/(x - x^2)$ is a bijection between $(0, 1)$ and $\mathbb{R}$. □

Proposition 10.3.29.

$$\mathbb{R} \not\approx \mathbb{N}$$

PROOF:
⟨1⟩1. ASSUME: for a contradiction $f : \mathbb{N} \approx \mathbb{R}$
⟨1⟩2. LET: z be the real number with integer part 0 whose $n+1$st decimal place is 7 unless the $n + 1$st decimal place of $f(n)$ is 7, in which case it is 6.
⟨1⟩3. $z \neq f(n)$ for all n.
⟨1⟩4. Q.E.D.
PROOF: This is a contradiction.
□

Chapter 11

Complex Analysis

Definition 11.0.1. 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 11.0.2. *If* $(x_n), (y_n) \in l^p$ *then* $(x_n + y_n) \in l^p$.

PROOF:
⟨1⟩1. LET: $(x_n), (y_n) \in l^p$
⟨1⟩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:
  ⟨2⟩1. For all $n \in \mathbb{N}$ we have $|x_n + y_n|^p \leq 2^p (|x_n|^p + |y_n|^p)$.
    PROOF:

$$\begin{aligned} |x_n + y_n|^p &\leq (|x_n| + |y_n|)^p && \text{(Triangle Inequality)} \\ &\leq (2 \max(|x_n|, |y_n|))^p \\ &\leq 2^p (|x_n|^p + |y_n|^p) \end{aligned}$$

□

Theorem 11.0.3 (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:
⟨1⟩1. ASSUME: w.l.o.g. neither (x_n) nor (y_n) are all zero.
⟨1⟩2. For $0 \leq x \leq 1$ we have

$$x^{1/p} \leq \frac{1}{p} x + \frac{1}{q} \ .$$

  ⟨2⟩1. LET: $f(x) = x/p + 1/q - x^{1/p}$
  ⟨2⟩2. $f'(x) = 1/p(1 - x^{(1-p)/p})$
  ⟨2⟩3. $f'(x) \geq 0$ for all $x \in [0, 1]$
  ⟨2⟩4. f is a monotonically decreasing function on $[0, 1]$

⟨2⟩5. $f(0) = 1/q$
⟨2⟩6. $f(1) = 0$
⟨2⟩7. $f(x) \geq 0$ for all $x \in [0,1]$
⟨1⟩3. For any $a, b \geq 0$ we have

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q} \quad .$$

⟨2⟩1. CASE: $a^p \leq b^q$
⟨3⟩1. $ab^{-q/p} \leq \frac{1}{p}\frac{a^p}{b^q} + \frac{1}{q}$
PROOF: Substituting $x = a^p/b^q$ in ⟨1⟩2.
⟨3⟩2. $ab^{1-q} \leq \frac{1}{p}\frac{a^p}{b^q} + \frac{1}{q}$
PROOF: From ⟨3⟩1 since $1 - q = -q/p$.
⟨3⟩3. $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$
PROOF: Multiplying ⟨3⟩2 by b^q.
⟨2⟩2. CASE: $b^q \leq a^p$
PROOF: Similar.
⟨1⟩4. For any integers $1 \leq j \leq n$, we have

$$\frac{|x_j|}{\left(\sum_{k=1}^n |x_k|^p\right)^{1/p}} \frac{|y_j|}{\left(\sum_{k=1}^n |y_k|^q\right)^{1/q}} \leq \frac{1}{p}\frac{|x_j|^p}{\sum_{k=1}^n |x_k|^p} + \frac{1}{q}\frac{|y_j|^q}{\sum_{k=1}^n |y_k|^q}$$

PROOF: From ⟨1⟩3 substituting

$$a = \frac{|x_j|}{\left(\sum_{k=1}^n |x_k|^p\right)^{1/p}} \text{ and } b = \frac{|y_j|}{\left(\sum_{k=1}^n |y_k|^q\right)^{1/q}}$$

⟨1⟩5. For any positive integer n we have

$$\frac{\sum_{k=1}^n |x_k||y_k|}{\left(\sum_{k=1}^n |x_k|^p\right)^{1/p} \left(\sum_{k=1}^n |y_k|^q\right)^{1/q}} \leq 1$$

PROOF:

$$\begin{aligned} \frac{\sum_{j=1}^n |x_j||y_j|}{\left(\sum_{k=1}^n |x_k|^p\right)^{1/p} \left(\sum_{k=1}^n |y_k|^q\right)^{1/q}} &\leq \frac{1}{p} + \frac{1}{q} \quad \text{(Summing ⟨1⟩4 from } j = 1 \text{ to } n) \\ &= 1 \end{aligned}$$

⟨1⟩6.

$$\sum_n |x_n y_n| \leq \left(\sum_n |x_n|^p\right)^{1/p} \left(\sum_n |y_n|^q\right)^{1/q}$$

PROOF: Taking the limit $n \to \infty$ in ⟨1⟩5.
□

Theorem 11.0.4 (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:
⟨1⟩1. CASE: $p = 1$
PROOF: This is just the Triangle Inequality.
⟨1⟩2. CASE: $p > 1$
⟨2⟩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:
$$\begin{aligned} \sum_{n=1}^{\infty} |x_n + y_n|^{(p-1)q} &= \sum_{n=1}^{\infty} |x_n + y_n|^p && (\langle 2 \rangle 2) \\ &< \infty && (\text{Proposition 11.0.2}) \end{aligned}$$

⟨3⟩2. Q.E.D.
PROOF:
$$\begin{aligned} \sum_{n=1}^{\infty} |x_n + y_n|^p &= \sum_{n=1}^{\infty} |x_n + y_n||x_n + y_n|^{p-1} \\ &\leq \sum_{n=1}^{\infty} |x_n||x_n + y_n|^{p-1} + \sum_{n=1}^{\infty} |y_n||x_n + y_n|^{p-1} \\ &\leq \left(\sum_{n=1}^{\infty} |x_n|^p \right)^{1/p} \left(\sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \\ &\quad + \left(\sum_{n=1}^{\infty} |y_n|^p \right)^{1/p} \left(\sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} && (\text{Hölder's Inequality}, \langle 2 \rangle 2) \end{aligned}$$

⟨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 12

Vector Spaces

12.1 Vector Spaces

Definition 12.1.1 (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 12.1.2. *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 $x, y \in \{0\}$. □

Proposition 12.1.3. *The set $\mathbb{R}$ is a real vector space under real addition and real multiplication.*

PROOF: TODO — after we have proved these facts about $\mathbb{R}$. □

Proposition 12.1.4. *The set $\mathbb{C}$ is a real vector space under complex addition and complex multiplication.*

PROOF: TODO

Proposition 12.1.5. *The set $\mathbb{C}$ is a complex vector space under complex addition and complex multiplication.*

PROOF: TODO

Proposition 12.1.6. *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*

$$\begin{aligned} \{x_i\}_{i \in I} + \{y_i\}_{i \in I} &= \{x_i + y_i\}_{i \in I} \\ \alpha\{x_i\}_{i \in I} &= \{\alpha x_i\}_{i \in I} \end{aligned}$$

PROOF: Each axiom follows from the corresponding axiom in V_i. □□

Corollary 12.1.6.1. *Let V be a vector space over K. For any set I, we have V^I is a vector space over K.*

Corollary 12.1.6.2. *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*

$$\begin{aligned} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n) \\ \lambda(x_1, \ldots, x_n) &= (\lambda x_1, \ldots, \lambda x_n) \end{aligned}$$

Proposition 12.1.7. *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. $u + 0 = u$

$$\begin{aligned} u + 0 &= v + u' + 0 && (\langle 3 \rangle 2) \\ &= v + u' && (\langle 2 \rangle 2) \\ &= u && (\langle 3 \rangle 2) \end{aligned}$$

⟨1⟩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 $0 = 0'$.
⟨2⟩1. LET: $0, 0' \in V$
⟨2⟩2. ASSUME: $\forall v \in V.v + 0 = v$
⟨2⟩3. ASSUME: $\forall v \in V.v + 0' = v$
⟨2⟩4. $0 = 0'$

$$\begin{aligned} 0 &= 0 + 0' && (\langle 2\rangle 2) \\ &= 0' && (\langle 2\rangle 3) \end{aligned}$$

□

Proposition 12.1.8. *Let V be a vector space. For any $v \in V$, there exists a unique $-v \in V$ such that $v + (-v) = 0$.*

PROOF:
⟨1⟩1. LET: $v \in V$
⟨1⟩2. There exists $-v \in V$ such that $v + (-v) = u$
PROOF: Axiom 3.
⟨1⟩3. If $v + x = 0$ and $v + y = 0$ then $x = y$
⟨2⟩1. ASSUME: $v + x = 0$
⟨2⟩2. ASSUME: $v + y = 0$
⟨2⟩3. $x = y$
PROOF:

$$\begin{aligned} x &= x + 0 && \text{(Proposition 12.1.7)} \\ &= x + v + y && (\langle 2\rangle 2) \\ &= 0 + y && (\langle 2\rangle 1) \\ &= y && \text{(Proposition 12.1.7)} \end{aligned}$$

□

Proposition 12.1.9. *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:
⟨1⟩1. LET: $u, v \in V$
⟨1⟩2. $v + (u + (-v)) = u$
PROOF:

$$\begin{aligned} v + u + (-v) &= u + 0 && \text{(Proposition 12.1.8)} \\ &= u && \text{(Proposition 12.1.7)} \end{aligned}$$

⟨1⟩3. For all $x \in V$, if $v + x = u$ then $x = u + (-v)$.
⟨2⟩1. LET: $x \in V$
⟨2⟩2. ASSUME: $v + x = u$
⟨2⟩3. $x = u + (-v)$
PROOF:

$$\begin{aligned} u + (-v) &= v + x + (-v) && (\langle 2\rangle 2) \\ &= x + 0 && \text{(Proposition 12.1.8)} \\ &= x && \text{(Proposition 12.1.7)} \end{aligned}$$

∎

Proposition 12.1.10. *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:

$$\begin{aligned} v &= v + 0 && \text{(Proposition 12.1.7)} \\ &= v + u + (-u) && \text{(Proposition 12.1.8)} \\ &= w + u + (-u) && (\langle 1\rangle 1) \\ &= w + 0 && \text{(Proposition 12.1.8)} \\ &= w && \text{(Proposition 12.1.7)} \end{aligned}$$

Proposition 12.1.11. *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:

$$\begin{aligned} \lambda 0 + \lambda 0 &= \lambda(0 + 0) && \text{(Axiom 6)} \\ &= \lambda 0 && \text{(Proposition 12.1.7)} \end{aligned}$$

⟨1⟩2. $\lambda 0 = 0$
PROOF: Proposition 12.1.10.
∎

Proposition 12.1.12. *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 12.1.13. *Let V be a vector space over K. For all $v \in V$ we have $0v = 0$.*

PROOF:
⟨1⟩1. $0v + 0 = 0v + 0v$

$$
\begin{aligned}
0v + 0 &= 0v && \text{(Proposition 12.1.7)} \\
&= (0+0)v \\
&= 0v + 0v && \text{(Axiom 5)}
\end{aligned}
$$

$\langle 1 \rangle 2.$ $0v = 0$

Proof: Proposition 12.1.10, $\langle 1 \rangle 1$.

□

Proposition 12.1.14. *Let V be a vector space over K. Let $v \in V$. Then $(-1)v = -v$.*

Proof:

$\langle 1 \rangle 1.$ $v + (-1)v = 0$

Proof:

$$
\begin{aligned}
v + (-1)v &= 1v + (-1)v && \text{(Axiom 7)} \\
&= (1 + (-1))v && \text{(Axiom 5)} \\
&= 0v \\
&= 0 && \text{(Proposition 12.1.13)}
\end{aligned}
$$

$\langle 1 \rangle 2.$ Q.E.D.

Proof: Proposition 12.1.8.

□

12.2 Subspaces

Definition 12.2.1 (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 12.2.2. *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 12.2.3. *Every vector space is a subspace of itself.*

Proof: Trivial. □

Proposition 12.2.4. *Let Ω 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 12.2.5. *Let Ω 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 12.2.6. *Let Ω 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 12.2.7. *Let Ω 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 12.2.8. *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 12.2.9. *Let V be a vector space over K . The intersection of a set of subspaces of V is a subspace of V.*

Proof:
⟨1⟩1. Let: $\mathcal{U}$ be a set of subspaces of V.
⟨1⟩2. Let: $u, v \in \bigcap \mathcal{U}$ and $\lambda, \mu \in K$
⟨1⟩3. $\lambda u + \mu v \in \bigcap \mathcal{U}$
 ⟨2⟩1. Let: $U \in \mathcal{U}$
 ⟨2⟩2. $u, v \in U$
  Proof: ⟨1⟩2, ⟨2⟩1.
 ⟨2⟩3. $\lambda u + \beta v \in U$
  Proof: ⟨1⟩1, ⟨1⟩2, ⟨2⟩1, ⟨2⟩2.
□

Proposition 12.2.10. *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 12.2.11. *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 12.2.12. *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 11.0.2, and it is easy to see that it is closed under scalar multiplication. □

12.3 Linear Independence and Bases

Definition 12.3.1 (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 $v_1, \ldots, v_n$ iff there exist scalars $\lambda_1, \ldots, \lambda_n \in K$ such that

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \ .$$

Definition 12.3.2 (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 12.3.3 (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 12.3.4. *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

$$\begin{aligned} &\alpha(\lambda_1 u_1 + \cdots + \lambda_m u_m) + \beta(\mu_1 v_1 + \cdots + \mu_n v_n) \\ &= \alpha\lambda_1 u_1 + \cdots + \alpha\lambda_m u_m + \beta\mu_1 v_1 + \cdots + \beta\mu_n v_n \\ &\in \operatorname{span} A \end{aligned}$$

□

Definition 12.3.5 (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 12.3.6 (Finite Dimensional)**.** A vector space is *finite dimensional* iff there exists a finite basis; otherwise it is *infinite dimensional*.

