

Mathematics

Robin Adams

August 16, 2023

Contents

1	Sets and Classes	7
1.1	Classes	7
1.1.1	Subclasses	8
1.1.2	Constructions of Classes	8
1.2	Sets and the Axiom of Extensionality	9
1.3	The Other Axioms	9
1.4	ZFC Extends Z	12
1.5	Consequences of the Axioms	13
1.6	Transitive Classes	15
2	Relations	19
2.1	Ordered Pairs	19
2.2	Relations	20
2.2.1	Identity Functions	21
2.2.2	Inverses	21
2.2.3	Composition	21
2.2.4	Properties of Relations	21
2.3	n-ary Relations	23
2.4	Well Founded Relations	23
3	Functions	27
3.1	Functions	27
3.1.1	Injective Functions	29
3.1.2	Surjective Functions	29
3.1.3	Bijections	30
3.1.4	Restrictions	31
3.1.5	Images	31
3.1.6	Inverse Images	34
3.1.7	Function Sets	35
3.2	Equinumerosity	35
3.3	Domination	36
3.4	Transfinite Recursion	36

4	Category Theory	39
4.1	Categories	39
4.2	Invertible Morphisms	40
5	Equivalence Relations	41
6	Ordering Relations	45
6.1	Partial Orders	45
6.2	Linear Orders	50
6.3	Well Orderings	53
7	Ordinal Numbers	57
7.1	Ordinals	57
7.2	Natural Numbers	67
7.3	Transitive Closure of a Set	68
7.4	The Well-Ordering Theorem and Zorn's Lemma	70
7.5	Ordinal Operations	73
7.6	Ordinal Arithmetic	76
7.6.1	Addition	76
7.6.2	Multiplication	79
7.6.3	Exponentiation	81
7.7	Sequences	84
7.8	Strict Supremum	84
8	Cardinal Numbers	85
8.1	Cardinal Numbers	85
8.2	Ordering on Cardinal Numbers	88
9	Natural Numbers	91
9.1	Inductive Sets	91
9.2	Cardinality	93
9.3	Countable Sets	95
9.4	Arithmetic	95
9.5	Sequences	97
9.6	Transitive Closure of a Set	97
9.7	The Veblen Fixed Point Theorem	98
9.8	Cantor Normal Form	100
10	The Cumulative Hierarchy	101
11	Models of Set Theory	105
12	Infinite Cardinals	109
12.1	Arithmetic of Infinite Cardinals	109
12.2	Alephs	111
12.3	Beths	111
12.4	Cofinality	112

12.5 Inaccessible Cardinals	116
13 Group Theory	119
13.1 Groups	119
13.2 Abelian Groups	120
14 Ring Theory	121
14.1 Rings	121
14.2 Ordered Rings	121
14.3 Integral Domains	122
15 Field Theory	123
15.1 Fields	123
15.2 Ordered Fields	126
16 Number Systems	131
16.1 The Integers	131
16.2 The Rationals	135
16.3 The Real Numbers	138
17 Real Analysis	153
17.1 Step Functions	153
17.2 Lebesgue Integration	157
18 Complex Analysis	159
19 Topology	163
19.1 Topological Spaces	163
19.2 Continuous Functions	164
19.3 Convergence	164
19.4 Homotopy	165
19.5 Metric Spaces	165
20 Ring Theory	167
21 Linear Algebra	169
21.1 Vector Spaces	169
21.2 Subspaces	170
21.3 Linear Transformations	172
21.4 Normed Spaces	173
21.4.1 Functionals	187
21.4.2 Contraction Mappings	187
21.5 Banach Spaces	187
21.6 Inner Product Spaces	198

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 $\forall x(x \in a \rightarrow \phi)$, and $\exists x \in a. \phi$ as an abbreviation for $\exists x(x \in a \wedge \phi)$.

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

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

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

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

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

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

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

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

If $\mathbf{A} = \mathbf{B}$ then $\mathbf{B} = \mathbf{A}$.

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

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

If $\mathbf{A} = \mathbf{B}$ and $\mathbf{B} = \mathbf{C}$ then $\mathbf{A} = \mathbf{C}$.