Proposition 12.3.7. *In a finite dimensional space, any two bases have the same size.*

TODO

Definition 12.3.8 (Dimension)**.** The *dimension* of a finite dimensional vector space V, $\dim V$, is the number of vectors in any basis.

Proposition 12.3.9. *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. □

Proposition 12.3.10. *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. □

Proposition 12.3.11. *Let Ω 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 12.3.12. *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. □

12.4 Linear Mappings

Definition 12.4.1 (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 12.4.2 (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 12.4.3. *Let U and V be vector spaces over K. The set of linear mappings from U to V is a subspace of V^U.*

12.5 Eigenvalues and Eigenvectors

Definition 12.5.1 (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* λ iff $A(v) = \lambda v$.

Chapter 13

Normed Spaces

Definition 13.0.1 (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*) $\|u + v\| \leq \|u\| + \|v\|$

A *normed space* over K is a pair $(V, \| \ \|)$ where V is a vector space over K and $\| \ \|$ is a norm on V.

Proposition 13.0.2. *In a normed space,* $\|0\| = 0$*.*

Proof: $\|0\| = |0|\|0\| = 0$ by Axiom 2. □

Proposition 13.0.3. *Let V be a normed vector space over K. For all $v \in V$ we have $\|v\| \geq 0$.*

Proof:

$$\begin{aligned}
0 &= \|0\| && \text{(Proposition 13.0.2)} \\
&= \|v - v\| \\
&\leq \|v\| + \|-v\| && \text{(Triangle Inequality)} \\
&= 2\|v\| && \text{(Axiom 2)}
\end{aligned}$$

Proposition 13.0.4. *Let V be a normed space. Let $u, v \in V$. Then*

$$|\|u\| - \|v\|| \leq \|u - v\| \ .$$

PROOF:

$$\begin{aligned}
\|u\| &\leq \|u-v\| + \|v\| && \text{(Triangle Inequality)} \\
\therefore \|u\| - \|v\| &\leq \|u-v\| \\
\|v\| &\leq \|v-u\| + \|u\| && \text{(Triangle Inequality)} \\
&= \|u-v\| + \|u\| && \text{(Axiom 2)} \\
\therefore \|v\| - \|u\| &\leq \|u-v\|
\end{aligned}$$

Definition 13.0.5 (Euclidean Norm)**.** The *Euclidean norm* on K^n is defined by

$$\|(x_1, \ldots, x_n)\| = \sqrt{|x_1|^2 + \cdots + |x_n|^2} \enspace .$$

Proposition 13.0.6. *The Euclidean norm on K^n is a norm.*

PROOF:
⟨1⟩1. If $\|\vec{x}\| = 0$ then $\vec{x} = \vec{0}$
PROOF: If $\sqrt{|x_1|^2 + \cdots + |x_n|^2} = 0$ then $x_1 = \cdots = x_n = 0$.
⟨1⟩2. $\|\lambda\vec{x}\| = |\lambda|\|\vec{x}\|$
PROOF:

$$\begin{aligned}
\|\lambda\vec{x}\| & \sqrt{|\lambda x_1|^2 + \cdots + |\lambda x_n|^2} \\
&= \sqrt{|\lambda|^2|x_1|^2 + \cdots + |\lambda|^2|x_n|^2} \\
&= |\lambda|\sqrt{|x_1|^2 + \cdots + |x_n|^2} \\
&= |\lambda|\|\vec{x}\|
\end{aligned}$$

⟨1⟩3. $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$
PROOF:

$$\begin{aligned}
\|\vec{u} + \vec{v}\|^2 &= |u_1 + v_1|^2 + \cdots + |u_n + v_n|^2 \\
&= |u_1|^2 + \cdots + |u_n|^2 + |v_1|^2 + \cdots + |v_n|^2 \\
&+ 2|u_1||v_1| + \cdots + 2|u_n||v_n| \\
&\leq \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2|u_1v_1 + \cdots + u_nv_n| \\
&\leq \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2\|\vec{u}\|\|\vec{v}\| && \text{(Cauchy-Schwarz)} \\
&= (\|\vec{u}\| + \|\vec{v}\|)^2
\end{aligned}$$

□

Corollary 13.0.6.1. *The absolute value function $|\ |$ is a norm on K.*

Proposition 13.0.7. *The function $\|\vec{x}\| = |x_1| + \cdots + |x_n|$ is a norm on $\mathbb{C}^n$.*

PROOF:
⟨1⟩1. If $\|\vec{x}\| = 0$ then $\vec{x} = \vec{0}$
PROOF: If $|x_1| + \cdots + |x_n| = 0$ then $x_1 = \cdots = x_n = 0$.
⟨1⟩2. $\|\lambda\vec{x}\| = |\lambda|\|\vec{x}\|$

PROOF:

$$\|\lambda\vec{x}\||\lambda x_1| + \cdots + |\lambda x_n|$$

$$\begin{aligned} &= |\lambda|(|x_1| + \cdots + |x_n|) \\ &= |\lambda|\|\vec{x}\| \end{aligned}$$

⟨1⟩3. $\|\vec{u}+\vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$
PROOF:

$$\begin{aligned} \|\vec{u}+\vec{v}\|^2 &= |u_1 + v_1| + \cdots + |u_n + v_n| \\ &\leq |u_1| + |v_1| + \cdots + |u_n| + |v_n| \\ &= \|\vec{u}\| + \|\vec{v}\| \end{aligned}$$

□

Proposition 13.0.8. *The function* $\|\vec{x}\| = \max(|x_1|, \ldots, |x_n|)$ *is a norm on* $\mathbb{C}^n$*.*

PROOF:
⟨1⟩1. If $\|\vec{x}\| = 0$ then $\vec{x} = \vec{0}$
PROOF: If $\max(|x_1|, \ldots, |x|n|) = 0$ then $x_1 = \cdots = x_n = 0$.
⟨1⟩2. $\|\lambda\vec{x}\| = |\lambda|\|\vec{x}\|$
PROOF:

$$\begin{aligned} \|\lambda\vec{x}\| &= \max(|\lambda x_1|, \ldots, |\lambda x_n|) \\ &= |\lambda| \max(|x_1|, \ldots, |x_n|) \\ &= |\lambda|\|\vec{x}\| \end{aligned}$$

⟨1⟩3. $\|\vec{u}+\vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$
PROOF:

$$\begin{aligned} \|\vec{u}+\vec{v}\| &= \max(|u_1 + v_1|, \ldots, |u_n + v_n|) \\ &\leq \max(|u_1| + |v_1|, \ldots, |u_n| + |v_n|) \\ &\leq \max(|u_1|, \ldots, |u_n|) + \max(|v_1|, \ldots, |v_n|) \end{aligned}$$

□

Definition 13.0.9 (Uniform Convergence Norm)**.** Let Ω 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 13.0.10. *Let* Ω *be a closed bounded subset of* $\mathbb{R}^n$*. The uniform convergence norm is a norm on* $\mathcal{C}(\Omega)$*.*

PROOF:
⟨1⟩1. If $\|f\| = 0$ then $f = 0$
PROOF: If $\max_x |f(x)| = 0$ then $f(x) = 0$ for all x.
⟨1⟩2. $\|\lambda f\| = |\lambda|\|f\|$
PROOF:

$$\begin{aligned} \|\lambda f\| &= \max_x |\lambda f(x)| \\ &= |\lambda| \max_x |f(x)| \\ &= |\lambda|\|f\| \end{aligned}$$

⟨1⟩3. $\|f+g\| \leq \|f\| + \|g\|$
PROOF:
$$\begin{aligned}\|f+g\| &= \max_x |f(x)+g(x)| \\ &\leq \max_x (|f(x)| + |g(x)|) \\ &\leq \max_x |f(x)| + \max_x |g(x)| \\ &= \|f\| + \|g\|\end{aligned}$$
□

Proposition 13.0.11. *Let $p \geq 1$. The function $\|(z_n)\| = \left(\sum_{n=1}^{\infty} |z_n|^p\right)^{1/p}$ is a norm on l^p.*

PROOF:
⟨1⟩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.
⟨1⟩2. $\|(\lambda z_n)\| = |\lambda| \|(z_n)\|$
PROOF:
$$\begin{aligned}\|(\lambda z_n)\| &= \left(\sum_n |\lambda z_n|^p\right)^{1/p} \\ &= |\lambda| \left(\sum_n |z_n|^p\right)^{1/p} \\ &= |\lambda| \, |(z_n)|\end{aligned}$$
⟨1⟩3. The triangle inequality holds.
PROOF: This is Minkowski's Inequality. □

Proposition 13.0.12. *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. □

Proposition 13.0.13. *Let V be a normed space over K. Let $x_1, \ldots, x_n$ 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*
$$\|\alpha_1 x_1 + \cdots + \alpha_n x_n\| \geq c(|\alpha_1| + \cdots + |\alpha_n|) \ .$$

PROOF:
⟨1⟩1. Define $f : K^n \to \mathbb{R}$ by
$$f(\alpha_1, \ldots, \alpha_n) = \|\alpha_1 x_1 + \cdots + \alpha_n x_n\|$$
⟨1⟩2. f is continuous.
⟨2⟩1. LET: $(\alpha_1, \ldots, \alpha_n) \in K^n$ and $\epsilon > 0$
⟨2⟩2. LET: $\delta = \epsilon / (\|x_1\| + \cdots + \|x_n\|)$
PROOF: $x_1, \ldots, x_n$ are not all zero because they are linearly independent.
⟨2⟩3. LET: $(\beta_1, \ldots, \beta_n)$ with $|\alpha_i - \beta_i| < \delta$ for all i

⟨2⟩4. $\|(\alpha_1 x_1 + \cdots + \alpha_n x_n) - (\beta_1 x_1 + \beta_n x_n)\| < \epsilon$
PROOF:

$$\begin{aligned}
&\|(\alpha_1 x_1 + \cdots + \alpha_n x_n) - (\beta_1 x_1 + \beta_n x_n)\| \\
\leq &|\alpha_1 - \beta_1|\|x_1\| + \cdots + |\alpha_n - \beta_n|\|x_n\| && \text{(Axioms 2 and 3)} \\
< &\delta(\|x_1\| + \cdots + \|x_n\|) && (\langle 2\rangle 3) \\
= &\epsilon && (\langle 2\rangle 2)
\end{aligned}$$

⟨1⟩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.
⟨1⟩4. Let $c = f(\beta_1, \ldots, \beta_n)$
⟨1⟩5. $c > 0$
PROOF: Linear independence.
⟨1⟩6. LET: $\alpha_1, \ldots, \alpha_n \in K$
⟨1⟩7. $\|\alpha_1 x_1 + \cdots + \alpha_n x_n\| \geq c(|\alpha_1| + \cdots + |\alpha_n|)$
⟨2⟩1. ASSUME: w.l.o.g. $\alpha_1 \ \ldots, \alpha_n$ are not all zero.
⟨2⟩2. LET: $\beta_i = \alpha_i/(|\alpha_1| + \cdots + |\alpha_n|)$ for $i = 1, \ldots, n$
⟨2⟩3. $|\beta_1| + \cdots + |\beta_n| = 1$
⟨2⟩4. $f(\beta_1, \ldots, \beta_n) \geq c$
⟨2⟩5. Q.E.D.
PROOF: Multiply both sides by $|\alpha_1| + \cdots + |\alpha_n|$.
□

Proposition 13.0.14. *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:
⟨1⟩1. For all $x, y \in V$ we have $d(x, y) \geq 0$
PROOF: Proposition 13.0.3.
⟨1⟩2. For all $x, y \in V$ we have $d(x, y) = 0$ iff $x = y$
⟨2⟩1. If $d(x, y) = 0$ then $x = y$
PROOF: Axiom 1.
⟨2⟩2. If $x = y$ then $d(x, y) = 0$
PROOF: Proposition 13.0.2.
⟨1⟩3. $\forall x, y \in V. d(x, y) = d(y, x)$
PROOF: By Axiom 2.
⟨1⟩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.

13.1 Convergence

Proposition 13.1.1. *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 13.1.2. *In a normed space, a sequence has at most one limit.*

PROOF:
⟨1⟩1. LET: V be a vector space over K.
⟨1⟩2. ASSUME: $x_n \to l$ and $x_n \to m$ as $n \to \infty$.
⟨1⟩3. ASSUME: for a contradiction $l \neq m$
⟨1⟩4. LET: $\epsilon = \|l - m\|/2$
⟨1⟩5. PICK N such that $\forall n \geq N. \|x_n - l\| < \epsilon$ and $\forall n \geq N. \|x_n - m\| < \epsilon$
PROOF: ⟨1⟩2, ⟨1⟩4
⟨1⟩6. $\|l - m\| < \|l - m\|$
PROOF:

$$\begin{aligned} \|l - m\| &\leq \|x_N - l\| + \|x_N - m\| && \text{(Triangle Inequality)} \\ &< 2\epsilon && (\langle 1\rangle 5) \\ &= \|l - m\| && (\langle 1\rangle 4 \end{aligned}$$

⟨1⟩7. Q.E.D.
PROOF: This is a contradiction.
□

Definition 13.1.3 (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 13.1.4. *Every convergent sequence is bounded.*

PROOF:
⟨1⟩1. LET: $x_n \to l$ as $n \to \infty$
⟨1⟩2. PICK N such that $\forall n \geq N. \|x_n - l\| < 1$
⟨1⟩3. LET: $B = \max(\|x_1\|, \|x_2\|, \ldots, \|x_{N-1}\|, \|l\| + 1)$
⟨1⟩4. LET: $n \in \mathbb{N}$
⟨1⟩5. $\|x_n\| \leq B$
⟨2⟩1. CASE: $n < N$
PROOF: $\|x_n\| \leq B$ from ⟨1⟩3.
⟨2⟩2. CASE: $n \geq N$
PROOF:

$$\begin{aligned} \|x_n\| &\leq \|l\| + \|x_n - l\| && \text{(Triangle Inequality)} \\ &< \|l\| + 1 && (\langle 1\rangle 2) \\ &\leq B && (\langle 1\rangle 3) \end{aligned}$$

□

Proposition 13.1.5. *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:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: $x_n \to l$ as $n \to \infty$
⟨1⟩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:

$$\begin{aligned} \|\lambda_n x_n - \lambda l\| &\leq \|\lambda_n x_n - \lambda x_n\| + \|\lambda x_n - \lambda l\| && \text{(Triangle Inequality)} \\ &= |\lambda_n - \lambda|\|x_n\| + |\lambda|\|x_n - l\| && \text{(Axiom 2)} \\ &< \sqrt{\epsilon/2}\sqrt{\epsilon/2} + |\lambda|\epsilon/2|\lambda| && (\langle 1\rangle 5) \\ &= \epsilon \end{aligned}$$

$\square$

Proposition 13.1.6. *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:

$$\begin{aligned} \|(x_n + y_n) - (l + m)\| &\leq \|x_n - l\| + \|y_n - m\| && \text{(Triangle Inequality)} \\ &< \epsilon/2 + \epsilon/2 && (\langle 1\rangle 2) \\ &= \epsilon \end{aligned}$$

$\square$

Definition 13.1.7 (Uniform Convergence)**.** Let Ω 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 13.1.8. *Let Ω 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:

$$\begin{aligned} & (f_n) \text{ converges to } f \text{ under the uniform convergence norm} \\ \Leftrightarrow & \forall \epsilon > 0 . \exists N . \forall n \geq N . \|f_n - f\| < \epsilon \\ \Leftrightarrow & \forall \epsilon > 0 . \exists N . \forall n \geq N . \forall x \in X . |f_n(x) - f(x)| < \epsilon \end{aligned}$$

$\square$

Definition 13.1.9 (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 13.1.10. *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

$$g_n(t) = \begin{cases} 2^n t & \text{if } 0 \leq t \leq 2^{-n} \\ 2 - 2^n t & \text{if } 2^{-n} \leq t \leq 2^{1-n} \\ 0 & \text{if } 2^{1-n} \leq t \leq 1 \end{cases}$$

⟨1⟩3. For all n, $\|g_n\| \neq 0$
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 13.1.11 (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 13.1.12. *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 α and β such that, for all $x \in E$,*

$$\alpha \|x\|_1 \leq \|x\|_2 \leq \beta \|x\|_1 \ .$$

PROOF:
⟨1⟩1. If $\| \|_1$ and $\| \|_2$ are equivalent then there exist positive real numbers α and β such that, for all $x \in E$, $\alpha\|x\|_1 \leq \|x\|_2 \leq \beta\|x\|_1$.
⟨2⟩1. ASSUME: $\| \|_1$ and $\| \|_2$ are equivalent.
⟨2⟩2. There exists $\alpha > 0$ such that, for all $x \in E$, we have $\alpha\|x\|_1 \leq \|x\|_2$
⟨3⟩1. ASSUME: for a contradiction there is no $\alpha > 0$ such that, for all $x \in E$, we have $\alpha\|x\|_1 \leq \|x\|_2$.
⟨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 $\|x\|_2 \leq \beta\|x\|_1$
PROOF: Similar.

⟨1⟩2. If there exist positive real numbers α and β such that, for all $x \in E$, $\alpha\|x\|_1 \leq \|x\|_2 \leq \beta\|x\|_1$. then $\| \|_1$ and $\| \|_2$ are equivalent.

⟨2⟩1. ASSUME: α and β are positive reals with $\forall x \in E.\alpha\|x\|_1 \leq \|x\|_2 \leq \beta\|x\|_1$.

⟨2⟩2. Let (x_n) be a sequence in E and $l \in E$

⟨2⟩3. If (x_n) converges to l under $\| \|_1$ then (x_n) converges to l under $\| \|_2$.

⟨3⟩1. ASSUME: (x_n) converges to l under $\| \|_1$

⟨3⟩2. LET: $\epsilon > 0$

⟨3⟩3. PICK N such that $\forall n \geq N.\|x_n - l\|_1 < \epsilon/\beta$

⟨3⟩4. $\forall n \geq N.\|x_n - l\|_2 < \epsilon$

⟨2⟩4. If (x_n) converges to l under $\| \|_2$ then (x_n) converges to l under $\| \|_1$.

PROOF: Similar.

□

Theorem 13.1.13. *Any two norms on a finite dimensional vector space are equivalent.*

PROOF:

⟨1⟩1. LET: V be a finite dimensional vector space over K.

⟨1⟩2. ASSUME: w.l.o.g. $\dim V > 0$

⟨1⟩3. PICK a basis $\{e_1, \ldots, e_n\}$ for V.

⟨1⟩4. LET: $\| \|_0 : V \to \mathbb{R}$ be the function: $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\|_0 = |\alpha_1| + \cdots + |\alpha_n|$.

⟨1⟩5. $\| \|_0$ is a norm.

⟨2⟩1. If $\|v\|_0 = 0$ then $v = 0$

PROOF: If $|\alpha_1| + \cdots + |\alpha_n| = 0$ then $\alpha_1 = \cdots = \alpha_n = 0$ so $\alpha_1 e_1 + \cdots + \alpha_n e_n = 0$.

⟨2⟩2. $\|\lambda v\|_0 = |\lambda|\|v\|_0$

PROOF:

$$\begin{aligned}
\|\lambda(\alpha_1 e_1 + \cdots + \alpha_n e_n)\|_0 &= \|\lambda\alpha_1 e_1 + \cdots + \lambda\alpha_n e_n\|_0 \\
&= |\lambda\alpha_1| + \cdots + |\lambda\alpha_n| && (\langle 1\rangle 4) \\
&= |\lambda|(|\alpha_1| + \cdots + |\alpha_n|) \\
&= |\lambda|\|\alpha_1 e_1 + \cdots + \alpha_n e_n\|_0 && (\langle 1\rangle 4)
\end{aligned}$$

⟨2⟩3. $\|u + v\|_0 \leq \|u\|_0 + \|v\|_0$

PROOF:

$$\begin{aligned}
\|(\alpha_1 e_1 + \cdots + \alpha_n e_n) + (\beta_1 e_1 + \cdots + \beta_n e_n)\| &= |\alpha_1 + \beta_1| + \cdots + |\alpha_n + \beta_n| \\
&\leq |\alpha_1| + \cdots + |\alpha_n| + |\beta_1| + \cdots + |\beta_n| \\
&= \|\alpha_1 e_1 + \cdots + \alpha_n e_n\|_0 + \|\beta_1 e_1 + \cdots + \beta_n e_n\|_0
\end{aligned}$$

⟨1⟩6. Any norm on V is equivalent to $\| \|_0$.

⟨2⟩1. LET: $\| \|$ be any norm on V.

⟨2⟩2. PICK $\alpha > 0$ such that, for all $\alpha_1, \ldots, \alpha_n \in K$, we have $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\| \geq \alpha(|\alpha_1| + \cdots + |\alpha_n|)$

PROOF: Proposition 13.0.13, ⟨2⟩1, ⟨1⟩3.

⟨2⟩3. LET: $\beta = \max(\|e_1\|, \ldots, \|e_n\|)$

⟨2⟩4. $\beta > 0$

PROOF: $e_1, \ldots, e_n$ cannot all be zero by ⟨1⟩3.

⟨2⟩5. For all $x \in V$ we have $\alpha\|x\|_0 \leq \|x\| \leq \beta\|x\|_0$
⟨3⟩1. LET: $x \in V$
⟨3⟩2. $\alpha\|x\|_0 \leq \|x\|$
PROOF: ⟨1⟩3, ⟨1⟩4, ⟨2⟩2.
⟨3⟩3. $\|x\| \leq \beta\|x\|_0$
⟨4⟩1. LET: $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$
⟨4⟩2. Q.E.D.
PROOF:

$$\begin{aligned}
\|x\| &= \|\alpha_1 e_1 + \cdots + \alpha_n e_n\| && (\langle 4\rangle 1) \\
&\leq |\alpha_1|\|e_1\| + \cdots + |\alpha_n|\|e_n\| && (\langle 2\rangle 1) \\
&\leq \beta(|\alpha_1| + \cdots + |\alpha_n|) && (\langle 2\rangle 3) \\
&= \beta\|x\|_0 && (\langle 1\rangle 4)
\end{aligned}$$

⟨2⟩6. Q.E.D.
PROOF: Theorem 13.1.12, ⟨1⟩5, ⟨2⟩1, ⟨2⟩2, ⟨2⟩4, ⟨2⟩5.
□

Definition 13.1.14 (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 13.1.15 (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 13.1.16 (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 13.1.17 (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 13.1.18. *Equivalent norms define the same set of open sets.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: $\| \|_1$ and $\| \|_2$ be equivalent norms on V.
⟨1⟩3. PICK reals $\alpha, \beta > 0$ such that, for all $x \in V$, we have $\alpha\|x\|_1 \leq \|x\|_2 \leq \beta\|x\|_1$
⟨1⟩4. LET: $S \subseteq V$
⟨1⟩5. If S is open under $\| \|_1$ then S is open under $\| \|_2$.
⟨2⟩1. ASSUME: S is open under $\| \|_1$.
⟨2⟩2. LET: $x \in S$
⟨2⟩3. PICK $\epsilon > 0$ such that $\{y \in V \mid \|x - y\|_1 < \epsilon\} \subseteq S$.
⟨2⟩4. LET: $\delta = \alpha\epsilon$

⟨2⟩5. $\{y \in V \mid \|x - y\|_2 < \delta\} \subseteq S$
⟨1⟩6. If S is open under $\| \|_2$ then S is open under $\| \|_1$.
PROOF: Similar.
□

Proposition 13.1.19. *Every open ball is open.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: $c \in V$ and $r > 0$
PROVE: $B(c, r)$ is open.
⟨1⟩3. LET: $x \in B(c, r)$
⟨1⟩4. LET: $\epsilon = r - \|x - c\|$
PROVE: $B(x, \epsilon) \subseteq B(c, r)$
⟨1⟩5. LET: $y \in B(x, \epsilon)$
PROVE: $y \in B(c, r)$
⟨1⟩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 13.1.20. *Let Ω 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:
⟨1⟩1. LET: $g \in U$
⟨1⟩2. LET: $\epsilon = \max_{x \in \Omega}(f(x) - g(x))$
PROVE: $B(g, \epsilon) \subseteq S$
⟨1⟩3. $\epsilon > 0$
⟨1⟩4. LET: $h \in B(g, \epsilon/2)$
PROVE: $h \in S$
⟨1⟩5. LET: $x \in \Omega$
⟨1⟩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 13.1.21. *Let Ω 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 13.1.22. *Let Ω 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 13.1.23. *Let Ω 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 13.1.24. *The union of a set of open sets is open.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: $\mathcal{U}$ be a set of open sets in V.
⟨1⟩3. LET: $x \in \bigcup \mathcal{U}$
⟨1⟩4. PICK $U \in \mathcal{U}$ such that $x \in U$.
⟨1⟩5. PICK $\epsilon > 0$ such that $B(x, \epsilon) \subseteq U$
⟨1⟩6. $B(x, \epsilon) \subseteq \bigcup \mathcal{U}$
□

Proposition 13.1.25. *The intersection of two open sets is open.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: U_1 and U_2 be open sets in V.
⟨1⟩3. LET: $x \in U_1 \cap U_2$
⟨1⟩4. PICK $\epsilon_1 > 0$ such that $B(x, \epsilon_1) \subseteq U_1$
⟨1⟩5. PICK $\epsilon_2 > 0$ such that $B(x, \epsilon_2) \subseteq U_2$
⟨1⟩6. LET: $\epsilon = \min(\epsilon_1, \epsilon_2)$
⟨1⟩7. $B(x, \epsilon) \subseteq U_1 \cap U_2$
□

Proposition 13.1.26. *In any normed space, $\emptyset$ is open.*

PROOF: Vacuous. □

Proposition 13.1.27. *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 13.1.28 (Closed Set)**.** Let V be a normed space over K. A set $S \subseteq V$ is *closed* iff $V - S$ is open.