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

1.1.1 Subclasses

Definition 1.1.4 (Subclass). We say a class \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 $\mathbf{A} \not\subseteq \mathbf{B}$ or $\mathbf{B} \not\supseteq \mathbf{A}$.

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 $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{A} \neq \mathbf{B}$.

Proposition Schema 1.1.5. *For any class \mathbf{A} , the following is a theorem.*

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

PROOF: Every element of \mathbf{A} is an element of \mathbf{A} . \square

Proposition Schema 1.1.6. *For any classes \mathbf{A} and \mathbf{B} , the following is a theorem.*

If $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{B} \subseteq \mathbf{A}$ then $\mathbf{A} = \mathbf{B}$.

PROOF: If every element of \mathbf{A} is an element of \mathbf{B} , and every element of \mathbf{B} is an element of \mathbf{A} , then \mathbf{A} and \mathbf{B} have exactly the same elements. \square

Proposition Schema 1.1.7. *For any classes \mathbf{A} , \mathbf{B} and \mathbf{C} , the following is a theorem.*

If $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{B} \subseteq \mathbf{C}$ then $\mathbf{A} \subseteq \mathbf{C}$.

PROOF: If every element of \mathbf{A} is an element of \mathbf{B} and every element of \mathbf{B} is an element of \mathbf{C} then every element of \mathbf{A} is an element of \mathbf{C} . \square

1.1.2 Constructions of Classes

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

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

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

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

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

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

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

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

1.2 Sets and the Axiom of Extensionality

Definition 1.2.1 (Axiom of Extensionality). The *Axiom of Extensionality* is the statement: if two sets have exactly the same members, then they are equal.

$$\forall x, y (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y) .$$

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

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

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

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

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

1.3 The Other Axioms

Definition 1.3.1 (Empty Set Axiom). The *Empty Set Axiom* is the statement: The empty class \emptyset is a set.

$$\exists e \forall x x \notin e$$

Definition 1.3.2 (Pairing Axiom). The *Pairing Axiom* or *Pair Set Axiom* is the statement: for any sets a and b , the class $\{a, b\}$ is a set.

$$\forall a \forall b \exists c \forall x (x \in c \Leftrightarrow x = a \vee x = b)$$

Definition 1.3.3 (Union Axiom). The *Union Axiom* is the statement: for any set A , the class $\bigcup A$ is a set.

$$\forall A \exists B \forall x (x \in B \Leftrightarrow \exists y (y \in A \wedge x \in y))$$

Definition 1.3.4 (Comprehension Axiom Scheme). The *Comprehension Axiom Scheme*, *Subset Axiom Scheme* or *Aussonderungsaxiom Scheme* is the set of sentences of the form, for any class \mathbf{A} : If \mathbf{A} is a subclass of a set then \mathbf{A} is a set.

That is, for any property $P[x, y_1, \dots, y_n]$:

For any sets a_1, \dots, a_n and B , the class $\{x \in B \mid P[x, a_1, \dots, a_n]\}$ is a set.

$$\forall a_1, \dots, a_n, B. \exists C. \forall x (x \in C \Leftrightarrow x \in B \wedge P[x, a_1, \dots, a_n])$$

Definition 1.3.5 (Replacement Axiom Scheme). The *Replacement Axiom Scheme* is the set of sentences of the form, for some property $P[x, y, z_1, \dots, z_n]$:

For any sets a_1, \dots, a_n, B , assume for all $x \in B$ there exists at most one y such that $P[x, y, a_1, \dots, a_n]$. Then $\{y \mid \exists x \in B. P[x, y, a_1, \dots, a_n]\}$ is a set.

$$\forall a_1, \dots, a_n, B (\forall x \in B. \forall y, y' (P[x, y, a_1, \dots, a_n] \wedge P[x, y', a_1, \dots, a_n] \Rightarrow y = y') \Rightarrow \\ \exists C \forall y (y \in C \Leftrightarrow \exists x \in B. P[x, y, a_1, \dots, a_n]))$$

Definition 1.3.6 (Power Set Axiom). The *Power Set Axiom* is the statement: the power class of a set is a set.

$$\forall A \exists B \forall x (x \in B \Leftrightarrow \forall y (y \in x \Rightarrow y \in A))$$

Definition 1.3.7 (Axiom of Infinity). The *Axiom of Infinity* is the statement: there exists a set I such that $\emptyset \in I$ and $\forall x \in I. x \cup \{x\} \in I$.

$$\exists I (\emptyset \in I. \forall x. x \notin e \wedge \forall x \in I. \exists y \in I. \forall z (z \in y \Leftrightarrow z \in x \vee z = x))$$

Definition 1.3.8 (Axiom of Choice). The *Axiom of Choice* is the statement: For any set A of pairwise disjoint, nonempty sets, there exists a set C such that, for all $x \in A$, we have $x \cap C$ has exactly one element.

$$\forall A (\forall x \in A. \exists y y \in x \wedge \\ \forall x, y \in A. \forall z (z \in x \wedge z \in y \Rightarrow x = y) \Rightarrow \\ \exists C. \forall x \in A. \exists y \forall z (z \in x \wedge z \in C \Leftrightarrow z = y))$$

Definition 1.3.9 (Axiom of Regularity). The *Axiom of Regularity* or *Axiom of Foundation* is the statement: for any A , if A has a member, then there exists $m \in A$ such that $m \cap A = \emptyset$.

$$\forall A (\exists x. x \in A \Rightarrow \exists m \in A. \neg \exists x (x \in m \wedge x \in A))$$

Definition 1.3.10 (Skolem Set Theory). *Skolem set theory* (S) is the theory whose axioms are:

- Extensionality
- Empty Set
- Pairing
- Union
- Comprehension
- Power Set

- Regularity

Let SC be the extension of S with the Axiom of Choice.

Definition 1.3.11 (Skolem-Fraenkel Set Theory). *Skolem-Fraenkel set theory* (SF) is the theory whose axioms are:

- Extensionality
- Empty Set
- Union
- Replacement
- Power Set
- Regularity

Let SFC be the extension of SF with the Axiom of Choice.

Definition 1.3.12 (Zermelo Set Theory). *Zermelo set theory* is the theory whose axioms are:

- Extensionality
- Pairing
- Union
- Comprehension
- Power Set
- Infinity
- Regularity

We label theorems with Z when they are provable in Zermelo set theory.

Let ZC be the extension of Z with the Axiom of Choice.

Definition 1.3.13 (Fraenkel-Mostowski Set Theory). *Fraenkel-Mostowski set theory* (FM) is the theory whose axioms are:

- The *Axiom of Extensionality with Urelements*: For any sets x and y , if x is nonempty and x and y have exactly the same elements, then $x = y$.
- Union
- Replacement
- Power Set
- Infinity

- Regularity

We write FMC for the extension of FM with Choice.

Definition 1.3.14 (Zermelo-Fraenkel Set Theory). *Zermelo-Fraenkel set theory* is the theory whose axioms are:

- Extensionality
- Union
- Replacement
- Power Set
- Infinity
- Regularity

We label theorems with ZF when they are provable in Zermelo-Fraenkel set theory.

Let ZFC be the extension of ZF with the Axiom of Choice.

We label a theorem with FOL if it can be proved in first-order logic, i.e. from no axioms.

1.4 ZFC Extends Z

Proposition 1.4.1. *The Axiom of Infinity implies the Empty Set Axiom.*

PROOF: Trivial. \square

Corollary 1.4.1.1. *Z is an extension of S.*

ZF is an extension of SF.

ZC is an extension of SC.

ZFC is an extension of SFC.

Proposition 1.4.2. *The Axiom of Pairing is a theorem of SF without Foundation.*

PROOF:

$\langle 1 \rangle 1$. LET: a, b be sets.

$\langle 1 \rangle 2$. LET: $P(x, y)$ be the predicate $(x = \emptyset \wedge y = a) \vee (x = \mathcal{P}\emptyset \wedge y = b)$.

$\langle 1 \rangle 3$. 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 $\emptyset \notin \emptyset$.

$\langle 2 \rangle 7$. $y = y'$

$\langle 1 \rangle 4$. LET: A be the set $\{y \mid \exists x \in \mathcal{P}\mathcal{P}\emptyset. P(x, y)\}$.

$\langle 1 \rangle 5$. $A = \{a, b\}$

□

Proposition Schema 1.4.3. *Every instance of the Comprehension Axiom Scheme is a theorem of SF.*

PROOF:

$\langle 1 \rangle 1$. LET: $P(x)$ be a predicate.