Proposition 13.1.29. *Every closed ball is closed.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: $c \in V$ and $r > 0$
PROVE: $\overline{B}(c, r)$ is closed.
⟨1⟩3. LET: $x \in V - \overline{B}(c, r)$
⟨1⟩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:

$$\begin{aligned} \|y - c\| &\geq \|x - c\| - \|x - y\| && \text{(Triangle Inequality)} \\ &> \|x - c\| - \epsilon && (\langle 1\rangle 6) \\ &= r && (\langle 1\rangle 4) \end{aligned}$$

∎

Proposition 13.1.30. *The intersection of a set of closed sets is closed.*

PROOF: From Proposition 13.1.24. ∎

Proposition 13.1.31. *The union of two closed sets is closed.*

PROOF: From Proposition 13.1.25. ∎

Proposition 13.1.32. *Every sphere is closed.*

PROOF: $S(c, r) = \overline{B}(c, r) - B(c, r)$. ∎

Proposition 13.1.33. *Let Ω 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 $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . g(x) > f(x)\}$. ∎

Proposition 13.1.34. *Let Ω 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 $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . g(x) < f(x)\}$. ∎

Proposition 13.1.35. *Let Ω 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 $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . |g(x)| > f(x)\}$. ∎

Proposition 13.1.36. *Let Ω 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 $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega . |g(x)| < f(x)\}$. ∎

Proposition 13.1.37. *Let Ω 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 $B(g, \epsilon) \subseteq \mathcal{C}(\Omega) - C$. ∎

Proposition 13.1.38. *In any normed space V, we have $\emptyset$ is closed.*

PROOF: Since $V - \emptyset = V$ is open. ∎

Proposition 13.1.39. *In any normed space V, the whole space V is closed.*

PROOF: Since $V - V = \emptyset$ is open. □

Theorem 13.1.40. *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 $\langle 2 \rangle 2$.
□

Definition 13.1.41 (Closure)**.** Let V be a normed space over K. Let S be a subset of V. The *closure* of S, $\mathrm{cl}\, S$, is the intersection of the set of closed sets that include S.

Proposition 13.1.42. *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 13.1.30. □

Theorem 13.1.43. *Let V be a normed space over K. Let S be a subset of V. Then*

$$\mathrm{cl}\, S = \{l \in V \mid \exists \text{ a sequence } (x_n) \text{ in } S . x_n \to l \text{ as } n \to \infty\} \ .$$

PROOF:
$\langle 1 \rangle 1$. For all $l \in \mathrm{cl}\, S$, there exists a sequence (x_n) in S such that $x_n \to l$ as $n \to \infty$.
 $\langle 2 \rangle 1$. LET: $l \in \mathrm{cl}\, S$
 $\langle 2 \rangle 2$. 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.

⟨2⟩3. $x_n \to l$ as $n \to \infty$
⟨1⟩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 13.1.40.
□

Definition 13.1.44 (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 13.1.45 (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 13.1.46. *Let $p \geq 1$. The set of all sequences that have only finitely many non-zero terms is dense in l^p.*

PROOF:
⟨1⟩1. LET: $(z_n) \in l^p$
⟨1⟩2. LET: $\epsilon > 0$
PROVE: There exists a sequence (x_n) with only finitely many non-zero terms such that $\left(\sum_{n=1}^{\infty} |z_n - x_n|^p\right)^{1/p} < \epsilon$
⟨1⟩3. PICK N such that $|\sum_{n=1}^{\infty} |z_n|^p - \sum_{n=1}^{N} |z_n|^p| < \epsilon^p$
⟨1⟩4. LET: (x_n) be the sequence that agrees with (z_n) up to term N, and then zeros after that.
⟨1⟩5. $\left(\sum_{n=1}^{\infty} |z_n - x_n|^p\right)^{1/p} < \epsilon$
PROOF:

$$\begin{aligned} \left(\sum_{n=1}^{\infty} |z_n - x_n|^p\right)^{1/p} &= \left(\sum_{n=N+1}^{\infty} |z_n|^p\right)^{1/p} && (\langle 1\rangle 4) \\ &< \epsilon && (\langle 1\rangle 2) \end{aligned}$$

□

Theorem 13.1.47. *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:
⟨1⟩1. $1 \Leftrightarrow 2$
PROOF: Theorem 13.1.43.
⟨1⟩2. $1 \Rightarrow 3$
⟨2⟩1. ASSUME: S is dense.
⟨2⟩2. LET: U be a nonempty open subset of V.
⟨2⟩3. $X - U$ does not include S.

PROOF: Lest we have $\operatorname{cl} S \subseteq X - U$.
⟨2⟩4. U intersects S.
⟨1⟩3. $3 \Rightarrow 1$
⟨2⟩1. ASSUME: Every nonempty subset of V intersects S.
⟨2⟩2. Every closed proper subset of V does not include S.
⟨2⟩3. $\operatorname{cl} S = V$
□

Definition 13.1.48 (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 13.1.49. *In K^n, a set is compact if and only if it is bounded and closed.*

PROOF: TODO

Definition 13.1.50 (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 13.1.51. *Every compact set is closed and bounded.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: $S \subseteq V$ be compact.
⟨1⟩3. S is closed.
⟨2⟩1. LET: (x_n) be a sequence in S that converges to l
⟨2⟩2. PICK a sequence (x_{n_r}) that converges to $x \in S$
PROOF: ⟨1⟩2, ⟨2⟩1
⟨2⟩3. $x_{n_r} \to l$ as $n \to \infty$
PROOF: ⟨2⟩1, ⟨2⟩2
⟨2⟩4. $l = x$
PROOF: Proposition 13.1.2.
⟨2⟩5. $l \in S$
PROOF: ⟨2⟩2, ⟨2⟩4
⟨2⟩6. Q.E.D.
PROOF: Theorem 13.1.40.
⟨1⟩4. S is bounded.
⟨2⟩1. ASSUME: for a contradiction S is unbounded.
⟨2⟩2. For $n \in \mathbb{Z}_+$, PICK $x_n \in S - B(0, n)$
⟨2⟩3. PICK a convergent subsequence (x_{n_r}) that converges to l, say.
⟨2⟩4. PICK $N \in \mathbb{Z}_+$ such that $\|l\| < N$
⟨2⟩5. PICK r such that $n_r > N$ and $\|x_{n_r} - l\| < N - \|l\|$
⟨2⟩6. $\|x_{n_r}\| < N < n_r$
⟨2⟩7. This contradicts ⟨2⟩2.
□

Proposition 13.1.52. *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. □

Theorem 13.1.53 (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:
⟨1⟩1. PICK $z \in V - X$
⟨1⟩2. LET: $d = \inf_{x \in X} \|z - x\|$
⟨1⟩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 $x \in X$.
⟨1⟩4. PICK $x_0 \in X$ such that $d \leq \|z - x_0\| \leq d/\epsilon$
PROOF: One exists since d/ϵ is not a lower bound for $\{\|z - x\| \mid x \in X\}$.
⟨1⟩5. LET: $x = (z - x_0)/\|z - x_0\|$
⟨1⟩6. LET: $y \in X$
⟨1⟩7. $\|x - y\| \geq \epsilon$
PROOF:

$$\begin{aligned} \|x - y\| &= \left\| \frac{z - x_0}{\|z - x_0\|} - y \right\| && (\langle 1 \rangle 5) \\ &= \frac{1}{\|z - x_0\|} \|z - (x_0 + \|z - x_0\| y)\| \\ &\geq \frac{1}{\|z - x_0\|} d && (\langle 1 \rangle 2) \\ &\geq \epsilon && (\langle 1 \rangle 4) \end{aligned}$$

□

Theorem 13.1.54. *Let V be a normed space over K. Then V is finite dimensional if and only if $\overline{B}(0,1)$ is compact.*

PROOF:
⟨1⟩1. If V is finite dimensional then $\overline{B}(0,1)$ is compact.
⟨2⟩1. ASSUME: V is finite dimensional.
⟨2⟩2. PICK a basis $\{e_1, \ldots, e_n\}$
⟨2⟩3. ASSUME: w.l.o.g. $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\| = |\alpha_1| + \cdots + |\alpha_n|$
⟨2⟩4. LET: $(\alpha_{k1} e_1 + \cdots + \alpha_{kn} e_n)$ be a sequence in $\overline{B}(0,1)$
⟨2⟩5. PICK a convergent subsequence $(\alpha_{k_r 1})$ of (α_{k1}), a convergent subsequence $(\alpha_{k'_r 2})$ of $(\alpha_{k_r 2})$, …, a convergent subsequence $(\alpha_{k''_r n})$.
⟨2⟩6. $(\alpha_{k''_r 1} e_1 + \cdots + \alpha_{k''_r n})$ converges.
⟨1⟩2. If V is infinite dimensional then $\overline{B}(0,1)$ is not compact.
⟨2⟩1. ASSUME: V is infinite dimensional.
⟨2⟩2. Choose a sequence (x_n) with $\|x_n\| = 1$ and $\|x_m - x_n\| \geq 1/2$ for $m \neq n$
⟨3⟩1. ASSUME: $x_1, \ldots, x_n$ satisfy $\|x_i\| = 1$ and $\|x_i - x_j\| \geq 1/2$ for $i \neq j$
⟨3⟩2. PICK $x_{n+1} \in V$ such that $\|x_{n+1}\| = 1$ and for all $y \in \text{span}\{x_1, \ldots, x_n\}$ we have $\|x_{n+1} - y\| \geq 1/2$

⟨4⟩1. span$\{x_1, \ldots, x_n\}$ is closed.
⟨5⟩1. LET: $S = \text{span}\{x_1, \ldots, x_n\}$
⟨5⟩2. LET: (a_n) be a sequence in S that converges to $a \in V$
PROVE: $a \in S$
⟨5⟩3. (a_n) is a Cauchy sequence in V.
⟨5⟩4. (a_n) is a Cauchy sequence in S.
⟨5⟩5. A finite dimensional normed space is a Banach space.
⟨5⟩6. S is complete.
⟨5⟩7. $a \in S$
⟨4⟩2. span$\{x_1, \ldots, x_n\}$ is a proper subspace of V.
PROOF: ⟨2⟩1
⟨4⟩3. Q.E.D.
PROOF: Riesz's Lemma.
⟨2⟩3. ASSUME: for a contradiction (x_{n_r}) is a subsequence that converges to l
⟨2⟩4. For all $r \in \mathbb{N}$, we have $\|x_{n_r} - l\| + \|x_{n_{r+1}} - l\| \geq 1/2$
⟨2⟩5. This is a contradiction.
□

Proposition 13.1.55. *Let V be a normed space. The closure of a subspace of V is a subspace.*

PROOF:
⟨1⟩1. LET: U be a subspace of V
⟨1⟩2. LET: $x, y \in \text{cl}\, U$ and $\alpha, \beta \in K$
⟨1⟩3. PICK sequences (x_n), (y_n) in U that converge to x and y respectively.
⟨1⟩4. $\alpha x_n + \beta y_n \to \alpha x + \beta y$ as $n \to \infty$
⟨1⟩5. $\alpha x + \beta y \in \text{cl}\, U$
□

13.2 Continuous Linear Mappings

Definition 13.2.1 (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 13.2.2. *Let V be a normed space. Then the norm is a continuous function $V \to \mathbb{R}$.*

PROOF: From Proposition 13.0.4. □

Proposition 13.2.3. *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 13.2.4. *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 $n \to \infty$.
□

Definition 13.2.5 (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 13.2.6. *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 $n \to \infty$
  $\langle 2 \rangle 5$. $T(y_n) \not\to 0$ 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:
$$\begin{aligned} \|T(x_n)\| &\leq \alpha \|x_n\| && (\langle 2 \rangle 2) \\ &\to 0 && \text{as } n \to \infty \end{aligned}$$
  $\langle 2 \rangle 4$. T is continuous.
    PROOF: Proposition 13.2.4.
□

Proposition 13.2.7. *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 13.1.13.
⟨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 13.2.7.1. *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 13.2.8. *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 13.2.9. *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. $\forall x \in U. \|(\alpha S + \beta T)(x)\| \leq (|\alpha| B + |\beta| C)\|x\|$