$\langle 1 \rangle 2$. LET: A be a set.

$\langle 1 \rangle 3$. LET: $Q(x, y)$ be the predicate $P(x) \wedge y = x$.

$\langle 1 \rangle 4$. 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 $\langle 2 \rangle 4$.

$\langle 1 \rangle 5$. 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 $\langle 1 \rangle 4$.

$\langle 1 \rangle 6$. $B = \{y \in A \mid P(y)\}$

PROOF:

$$y \in B \Leftrightarrow \exists x \in A. Q(x, y) \quad (\langle 1 \rangle 5)$$

$$\Leftrightarrow \exists x \in A. (P(x) \wedge y = x) \quad (\langle 1 \rangle 3)$$

$$\Leftrightarrow P(y)$$

□

Corollary 1.4.3.1. *SF without Foundation is an extension of S without Foundation.*

SFC without Foundation is an extension of SC without Foundation.

ZF without Foundation is an extension of Z without Foundation.

ZFC without Foundation is an extension of ZC without Foundation.

SF is an extension of S.

SFC is an extension of SC.

ZF is an extension of Z.

ZFC is an extension of ZC.

1.5 Consequences of the Axioms

Proposition 1.5.1 (S without Foundation). *The union of two sets is a set.*

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

Proposition Schema 1.5.2 (S without Foundation). *For any number n , the following is a theorem:*

For any sets a_1, \dots, a_n , the class $\{a_1, \dots, a_n\} = \{x \mid x = a_1 \vee \dots \vee x = a_n\}$ 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 $\{a_1, \dots, a_n, a_{n+1}\} = \{a_1, \dots, a_n\} \cup \{a_{n+1}\}$. \square

Proposition 1.5.3 (S). *No set is a member of itself.*

PROOF:

$\langle 1 \rangle 1$. LET: x be any set.

$\langle 1 \rangle 2$. PICK $m \in \{x\}$ such that $m \cap \{x\} = \emptyset$.

PROOF: Axiom of Foundation.

$\langle 1 \rangle 3$. $m = x$

$\langle 1 \rangle 4$. $x \cap \{x\} = \emptyset$

$\langle 1 \rangle 5$. $x \notin x$

\square

Theorem 1.5.4 (Russell's Paradox (S without Foundation)). *The universal class \mathbf{V} is a proper class.*

PROOF: If \mathbf{V} is a set then $R = \{x \in \mathbf{V} \mid x \notin x\}$ is a set. Then we have $R \in R$ if and only if $R \notin R$, which is a contradiction. \square

Proposition 1.5.5 (S). *There are no sets a and b such that $a \in b$ and $b \in a$.*

PROOF:

$\langle 1 \rangle 1$. LET: a and b be any sets.

$\langle 1 \rangle 2$. PICK $m \in \{a, b\}$ such that $m \cap \{a, b\} = \emptyset$

$\langle 1 \rangle 3$. CASE: $m = a$

PROOF: Then $b \notin a$.

$\langle 1 \rangle 4$. CASE: $m = b$

PROOF: Then $a \notin b$.

\square

Proposition 1.5.6 (S without Foundation). *The intersection of a set and a class is a set.*

PROOF: Immediate from Comprehension. \square

Proposition 1.5.7 (S without Foundation). *The relative complement of a class in a set is a set.*

PROOF: Immediate from Comprehension. \square

Corollary 1.5.7.1 (S without Foundation). *The symmetric difference of two sets is a set.*

Proposition 1.5.8 (S without Foundation). *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 $B \in \mathbf{A}$

$\langle 1 \rangle 3$. $\bigcap \mathbf{A} \subseteq B$

$\langle 1 \rangle 4$. $\bigcap \mathbf{A}$ is a set.

PROOF: By Comprehension.

□

Proposition Schema 1.5.9 (FOL). *For any classes \mathbf{A} and \mathbf{B} , the following is a theorem:*

If $\mathbf{A} \subseteq \mathbf{B}$ then $\mathcal{P}\mathbf{A} \subseteq \mathcal{P}\mathbf{B}$.