$\square$

Proposition 13.2.10. *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:
⟨1⟩1. For all $T \in \mathcal{B}(U,V)$, the set $\{\|T(x)\| \mid x \in U, \|x\| = 1\}$ is bounded above.
  ⟨2⟩1. LET: $T \in \mathcal{B}(U,V)$
  ⟨2⟩2. PICK B such that $\forall x \in U. \|T(x)\| \leq B\|x\|$.
  ⟨2⟩3. B is an upper bound for $\{\|T(x)\| \mid x \in U, \|x\| = 1\}$.
⟨1⟩2. If $\|T\| = 0$ then $T = 0$.
  ⟨2⟩1. ASSUME: $\|T\| = 0$
  ⟨2⟩2. LET: $x \in U$
    PROVE: $T(x) = 0$
  ⟨2⟩3. ASSUME: w.l.o.g. $\|x\| \neq 0$
  ⟨2⟩4. LET: $y = x/\|x\|$
  ⟨2⟩5. $\|y\| = 1$
  ⟨2⟩6. $\|T(y)\| = 0$
  ⟨2⟩7. $T(y) = 0$
  ⟨2⟩8. $T(x) = 0$
⟨1⟩3. For all $\lambda \in K$ and $T \in \mathcal{B}(U,V)$, we have $\|\lambda T\| = |\lambda|\|T\|$
  ⟨2⟩1. LET: $\lambda \in K$ and $T \in \mathcal{B}(U,V)$
  ⟨2⟩2. $\|\lambda T\| = |\lambda|\|T\|$
    PROOF:
$$\begin{aligned}
\|\lambda T\| &= \sup\{\|\lambda T(x)\| \mid x \in U, \|x\| = 1\} \\
&= \sup\{|\lambda|\|T(x)\| \mid x \in U, \|x\| = 1\} \\
&= |\lambda| \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\} \\
&= |\lambda|\|T\|
\end{aligned}$$
⟨1⟩4. For all $S, T \in \mathcal{B}(U,V)$, we have $\|S + T\| \leq \|S\| + \|T\|$.
  ⟨2⟩1. LET: $S, T \in \mathcal{B}(U,V)$
  ⟨2⟩2. $\|S + T\| \leq \|S\| + \|T\|$
    PROOF:
$$\begin{aligned}
\|S + T\| &= \sup\{\|S(x) + T(x)\| \mid x \in U, \|x\| = 1\} \\
&\leq \sup\{\|S(x)\| + \|T(x)\| \mid x \in U, \|x\| = 1\} \\
&\leq \sup\{\|S(x)\| \mid x \in U, \|x\| = 1\} + \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\} \\
&= \|S\| + \|T\|
\end{aligned}$$

$\square$

Proposition 13.2.11. *Let U and V be normed spaces. Let $T \in \mathcal{B}(U,V)$. Then $\|T\|$ is the least number such that $\forall u \in U. \|T(u)\| \leq \|T\|\|u\|$.*

PROOF:
⟨1⟩1. $\forall u \in U. \|T(u)\| \leq \|T\|\|u\|$
  ⟨2⟩1. LET: $u \in U$
  ⟨2⟩2. LET: $v = u/\|u\|$

⟨2⟩3. $\|T(v)\| \leq \|T\|$
⟨2⟩4. $\|T(u)\| \leq \|T\|\|u\|$
⟨1⟩2. If α satisfies $\forall u \in U. \|T(u)\| \leq \alpha\|u\|$, then $\|T\| \leq \alpha$
⟨2⟩1. Assume: $\forall u \in U. \|T(u)\| \leq \alpha\|u\|$
⟨2⟩2. For all $x \in U$, if $\|x\| = 1$ then $\|T(x)\| \leq \alpha$
⟨2⟩3. $\|T\| \leq \alpha$
□

Proposition 13.2.12. *Let V be a normed space. Then id_V is a bounded linear function $V \to V$, and $\|\mathrm{id}_V\| = 1$.*

Proposition 13.2.13. *Let U and V be normed spaces. The constant zero function $U \to V$ is a bounded linear transformation with norm 0.*

Proposition 13.2.14. *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*

$$\|T\| \leq \sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} |a_{ij}|^2} \enspace .$$

Definition 13.2.15 (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 13.2.16. *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:
⟨1⟩1. $\ker T$ is a subspace of U
Proof: If $x, y \in \ker T$ and $\alpha, \beta \in K$ then $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) = 0$.
⟨1⟩2. $\ker T$ is closed.
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 13.2.17. *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:
⟨1⟩1. Assume: w.l.o.g. $T \neq 0$
⟨1⟩2. Let: $(x, y) \in (U \times V) - G$, i.e. $y \neq T(x)$
⟨1⟩3. Let: $\epsilon = \|y - T(x)\| > 0$
⟨1⟩4. Let: $x' \in W$ with $\|x - x'\| < \epsilon/3\|T\|$
⟨1⟩5. Let: $y' \in V$ with $\|y - y'\| < \epsilon/3$
⟨1⟩6. $y' \neq T(x')$

PROOF:
$$\begin{aligned}\|y' - T(x')\| &\geq \|y - T(x)\| - \|y - y'\| - \|T(x) - T(x')\| \\ &> \epsilon/3 \\ &> 0\end{aligned}$$
∎

Theorem 13.2.18 (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*
$$\sum_{s=1}^{\infty} x_{p_{j_r} p_{j_s}} \to 0 \text{ as } r \to \infty$$

then $x_{ii} \to 0$ as $i \to \infty$.

PROOF:
⟨1⟩1. ASSUME: for a contradiction $x_{ii} \not\to 0$ as $i \to \infty$
⟨1⟩2. PICK $\epsilon > 0$ such that, for all N, there exists $n \geq N$ such that $\|x_{nn}\| \geq \epsilon$
⟨1⟩3. PICK an increasing sequence of integers (p_j) such that $\|x_{p_j p_j}\| \geq \epsilon$ for all j.
⟨1⟩4. PICK a subsequence (q_i) such that $\sum_{j=1}^{\infty} x_{q_i q_j} \to 0$ as $i \to \infty$
⟨1⟩5. For all i, we have $x_{q_i q_j} \to 0$ as $j \to \infty$
⟨1⟩6. For all j, we have $x_{q_i q_j} \to 0$ as $i \to \infty$
⟨1⟩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 $j = 1, \ldots, n$.
⟨1⟩8. $\|x_{r_i r_j}\| < \epsilon/2^{j+1}$ for all i, j such that $i \neq j$
⟨1⟩9. PICK a subsequence (s_j) of (r_j) such that $\sum_{j=1}^{\infty} x_{s_i s_j} \to 0$ as $i \to \infty$
⟨1⟩10. For all i we have $\| \sum_{j=1}^{\infty} x_{s_i s_j}\| \geq \epsilon/2$
PROOF:
$$\begin{aligned}\left\|\sum_{j=1}^{\infty} x_{s_i s_j}\right\| &= \left\|x_{s_i s_i} + \sum_{i \neq j} x_{s_i s_j}\right\| \\ &\geq \left| \|x_{s_i s_i}\| - \left\|\sum_{i \neq j} x_{s_i s_j}\right\| \right| && \text{(Proposition 13.0.4)} \\ &\geq \left| \|x_{s_i s_i}\| - \sum_{i \neq j} \|x_{s_i s_j}\| \right| \\ &\geq \epsilon/2 && (\langle 1\rangle 2,\ \langle 1\rangle 8)\end{aligned}$$
⟨1⟩11. Q.E.D.
PROOF: ⟨1⟩9 and ⟨1⟩10 form a contradiction.
∎

13.3 Banach Spaces

Definition 13.3.1 (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 13.3.2. *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 $\forall n \geq N. \|x_{q_n} - x_n\| < \epsilon/2$
  $\langle 2 \rangle 5.$ $\forall n \geq N. \|x_{p_n} - x_{q_n}\| < \epsilon$
$\square$

Proposition 13.3.3. *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 $\forall n \geq N. \|x_n - l\| < \epsilon/2$

⟨1⟩4. For all $m, n \geq N$ we have $\|x_m - x_n\| < \epsilon$.
□

Proposition 13.3.4. *In $\mathcal{P}([0,1])$, let*

$$P_n(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!} \quad .$$

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. □

Proposition 13.3.5. *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:
⟨1⟩1. $(\|x_n\|)$ is Cauchy.
  ⟨2⟩1. LET: $\epsilon > 0$
  ⟨2⟩2. PICK N such that $\forall m, n \geq N. \|x_m - x_n\| < \epsilon$
  ⟨2⟩3. $\forall m, n \geq N. |\|x_m\| - \|x_n\|| < \epsilon$
    PROOF: Proposition 13.0.4.
⟨1⟩2. Q.E.D.
  PROOF: Since every Cauchy sequence in $\mathbb{R}$ converges.
□

Proposition 13.3.6. *Every Cauchy sequence is bounded.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. LET: (x_n) be a Cauchy sequence in V.
⟨1⟩3. PICK N such that $\forall m, n \geq N. \|x_m - x_n\| < 1$.
⟨1⟩4. LET: $B = \max(\|x_1\|, \ldots, \|x_{N-1}\|, \|x_N\| + 1$
⟨1⟩5. $\forall n. \|x_n\| \leq B$
□

Definition 13.3.7 (Banach Space)**.** A normed space V over K is *complete* or a *Banach space* iff every Cauchy sequence converges.

Proposition 13.3.8. *l^2 is complete.*

PROOF:
⟨1⟩1. LET: (a_n) be a Cauchy sequence in l^2 where $a_n = (\alpha_{n1}, \alpha_{n2}, \ldots)$.
⟨1⟩2. For all $\epsilon > 0$, there exists $n_0 \in \mathbb{Z}_+$ such that $\forall m, n \geq n_0. \sum_{k=1}^{\infty} |\alpha_{mk} - \alpha_{nk}|^2 < \epsilon^2$.
⟨1⟩3. For every $k \in \mathbb{Z}_+$ and $\epsilon > 0$, there exists $n_0 \in \mathbb{Z}_+$ such that $\forall m, n \geq n_0. |\alpha_{mk} - \alpha_{nk}| < \epsilon$.
⟨1⟩4. For every $k \in \mathbb{Z}_+$, (α_{nk}) is Cauchy in $\mathbb{C}$.
⟨1⟩5. For every $k \in \mathbb{Z}_+$, (α_{nk}) converges in $\mathbb{C}$.
⟨1⟩6. For $k \in \mathbb{Z}_+$,

LET: $\alpha_k = \lim_{n\to\infty} \alpha_{nk}$
⟨1⟩7. Let a be the sequence (α_k)
⟨1⟩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 ⟨1⟩2.
⟨1⟩9. $a \in l^2$
⟨2⟩1. PICK n_0 such that $\forall n \geq n_0. \sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2 \leq 1$
PROOF: ⟨1⟩8
⟨2⟩2. $(\alpha_k - \alpha_{n_0 k}) \in l^2$
⟨2⟩3. $(\alpha_{n_0 k}) \in l^2$
PROOF: By ⟨1⟩1 since the sequence is a_{n_0}.
⟨2⟩4. $(\alpha_k) \in l^2$
PROOF: Proposition 11.0.2.
⟨1⟩10. $a_n \to a$ as $n \to \infty$
PROOF: By ⟨1⟩8 since $\|a - a_n\| = \sqrt{\sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2}$.
□

Proposition 13.3.9. *Let a and b be real numbers with $a < b$. The space $\mathcal{C}([a, b])$ is complete.*

PROOF:
⟨1⟩1. LET: $X = [a, b]$
⟨1⟩2. LET: (f_n) be a Cauchy sequence in $\mathcal{C}([a, b])$.
⟨1⟩3. For all $\epsilon > 0$, there exists n_0 such that $\forall n, m \geq n_0. \|f_n - f_m\| < \epsilon$.
⟨1⟩4. For all $\epsilon > 0$, there exists n_0 such that $\forall n, m \geq n_0. \forall x \in X. |f_n(x) - f_m(x)| < \epsilon$.
⟨1⟩5. For all $x \in [a, b]$, $(f_n(x))$ is Cauchy.
⟨1⟩6. Define $f : [a, b] \to \mathbb{C}$ by $f(x) = \lim_{n\to\infty} f_n(x)$.
⟨1⟩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 ⟨1⟩4.
⟨1⟩8. f is continuous
⟨2⟩1. LET: $x_0 \in X$
⟨2⟩2. LET: $\epsilon > 0$
⟨2⟩3. PICK n_0 such that $\forall n \geq n_0. \forall x \in X. |f_n(x) - f(x)| < \epsilon/3$
PROOF: By ⟨1⟩7.
⟨2⟩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.
⟨2⟩5. LET: $x \in X$
⟨2⟩6. ASSUME: $|x - x_0| < \delta$
⟨2⟩7. $|f(x) - f(x_0)| < \epsilon$
PROOF:
$$\begin{aligned} |f(x) - f(x_0)| &\leq |f(x) - f_{n_0}(x)| + |f_{n_0}(x) - f_{n_0}(x_0)| + |f_{n_0}(x_0) - f(x_0)| && \text{(Triangle Inequality)} \\ &< \epsilon/3 + \epsilon/3 + \epsilon/3 && (\langle 2\rangle 3,\ \langle 2\rangle 4) \\ &= \epsilon \end{aligned}$$
⟨1⟩9. (f_n) converges to f uniformly.
PROOF: From ⟨1⟩7
□

Definition 13.3.10 (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 13.3.11 (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 13.3.12. *In $\mathcal{P}([0,1])$, the series $\sum_{n=0}^{\infty} x^n/n!$ is absolutely convergent but not convergent.*

PROOF: Proposition 13.3.4. □

Theorem 13.3.13. *A normed space is complete if and only if every absolutely convergent series is convergent.*

PROOF:
⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. If V is complete then every absolutely convergent series is convergent.
⟨2⟩1. ASSUME: V is complete.
⟨2⟩2. LET: $\sum_{n=1}^{\infty} a_n$ be absolutely convergent in V.
⟨2⟩3. For $n \in \mathbb{Z}_+$,
LET: $s_n = \sum_{k=1}^{n} a_k$
.
⟨2⟩4. (s_n) is Cauchy.
⟨3⟩1. LET: $\epsilon > 0$
⟨3⟩2. PICK k such that $\sum_{n=k+1}^{\infty} \|a_n\| < \epsilon$
⟨3⟩3. LET: $m > n > k$
⟨3⟩4. $\|s_m - s_n\| < \epsilon$
PROOF:

$$\begin{aligned} \|s_m - s_n\| &= \left\| \sum_{i=n+1}^{m} a_i \right\| && (\langle 2\rangle 3,\ \langle 3\rangle 3) \\ &\leq \sum_{i=s+1}^{m} \|a_i\| && (\text{Triangle inequality}) \\ &\leq \sum_{i=k+1}^{\infty} \|a_i\| \\ &< \epsilon && (\langle 3\rangle 2,\ \langle 3\rangle 3) \end{aligned}$$

⟨2⟩5. (s_n) converges.
⟨1⟩3. If every absolutely convergent series is convergent then V is complete.
⟨2⟩1. ASSUME: Every absolutely convergent series in V is convergent.
⟨2⟩2. LET: (a_n) be a Cauchy sequence in V.
⟨2⟩3. PICK a strictly increasing sequence of positive integers (p_n) such that $\forall k. \forall m, n \geq p_k. \|x_m - x_n\| < 2^{-k}$.
⟨2⟩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: $\langle 2\rangle 2$, $\langle 2\rangle 7$
$\langle 3\rangle 3.$ $\forall n \geq N. \|x_n - (s + x_{p_1})\| < \epsilon$
□

Theorem 13.3.14. *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 13.1.40.
$\langle 1\rangle 7.$ $a_n \to l$ as $n \to \infty$ in U.
□

Definition 13.3.15 (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 13.3.16. *Every normed space has a completion.*

PROOF:

⟨1⟩1. LET: V be a normed space over K.
⟨1⟩2. Let us say two Cauchy sequences (x_n), (y_n) ore *equivalent* iff $x_n - y_n \to 0$ as $n \to \infty$.
⟨1⟩3. Equivalence is an equivalence relation on the set of Cauchy sequences.
⟨1⟩4. LET: W be the set of Cauchy sequences in V quotiented by equivalence.
⟨1⟩5. Define addition and multiplication on W by

$$[(x_n)] + [(y_n)] = [(x_n + y_n)]$$
$$\lambda[(x_n)] = [(\lambda x_n)]$$

⟨1⟩6. Define a norm on W by $\|[(x_n)]\| = \lim_{n\to\infty} \|x_n\|$
⟨1⟩7. Define $\phi : V \to W$ by $\phi(v) = [(v)]$.
⟨1⟩8. ϕ is injective.
⟨1⟩9. $\forall x, y \in V.\forall \alpha, \beta \in K.\phi(\alpha x + \beta y) = \alpha\phi(x) + \beta\phi(y)$
⟨1⟩10. $\forall x \in V.\|\phi(x)\| = \|x\|$
⟨1⟩11. $\phi(V)$ is dense in W.
⟨2⟩1. LET: $[(a_n)] \in W$ and $\epsilon > 0$.
PROVE: $B([(a_n)], \epsilon)$ intersects $\phi(V)$.
⟨2⟩2. PICK N such that $\forall m, n \geq N.\|a_m - a_n\| < \epsilon/2$
⟨2⟩3. $\phi(a_N) \in B([(a_n)], \epsilon)$
PROOF:

$$\begin{aligned}\|[(a_n)] - \phi(a_N)\| &= \lim_{n\to\infty} \|a_n - a_N\| \\ &\leq \epsilon/2 && (\langle 2\rangle 2) \\ &< \epsilon\end{aligned}$$

⟨1⟩12. W is complete.
⟨2⟩1. LET: (X_n) be a Cauchy sequence in W.
⟨2⟩2. For $n \in \mathbb{Z}_+$, PICK $x_n \in V$ such that

$$\|\phi(x_n) - X_n\| < 1/n \ .$$

⟨2⟩3. (x_n) is Cauchy in V.
⟨3⟩1. LET: $\epsilon > 0$
⟨3⟩2. PICK N such that $\forall m, n \geq N.\|X_n - X_m\| < \epsilon/3$ and $1/N < \epsilon/3$
⟨3⟩3. LET: $m, n \geq N$
⟨3⟩4. $\|x_m - x_n\| < \epsilon$
PROOF:

$$\begin{aligned}\|x_m - x_n\| &= \|\phi(x_m) - \phi(x_n)\| \\ &\leq \|\phi(x_m) - X_m\| + \|X_m - X_n\| + \|X_n - \phi(x_n)\| \\ &< \|X_m - X_n\| + 1/m + 1/n \\ &< \epsilon\end{aligned}$$

⟨2⟩4. LET: $X = [(x_n)]$
⟨2⟩5. $X_n \to X$ as $n \to \infty$
PROOF:

$$\begin{aligned}\|X_n - X\| &\leq \|X_n - \phi(x_n)\| + \|\phi(x_n) - X\| \\ &< \|\phi(x_n) - X\| + 1/n \\ &\to 0 && \text{as } n \to \infty\end{aligned}$$

□

Proposition 13.3.17. *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:

$$\begin{aligned} \|T_m(u) - T_n(u)\| &\leq \|T_m - T_n\| \|u\| && \text{(Proposition 13.2.11)} \\ &< \epsilon \end{aligned}$$

$\langle 1 \rangle 3$. 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:

$$\begin{aligned} \|T(x)\| &\leq \|T_N(x) - T(x)\| + \|T(x)\| && \text{(Triangle inequality)} \\ &\leq \|T_N - T\| \|x\| + \|T\| \|x\| && \text{(Proposition 13.2.11)} \\ &< \|x\| + B\|x\| && (\langle 3 \rangle 1,\ \langle 3 \rangle 2) \\ &= (B+1)\|x\| \end{aligned}$$

$\langle 1 \rangle 5$. $T_n \to T$ 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 13.3.17.1. *For any normed space V over K, the space $\mathcal{B}(V,K)$ is a Banach space.*

Theorem 13.3.18. *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 $\mathrm{cl}\, W \to V$.*

PROOF:
$\langle 1\rangle 1$. Define $S : \mathrm{cl}\, W \to V$ by: $S(x) = \lim_{n\to\infty} T(x_n)$, where (x_n) is any sequence in W that converges to x.
$\langle 2\rangle 1$. For all $x \in \mathrm{cl}\, W$, there exists a sequence (x_n) in W that converges to x.
PROOF: Theorem 13.1.43.
$\langle 2\rangle 2$. If (x_n) is a Cauchy sequence in W then $(T(x_n))$ is Cauchy in V.
$\langle 3\rangle 1$. ASSUME: w.l.o.g. $T \neq 0$
$\langle 3\rangle 2$. LET: (x_n) be a Cauchy sequence in W.
$\langle 3\rangle 3$. PICK $B > 0$ such that $\forall x \in W. \|T(x)\| \leq B\|x\|$
$\langle 3\rangle 4$. LET: $\epsilon > 0$
$\langle 3\rangle 5$. PICK N such that $\forall m, n \geq N. \|x_m - x_n\| < \epsilon/\|T\|$
$\langle 3\rangle 6$. LET: $m, n \geq N$
$\langle 3\rangle 7$. $\|T(x_m) - T(x_n)\| < \epsilon$
$\langle 2\rangle 3$. If (x_n) and (y_n) are sequences in W that converge to the same element in $\mathrm{cl}\, W$ then $(T(x_n))$ and $(T(y_n))$ have the same limit in V.
$\langle 3\rangle 1$. ASSUME: w.l.o.g. $T \neq 0$
$\langle 3\rangle 2$. ASSUME: $x_n \to l$ and $y_n \to l$ as $n \to \infty$
$\langle 3\rangle 3$. LET: $T(x_n) \to a$ and $T(y_n) \to b$ as $n \to \infty$
$\langle 3\rangle 4$. ASSUME: for a contradiction $a \neq b$
$\langle 3\rangle 5$. LET: $\epsilon = \|a - b\|$
$\langle 3\rangle 6$. PICK N such that $\forall n \geq N. \|x_n - l\| < \epsilon/3\|T\|$ and $\forall n \geq N. \|y_n - l\| < \epsilon/3\|T\|$
$\langle 3\rangle 7$. $\forall n \geq N. \|T(x_n) - T(y_n)\| < 2\epsilon/3$
$\langle 3\rangle 8$. $\|a - b\| \leq 2\epsilon/3$
$\langle 3\rangle 9$. This contradicts $\langle 3\rangle 5$.
$\langle 1\rangle 2$. S extends T
$\langle 2\rangle 1$. LET: $w \in W$
$\langle 2\rangle 2$. $w \to w$ as $n \to \infty$
$\langle 2\rangle 3$. $T(w) \to T(w)$ as $n \to \infty$
$\langle 2\rangle 4$. $S(w) = T(w)$
$\langle 1\rangle 3$. S is bounded.
$\langle 2\rangle 1$. LET: $x \in \mathrm{cl}\, W$
PROVE: $\|S(x)\| \leq \|T\|\|x\|$
$\langle 2\rangle 2$. PICK a sequence (x_n) in W that converges to x.
$\langle 2\rangle 3$. $\|T(x_n)\| \leq \|T\|\|x_n\|$ for all n.
$\langle 2\rangle 4$. $\|S(x)\| \leq \|T\|\|x\|$
PROOF: Taking the limit as $n \to \infty$.
$\langle 1\rangle 4$. S is linear.

⟨2⟩1. LET: $x, y \in \mathrm{cl}\, W$ and $\alpha, \beta \in K$
⟨2⟩2. PICK sequences (x_n) and (y_n) in W that converge to x and y.
⟨2⟩3. $T(\alpha x_n + \beta y_n) = \alpha T(x_n) + \beta T(y_n)$ for all n.
⟨2⟩4. $S(\alpha x + \beta y) = \alpha S(x) + \beta S(y)$
PROOF: Taking the limit as $n \to \infty$.
⟨1⟩5. S is unique.
⟨2⟩1. LET: S' be a continuous linear extension of S defined on $\mathrm{cl}\, W$.
⟨2⟩2. LET: $x \in W$
PROVE: $S(x) = S'(x)$
⟨2⟩3. PICK a sequence (x_n) in W that converges to x.
⟨2⟩4. $T(x_n) = S'(x_n) \to S'(x)$ as $n \to \infty$
⟨2⟩5. $S'(x) = S(x)$
□

Corollary 13.3.18.1. *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 13.3.19 (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 13.3.20 (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:
⟨1⟩1. ASSUME: for a contradiction no such M exists.
⟨1⟩2. For $n \in \mathbb{Z}_+$, PICK $T_n \in \mathcal{T}$ such that $\|T_n\| > n2^n$.
⟨1⟩3. For $n \in \mathbb{Z}_+$, PICK $x_n \in X$ such that $\|x_n\| = 1$ and $\|T_n(x_n)\| > n2^n$.
⟨1⟩4. For $n \in \mathbb{Z}_+$,
$$\left\| \frac{1}{n} T_n \left(\frac{x_n}{2^n} \right) \right\| > 1 \ .$$
⟨1⟩5. For $i, j \in \mathbb{Z}_+$,
LET: $y_{ij} = \frac{1}{i} T_i(\frac{x_j}{2^j})$.
⟨1⟩6. For all $j \in \mathbb{Z}_+$, $y_{ij} \to 0$ as $i \to \infty$
⟨2⟩1. LET: $j \in \mathbb{Z}_+$
⟨2⟩2. PICK M such that $\forall T \in \mathcal{T}. \|T(x_j/2^j)\| \leq M$
⟨2⟩3. For all i, $\|y_{ij}\| \leq M/i$
⟨1⟩7. For any increasing sequence of positive integers (p_i), we have $\sum_{j=1}^{\infty} y_{p_i p_j} \to 0$ as $i \to \infty$
⟨2⟩1. LET: (p_i) be an increasing sequence of positive integers.
⟨2⟩2. LET: $z = \sum_{j=1}^{\infty} x_{p_j}/2^{p_j}$
PROOF: This converges by Theorem 13.3.13.
⟨2⟩3. PICK C such that $\forall T \in \mathcal{T}. \|T(z)\| \leq C$
⟨2⟩4. For all i, $\| \sum_{j=1}^{\infty} y_{p_i p_j} \| \leq C/p_i$.