PROOF: Every subset of \mathbf{A} is a subset of \mathbf{B} . □

Proposition Schema 1.5.10 (FOL). *For any classes \mathbf{A} and \mathbf{B} , the following is a theorem:*

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

PROOF: If $x \in X \in \mathbf{A}$ then $x \in X \in \mathbf{B}$. □

Proposition Schema 1.5.11 (S without Foundation). *For any class \mathbf{A} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1$. $\mathbf{A} \subseteq \bigcup \mathcal{P}\mathbf{A}$

PROOF: For all $x \in \mathbf{A}$ we have $x \in \{x\} \in \mathcal{P}\mathbf{A}$.

$\langle 1 \rangle 2$. $\bigcup \mathcal{P}\mathbf{A} \subseteq \mathbf{A}$

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

$\langle 2 \rangle 2$. PICK $X \in \mathcal{P}\mathbf{A}$ such that $x \in X$

$\langle 2 \rangle 3$. $X \subseteq \mathbf{A}$

$\langle 2 \rangle 4$. $x \in \mathbf{A}$

□

1.6 Transitive Classes

Definition 1.6.1 (Transitive Class). A class \mathbf{A} is a *transitive class* iff whenever $x \in y \in \mathbf{A}$ then $x \in \mathbf{A}$.

Proposition Schema 1.6.2 (FOL). *For any class \mathbf{A} , the following is a theorem:*

The following are equivalent.

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

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

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

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

PROOF: Immediate from definitions. \square

Proposition Schema 1.6.3 (FOL). *For any class \mathbf{A} , the following is a theorem:*

If \mathbf{A} is a transitive class then $\bigcup \mathbf{A}$ is a transitive class.

PROOF:

$\langle 1 \rangle 1.$ ASSUME: \mathbf{A} is a transitive class.

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

$\langle 1 \rangle 3.$ $y \in \mathbf{A}$

PROOF: Since $\bigcup \mathbf{A} \subseteq \mathbf{A}$ by Proposition 1.6.2.

$\langle 1 \rangle 4.$ $x \in \bigcup \mathbf{A}$

\square

Proposition Schema 1.6.4 (S without Foundation). *For any class \mathbf{A} , the following is a theorem:*

We have \mathbf{A} is a transitive class if and only if $\mathcal{P}\mathbf{A}$ is a transitive class.

PROOF:

$\langle 1 \rangle 1.$ If \mathbf{A} is a transitive class then $\mathcal{P}\mathbf{A}$ is a transitive class.

$\langle 2 \rangle 1.$ ASSUME: \mathbf{A} is a transitive class.

$\langle 2 \rangle 2.$ $\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$

PROOF: Proposition 1.6.2.

$\langle 2 \rangle 3.$ $\mathcal{P}\mathbf{A} \subseteq \mathcal{P}\mathcal{P}\mathbf{A}$

PROOF: Proposition 1.5.9.

$\langle 2 \rangle 4.$ $\mathcal{P}\mathbf{A}$ is a transitive class.

PROOF: Proposition 1.6.2.

$\langle 1 \rangle 2.$ If $\mathcal{P}\mathbf{A}$ is a transitive class then \mathbf{A} is a transitive class.

$\langle 2 \rangle 1.$ ASSUME: $\mathcal{P}\mathbf{A}$ is a transitive class.

$\langle 2 \rangle 2.$ $\bigcup \mathcal{P}\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$

PROOF: Proposition 1.6.2.

$\langle 2 \rangle 3.$ $\mathbf{A} \subseteq \mathcal{P}\mathbf{A}$

PROOF: Proposition 1.5.11.

$\langle 2 \rangle 4.$ \mathbf{A} is a transitive class.

PROOF: Proposition 1.6.2.

\square

Proposition Schema 1.6.5 (FOL). *For any class \mathbf{A} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1.$ 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 $y \in A$.

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

PROOF: Since A is a transitive set.

$\langle 1 \rangle 5$. $x \in \bigcup \mathbf{A}$

□

Proposition Schema 1.6.6 (FOL). *For any class \mathbf{A} , the following is a theorem:*

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

PROOF:

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

$\langle 1 \rangle 4$. $y \in A$

$\langle 1 \rangle 5$. $x \in A$

PROOF: Since A is a transitive set.