PROOF:
$$\begin{aligned}
\left\| \sum_{j=1}^{\infty} y_{p_i p_j} \right\| &= \left\| \sum_{j=1}^{\infty} \frac{1}{p_i} T_{p_i} \left(\frac{x_{p_j}}{2^{p_j}} \right) \right\| && (\langle 1 \rangle 5) \\
&= \frac{1}{p_i} \left\| T_{p_i} \left(\sum_{j=1}^{\infty} \frac{x_{p_j}}{2^{p_j}} \right) \right\| && (T_{p_i} \text{ continuous}) \\
&= \frac{1}{p_i} \| T_{p_i}(z) \| && (\langle 2 \rangle 2) \\
&\leq \frac{C}{p_i} && (\langle 2 \rangle 3)
\end{aligned}$$

$\langle 2 \rangle 5$. $\sum_{j=1}^{\infty} y_{p_i p_j} \to 0$ 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.

□

13.4 Contraction Mappings

Definition 13.4.1 (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 α such that $0 < \alpha < 1$ and

$$\forall x, y \in A. \| f(x) - f(y) \| \leq \alpha \| x - y \| \ .$$

Proposition 13.4.2. *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 α 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 13.4.3 (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 α 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:

$$\begin{aligned} \|x_n - x_m\| &\leq \|x_n - x_{n-1}\| + \|x_{n-1} - x_{n-2}\| + \cdots + \|x_{m+1} - x_m\| && \text{(Triangle inequality)} \\ &\leq (\alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha^m)\|x_1 - x_0\| && (\langle 2 \rangle 1) \\ &< \frac{\|x_1 - x_0\|}{1 - \alpha} \alpha^m \end{aligned}$$

$\langle 2 \rangle 3$. 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:

$$\begin{aligned} f(z) &= f\left(\lim_{n \to \infty} x_n\right) \\ &= \lim_{n \to \infty} f(x_n) && \text{(Proposition 13.4.2)} \\ &= \lim_{n \to \infty} x_{n+1} \\ &= z \end{aligned}$$

$\langle 1 \rangle 7$. 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: $\|z - w\| = \|f(z) - f(w)\| \leq \alpha \|z - w\|$
$\langle 2 \rangle 4$. $\|z - w\| = 0$
$\langle 2 \rangle 5$. $z = w$
$\square$

Chapter 14

Inner Product Spaces

Definition 14.0.1 (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 14.0.2. *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 14.0.3.

$$\langle x, \alpha y + \beta z \rangle = \overline{\alpha} \langle x, y \rangle + \overline{\beta} \langle x, z \rangle$$

Proposition 14.0.4.

$$\langle 0, y \rangle = \langle x, 0 \rangle = 0$$

Proposition 14.0.5. *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 14.0.6. *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 14.0.7. *The function $\langle f, g \rangle = \int_a^b f(x) \overline{g(x)} dx$ is an inner product on $\mathcal{C}([a, b])$.*

Proposition 14.0.8. *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 14.0.9. *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 14.0.10 (Norm)**.** In an inner product space, define $\|x\| = \sqrt{\langle x, x\rangle}$.

Proposition 14.0.11 (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:
⟨1⟩1. Assume: w.l.o.g. $y \neq 0$
⟨1⟩2. $|\langle x, y\rangle| \leq \|x\|\|y\|$
  ⟨2⟩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 $\langle x + \alpha y, x + \alpha y\rangle$.
  ⟨2⟩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 ⟨2⟩1.
⟨1⟩3. If $|\langle x, y\rangle| = \|x\|\|y\|$ then x and y are linearly dependent.
  ⟨2⟩1. Assume: $|\langle x, y\rangle| = \|x\|\|y\|$
  ⟨2⟩2. $\langle x, y\rangle\langle y, x\rangle = \langle x, x\rangle\langle y, y\rangle$
  ⟨2⟩3. $\langle y, y\rangle x - \langle x, x\rangle y = 0$
    Proof:

$$\begin{aligned}\langle\langle y, y\rangle x - \langle x, y\rangle y, \langle y, y\rangle x - \langle x, y\rangle y\rangle &= \langle y, y\rangle^2\langle x, x\rangle - \langle y, y\rangle\langle y, x\rangle\langle x, y\rangle - \langle x, y\rangle\langle y, y\rangle\langle y, x\rangle + \langle x, y\rangle\langle y, x \\ &= 0\end{aligned}$$

⟨1⟩4. If x and y are linearly dependent then $|\langle x, y\rangle| = \|x\|\|y\|$
  ⟨2⟩1. Assume: x and y are linearly dependent.
  ⟨2⟩2. Let: $y = \alpha x$
  ⟨2⟩3. $|\langle x, y\rangle| = \|x\|\|y\|$
    Proof:

$$\begin{aligned}|\langle x, y\rangle| &= |\langle x, \alpha x\rangle| \\ &= |\alpha||\langle x, x\rangle| \\ &= |\alpha|\|x\|^2 \\ &= \|x\|\|\alpha x\| \\ &= \|x\|\|y\|\end{aligned}$$

□

Corollary 14.0.11.1 (Triangle Inequality)**.** *In any inner product space,*

$$\|x + y\| \leq \|x\| + \|y\|$$

Proof:

$$\begin{aligned}
\|x+y\|^2 &= \langle x+y, x+y\rangle \\
&= \langle x,x\rangle + \langle x,y\rangle + \langle y,x\rangle + \langle y,y\rangle \\
&\leq \langle x,x\rangle + 2|\langle x,y\rangle| + \langle y,y\rangle \\
&\leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 && \text{(Schwarz's Inequality)} \\
&= (\|x\| + \|y\|)^2
\end{aligned}$$

□

Corollary 14.0.11.2. *The norm in an inner product space is a norm.*

Theorem 14.0.12 (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 $\langle 1\rangle 2$.
□

Proposition 14.0.13. *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 14.0.14 (Orthogonal)**.** Vectors x and y in an inner product space are *orthogonal*, $x \perp y$, iff $\langle x,y\rangle = 0$.

Theorem 14.0.15 (Pythagorean Formula)**.** *If x and y are orthogonal then*

$$\|x+y\|^2 = \|x\|^2 + \|y\|^2 \ .$$

Definition 14.0.16 (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, $x_n \stackrel{w}{\to} l$ as $n \to \infty$, iff $\forall y \in E.\langle x_n, y\rangle \to \langle l, y\rangle$ as $n \to \infty$.

Proposition 14.0.17. *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:

$$\begin{aligned}
|\langle x_n, y_n\rangle - \langle x,y\rangle| &\leq |\langle x_n,y_n\rangle - \langle x_n,y\rangle| + |\langle x_n,y\rangle - \langle x,y\rangle| \\
&= |\langle x_n, y_n - y\rangle| + |\langle x_n - x, y\rangle| \\
&\leq \|x_n\|\|y_n - y\| + \|x_n - x\|\|y\| && \text{(Schwarz's Inequality)} \\
&\to 0
\end{aligned}$$

using the fact that (x_n) is bounded.

□

Theorem 14.0.18. *$x_n \to l$ if and only if $x_n \stackrel{w}{\to} l$ and $\|x_n\| \to \|x\|$.*

PROOF:
⟨1⟩1. If $x_n \to l$ then $x_n \stackrel{w}{\to} l$ and $\|x_n\| \to \|l\|$.
PROOF: Easy using the fact that the inner product is continuous.
⟨1⟩2. If $x_n \stackrel{w}{\to} l$ and $\|x_n\| \to \|l\|$ then $x_n \to l$.
⟨2⟩1. ASSUME: $x_n \stackrel{w}{\to} l$ and $\|x_n\| \to \|l\|$
⟨2⟩2. $\langle x_n, l\rangle \to \|l\|^2$
⟨2⟩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 14.0.19. *Let S be a subset of an inner product space E such that $\operatorname{span} S$ 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 $x_n \stackrel{w}{\to} x$.*

PROOF:
⟨1⟩1. For all $y \in \operatorname{span} S$, we have $\langle x_n, y\rangle \to \langle x, y\rangle$
⟨1⟩2. LET: $z \in E$
PROVE: $\langle x_n, z\rangle \to \langle x, z\rangle$
⟨1⟩3. LET: $\epsilon > 0$
PROVE: There exists n_0 such that $\forall n \geq n_0 . |\langle x_n, z\rangle - \langle x, z\rangle| < \epsilon$
⟨1⟩4. PICK $M > 0$ such that $\|x\| \leq M$ and $\forall n \in \mathbb{Z}_+ . \|x_n\| \leq M$.
⟨1⟩5. PICK $y_0 \in \operatorname{span} S$ such that $\|z - y_0\| < \epsilon/3M$
⟨1⟩6. PICK $n_0 \in \mathbb{Z}_+$ such that, for all $n \geq n_0$, we have $|\langle x_n, y_0\rangle - \langle x, y_0\rangle| < \epsilon/3$
⟨1⟩7. LET: $n \geq n_0$
⟨1⟩8. $|\langle x_n, z\rangle - \langle x, z\rangle| < \epsilon$
PROOF:

$$\begin{aligned}|\langle x_n, z\rangle - \langle x, z\rangle| &\leq |\langle x_n, z\rangle - \langle x_n, y_0\rangle| + |\langle x_n, y_0\rangle - \langle x, y_0\rangle| + |\langle x, y_0\rangle - \langle x, z\rangle| \\ &< \|x_n\|\|z - y_0\| + \epsilon/3 + \|x\|\|y_0 - z\| \\ &< M(\epsilon/3M) + \epsilon/3 + M(\epsilon/3M) \\ &= \epsilon\end{aligned}$$

□

14.1 Orthonormal Bases

Definition 14.1.1 (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 14.1.2 (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 14.1.3. *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:

$$\begin{aligned} 0 &= \sum_{m=1}^{n} \langle 0, \alpha_m e_m \rangle \\ &= \sum_{m=1}^{n} \langle \sum_{k=1}^{n} \alpha_k e_k, \alpha_m e_m \rangle \\ &= \sum_{m=1}^{n} \sum_{k=1}^{n} \alpha_k \overline{\alpha_m} \langle e_k, e_m \rangle \\ &= \sum_{k=1}^{n} |\alpha_k|^2 \end{aligned}$$

$\langle 1 \rangle 4$. $\alpha_1 = \cdots = \alpha_n = 0$
□

Proposition 14.1.4. *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 14.1.5. *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 14.1.6 (Legendre Polynomials)**.** The *Legendre polynomials $P_n \in \mathbb{Q}[x]$* for $n \in \mathbb{N}$ are defined by

$$\begin{aligned} P_0 &= 1 \\ P_n &= \frac{1}{2^n n!} \frac{d^n}{dx^n} (x^2 - 1)^n \end{aligned}$$

Proposition 14.1.7. *Let P_n be the nth Legendre polynomial. Then $\{P_n \mid n \in \mathbb{N}\}$ is orthogonal in $L^2([-1, 1])$.*

Definition 14.1.8 (Hermite Polynomial)**.** The *Hermite polynomials $H_n \in \mathbb{R}[x]$* for $n \in \mathbb{N}$ are defined by

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2} \quad .$$

Proposition 14.1.9. *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 14.1.10. *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 14.1.11 (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:

$$\begin{aligned}
\left\| x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\|^2 &= \left\langle x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k, x - \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\rangle \\
&= \langle x, x \rangle - \left\langle x, \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\rangle - \left\langle \sum_{k=1}^{n} \langle x, x_k \rangle x_k, x \right\rangle \\
&+ \left\langle \sum_{k=1}^{n} \langle x, x_k \rangle x_k, \sum_{k=1}^{n} \langle x, x_k \rangle x_k \right\rangle \\
&= \langle x, x \rangle - 2 \sum_{k=1}^{n} \langle x, x_k \rangle \langle x_k, x \rangle + \sum_{i=1}^{n} \sum_{j=1}^{n} \langle x, x_i \rangle \langle x_j, x \rangle \langle x_i, x_j \rangle \\
&= \|x\|^2 - 2 \sum_{k=1}^{n} |\langle x, x_k \rangle|^2 + \sum_{i=1}^{n} \langle x, x_i \rangle \langle x_i, x \rangle \\
&= \|x\|^2 - \sum_{k=1}^{n} |\langle x, x_k \rangle|^2
\end{aligned}$$

□

Corollary 14.1.11.1 (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 14.1.11.2. *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 $k \to \infty$. □

Corollary 14.1.11.3 (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* n*th* generalized Fourier coefficient *of* x *with respect to* (e_n)*. We have* $(\langle x, e_n \rangle e_n)_n \in l^2$*.*

Definition 14.1.12 (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

$$\sum_{n=1}^{\infty} \langle x, x_n \rangle x_n = x \quad .$$

Chapter 15

Hilbert Spaces

Definition 15.0.1 (Hilbert Space)**.** A *Hilbert space* is a complete inner product space.

Proposition 15.0.2. *For $n \in \mathbb{N}$, $\mathbb{C}^n$ is a Hilbert space.*

Proposition 15.0.3. *l^2 is a Hilbert space.*

Proposition 15.0.4. *$L^2(\mathbb{R})$ is a Hilbert space.*

Proposition 15.0.5. *$L^2([a,b])$ is a Hilbert space.*

Proposition 15.0.6. *Let ρ 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 15.0.7. *Let m and N be positive integers. Let Ω 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 15.0.8. *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 $\|f_n\| \leq M$.
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: $n \in \mathbb{Z}_+$
$\langle 2\rangle 2$. $\|f_n\| \leq \|x_n\|$
PROOF: Since for all $x \in H$ we have $|f_n(x)| = |\langle x, x_n\rangle| \leq \|x\|\|x_n\|$ by Schwarz's Inequality.
$\langle 2\rangle 3$. $\|x_n\| \leq \|f_n\|$
PROOF: Since $\|x_n\|^2 = |\langle x_n, x_n\rangle| = |f_n(x_n)| \leq \|f_n\|\|x_n\|$.
$\langle 1\rangle 8$. $\forall n \in \mathbb{Z}_+ . \|x_n\| \leq M$
PROOF: $\langle 1\rangle 6$, $\langle 1\rangle 7$
□

Theorem 15.0.9. *Let H be a Hilbert space. Let (x_n) be an orthonormal sequence in H and let (α_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*

$$\left\| \sum_{n=1}^{\infty} \alpha_n x_n \right\|^2 = \sum_{n=1}^{\infty} |\alpha_n|^2 \quad .$$

PROOF:
$\langle 1\rangle 1$. For $m > k > 0$ we have

$$\left\| \sum_{n=k}^{m} \alpha_n x_n \right\|^2 = \sum_{n=k}^{m} |\alpha_n|^2 \quad .$$

PROOF: Theorem 14.1.10.
$\langle 1\rangle 2$. 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

$$\left\| \sum_{n=1}^{\infty} \alpha_n x_n \right\|^2 = \sum_{n=1}^{\infty} |\alpha_n|^2 \quad .$$

PROOF: From ⟨1⟩1.
□

Proposition 15.0.10. *Every complete orthonormal sequence in a Hilbert space is a basis.*

PROOF:
⟨1⟩1. LET: E be an inner product space.
⟨1⟩2. LET: (e_n) be a complete orthonormal sequence in E.
⟨1⟩3. For all $x \in E$, there exists a sequence (α_n) in $\mathbb{C}$ such that $x = \sum_n \alpha_n e_n$.
PROOF: Immediate from ⟨1⟩2.
⟨1⟩4. If $\sum_n \alpha_n e_n = \sum_n \beta_n e_n$ then $\alpha_n = \beta_n$ for all n.
⟨2⟩1. LET: $x = \sum_n \alpha_n e_n = \sum_n \beta_n e_n$
⟨2⟩2. $\sum_n |\alpha_n - \beta_n|^2 = 0$
PROOF:

$$\begin{aligned} 0 &= \|x - x\|^2 \\ &= \left\| \sum_{n=1}^{\infty} \alpha_n e_n - \sum_{n=1}^{\infty} \beta_n e_n \right\|^2 && (\langle 2\rangle 1) \\ &= \left\| \sum_{n=1}^{\infty} (\alpha_n - \beta_n) e_n \right\|^2 \\ &= \sum_{n=1}^{\infty} |\alpha_n - \beta_n|^2 && \text{(Theorem 15.0.9)} \end{aligned}$$

⟨2⟩3. $\alpha_n = \beta_n$ for all n.
□

Theorem 15.0.11. *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:
⟨1⟩1. If (x_n) is complete then, for all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$ then $x = 0$.
⟨2⟩1. ASSUME: (x_n) is complete.
⟨2⟩2. LET: $x \in H$
⟨2⟩3. ASSUME: $\forall n. \langle x, x_n \rangle = 0$
⟨2⟩4. $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n = 0$
⟨1⟩2. If, for all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$ then $x = 0$, then (x_n) is complete.
⟨2⟩1. ASSUME: For all $x \in H$, if $\forall n. \langle x, x_n \rangle = 0$, then $x = 0$.
⟨2⟩2. LET: $y = x - \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$
⟨2⟩3. For all n, $\langle y, x_n \rangle = 0$
⟨3⟩1. LET: $n \in \mathbb{Z}_+$
⟨3⟩2. $\langle y, x_n \rangle = 0$

PROOF:

$$\begin{aligned}\langle y, x_n \rangle &= \left\langle x - \sum_{m=1}^{\infty} \langle x, x_m \rangle x_m, x_n \right\rangle \\ &= \langle x, x_n \rangle - \sum_{m=1}^{\infty} \langle x, x_m \rangle \langle x_m, x_n \rangle \\ &= \langle x, x_n \rangle - \langle x, x_n \rangle \\ &= 0\end{aligned}$$

⟨2⟩4. $y = 0$
⟨2⟩5. $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

□

Theorem 15.0.12 (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 $x \in H$,*

$$\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2 \enspace .$$

PROOF:
⟨1⟩1. If (x_n) is complete then for all $x \in H$ we have $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$.
⟨2⟩1. ASSUME: (x_n) is complete.
⟨2⟩2. LET: $x \in H$
⟨2⟩3. $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$
PROOF:

$$\begin{aligned}\|x\|^2 &= \left\| \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n \right\|^2 && (\langle 2 \rangle 1) \\ &= \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2 && (\text{Theorem 15.0.9})\end{aligned}$$

⟨1⟩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.
⟨2⟩1. ASSUME: For all $x \in H$, we have $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$
⟨2⟩2. LET: $x \in H$
⟨2⟩3. $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

□

Proposition 15.0.13. *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 15.0.14. $B = \{1/\sqrt{2\pi}\} \cup \{\cos nx/\sqrt{\pi} \mid n \in \mathbb{Z}_+\} \cup \{\sin nx/\sqrt{\pi} \mid n \in \mathbb{Z}_+\}$ *is a complete orthonormal set in $L^2([-\pi, \pi])$.*

PROOF:
⟨1⟩1. For all $f \in B$ we have $\|f\| = 1$
⟨2⟩1. $\|1/\sqrt{2\pi}\| = 1$

PROOF:

$$\begin{aligned}\|1/\sqrt{2\pi}\| &= \int_{-\pi}^{\pi} dx/2\pi \\ &= 1\end{aligned}$$

⟨2⟩2. For all $n \in \mathbb{Z}_+$ we have $\|\cos nx/\sqrt{\pi}\| = 1$

PROOF:

$$\begin{aligned}\|\cos nx/\sqrt{\pi}\| &= 1/\pi \int_{-\pi}^{\pi} \cos^2 nx\, dx \\ &= 1/2\pi \int_{-\pi}^{\pi} (\cos 2nx + 1) dx \\ &= 1/2\pi \left[1/2n \sin 2nx + x\right]_{-\pi}^{\pi} \\ &= (1/2\pi)(2\pi) \\ &= 1\end{aligned}$$

⟨2⟩3. For all $n \in \mathbb{Z}_+$ we have $\|\sin nx/\sqrt{\pi}\| = 1$

PROOF:

$$\begin{aligned}\|\sin nx/\sqrt{\pi}\| &= 1/\pi \int_{-\pi}^{\pi} \sin^2 nx\, dx \\ &= -1/2\pi \int_{-\pi}^{\pi} (\cos 2nx - 1) dx \\ &= -1/2\pi \left[1/2n \sin 2nx - x\right]_{-\pi}^{\pi} \\ &= (-1/2\pi)(-2\pi) \\ &= 1\end{aligned}$$

⟨1⟩2. For all $f, g \in B$ with $f \neq g$ we have $\langle f, g\rangle = 0$

⟨2⟩1. $\langle 1, \cos nx\rangle = 0$

PROOF:

$$\begin{aligned}\int_{-\pi}^{\pi} \cos nx\, dx &= \left[1/n \sin nx\right]_{-\pi}^{\pi} \\ &= 0\end{aligned}$$

⟨2⟩2. $\langle 1, \sin nx\rangle = 0$

PROOF:

$$\begin{aligned}\int_{-\pi}^{\pi} \sin nx\, dx &= \left[-1/n \cos nx\right]_{-\pi}^{\pi} \\ &= -1/n \cos n\pi + 1/n \cos n\pi \\ &= 0\end{aligned}$$

⟨2⟩3. If $m \neq n$ then $\langle \cos mx, \cos nx\rangle = 0$

PROOF:

$$\begin{aligned}\int_{-\pi}^{\pi} \cos mx \cos nx\, dx &= 1/2 \int_{-\pi}^{\pi} (\cos(n+m)x - \cos(n-m)x) dx \\ &= 1/2 \left[\frac{1}{n+m} \sin(n+m)x - \frac{1}{n-m} \sin(n-m)x\right]_{-\pi}^{\pi} \\ &= 0\end{aligned}$$

⟨2⟩4. $\langle \cos mx, \sin nx\rangle = 0$

PROOF:
$$\begin{aligned}\int_{-\pi}^{\pi} \cos mx \sin nx \, dx &= 1/2 \int_{-\pi}^{\pi} (\sin(n+m)x - \sin(n-m)x) dx \\ &= 1/2 \left[-\frac{1}{n+m} \cos(n+m)x + \frac{1}{n-m} \cos(n-m)x \right]_{-\pi}^{\pi} \\ &= 0 \qquad \text{(cos is odd)}\end{aligned}$$

⟨2⟩5. If $m \neq n$ then $\langle \sin mx, \sin nx \rangle = 0$

PROOF:
$$\begin{aligned}\int_{-\pi}^{\pi} \sin mx \sin nx \, dx &= 1/2 \int_{-\pi}^{\pi} (\cos(n-m)x - \cos(n+m)x) dx \\ &= 1/2 \left[\frac{1}{n-m} \sin(n-m)x - \frac{1}{n+m} \sin(n+m)x \right]_{-\pi}^{\pi} \\ &= 0\end{aligned}$$

⟨1⟩3. For all $f \in L^2([-\pi, \pi])$, if $\forall g \in B. \langle f, g \rangle = 0$ then $f = 0$

⟨2⟩1. LET: $f \in L^2([-\pi, \pi])$

⟨2⟩2. ASSUME: $\forall g \in B. \langle f, g \rangle = 0$

⟨2⟩3. For all $n \in \mathbb{Z}$, $\langle f, e^{inx} \rangle = 0$

PROOF: Since $e^{inx} = \cos nx + i \sin nx$.

⟨2⟩4. $f = 0$

PROOF: From Proposition 15.0.13.

□

Proposition 15.0.15. $\{\frac{1}{\sqrt{\pi}}\} \cup \{\sqrt{\frac{2}{\pi}} \cos nx \mid n \in \mathbb{Z}_+\}$ *is a complete orthonormal set in* $L^2([0, \pi])$.

Proposition 15.0.16. $\{\sqrt{\frac{2}{\pi}} \sin nx \mid n \in \mathbb{Z}_+\}$ *is a complete orthonormal set in* $L^2([0, \pi])$.

Definition 15.0.17 (Signum)**.** The *signum* function $\operatorname{sgn} : \mathbb{R} \to \mathbb{R}$ is defined by

$$\operatorname{sgn} x = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

Definition 15.0.18 (Rademacher Functions)**.** The *Rademarcher functions* $R : \mathbb{N} \times [0, 1] \to \{-1, 0, 1\}$ are defined by

$$R(m, x) = \operatorname{sgn}(\sin(2^m \pi x)) \ .$$

Proposition 15.0.19. *The Rademacher functios* $\{R(m, -) \mid m \in \mathbb{N}\}$ *are orthonormal in* $L^2([0, 1])$.

PROOF:

⟨1⟩1. $\forall m \in \mathbb{N}. \|R(m, -)\| = 1$

PROOF: $\int_0^1 \operatorname{sgn}(\sin(2^m \pi x))^2 dx = 1$ 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:

$$\begin{aligned}\int_0^1 R(m,x)R(n,x)dx &= \sum_{k=1}^{2^n} \int_{\frac{k-1}{2^n}}^{\frac{k}{2^n}} R(m,x)R(n,x)dx \\ &= \sum_{k=1}^{2^n} (-i)^{k+1} \int_{\frac{k-1}{2^n}}^{\frac{k}{2^n}} R(m,x)dx \\ &= 0 && \left(\langle 2\rangle 1, 2^m\left(\frac{k}{2^n} - \frac{k-1}{2^n}\right) = 2^{m-n} \text{ is an even integer}\right)\end{aligned}$$

∎

Proposition 15.0.20. *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. $f \neq 1/2R(0,-)$

∎

Definition 15.0.21 (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

$$W(m,x) = \prod_{k=1}^n R(k,x)^{a_k} \quad .$$

Proposition 15.0.22. *The set of Walsh functions $\{W(m,-) \mid m \in \mathbb{N}\}$ is a compete orthonormal set.*

TODO