□

Chapter 2

Relations

2.1 Ordered Pairs

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

Theorem 2.1.2 (S without Foundation). *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 (S without Foundation). *For any sets A and B , the class $A \times B$ is a set.*

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

Proposition Schema 2.1.5 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{C} , the following is a theorem:*

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

PROOF:

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

Proposition Schema 2.1.6 (S without Foundation). *For any classes \mathbf{A} and \mathbf{B} , the following is a theorem:*

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

PROOF:

- $\langle 1 \rangle 1$. PICK $a \in \mathbf{A}$
 $\langle 1 \rangle 2$. For all x we have $x \in \mathbf{B}$ iff $x \in \mathbf{C}$.

PROOF:

$$\begin{aligned} x \in \mathbf{B} &\Leftrightarrow (a, x) \in \mathbf{A} \times \mathbf{B} \\ &\Leftrightarrow (a, x) \in \mathbf{A} \times \mathbf{C} \\ &\Leftrightarrow x \in \mathbf{C} \end{aligned}$$

\square

Proposition Schema 2.1.7 (S without Foundation). *For any classes \mathbf{A} and \mathbf{B} , the following is a theorem:*

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

PROOF:

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

2.2 Relations

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

A *relation* \mathbf{R} between classes \mathbf{A} and \mathbf{B} is a subclass of $\mathbf{A} \times \mathbf{B}$.

A *(binary) relation on \mathbf{A}* is a relation between \mathbf{A} and \mathbf{A} .

We write $x\mathbf{R}y$ for $(x, y) \in \mathbf{R}$.

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

$$\text{dom } \mathbf{R} := \{x \mid \exists y. x\mathbf{R}y\} .$$

Proposition 2.2.3 (S without Foundation). *The domain of a set is a set.*

Definition 2.2.4 (Range). The *range* of a class \mathbf{R} is the class

$$\text{ran } \mathbf{R} := \{y \mid \exists x. x\mathbf{R}y\}$$

Proposition 2.2.5 (S without Foundation). *The range of a set is a set.*

2.2.1 Identity Functions

Definition 2.2.6 (Identity Function). For any class \mathbf{A} , the *identity function* or *diagonal relation* $\text{id}_{\mathbf{A}}$ on \mathbf{A} is

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

2.2.2 Inverses

Definition 2.2.7 (Inverse). The *inverse* of a relation \mathbf{R} between \mathbf{A} and \mathbf{B} is the relation \mathbf{R}^{-1} between \mathbf{B} and \mathbf{A} defined by

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

Proposition Schema 2.2.8 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{R} , the following is a theorem:*

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

PROOF:

$$\begin{aligned} x(\mathbf{R}^{-1})^{-1}y &\Leftrightarrow y\mathbf{R}^{-1}x \\ &\Leftrightarrow x\mathbf{R}y \end{aligned} \quad \square$$

2.2.3 Composition

Definition 2.2.9 (Composition). Let \mathbf{R} be a relation between \mathbf{A} and \mathbf{B} , and \mathbf{S} be a relation between \mathbf{B} and \mathbf{C} . The *composition* $\mathbf{S} \circ \mathbf{R}$ is the relation between \mathbf{A} and \mathbf{C} defined by

$$a(\mathbf{S} \circ \mathbf{R})c \Leftrightarrow \exists b(a\mathbf{R}b \wedge b\mathbf{S}c) .$$

Proposition Schema 2.2.10 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{R} and \mathbf{S} , the following is a theorem:*

If \mathbf{R} is a relation between \mathbf{A} and \mathbf{B} , and \mathbf{S} is a relation between \mathbf{B} and \mathbf{C} , then

$$(\mathbf{S} \circ \mathbf{R})^{-1} = \mathbf{R}^{-1} \circ \mathbf{S}^{-1} .$$

PROOF:

$$\begin{aligned} z(\mathbf{S} \circ \mathbf{R})^{-1}x &\Leftrightarrow x(\mathbf{S} \circ \mathbf{R})z \\ &\Leftrightarrow \exists y.(x\mathbf{R}y \wedge y\mathbf{S}z) \\ &\Leftrightarrow \exists y.(y\mathbf{R}^{-1}x \wedge z\mathbf{S}^{-1}y) \\ &\Leftrightarrow z(\mathbf{R}^{-1} \circ \mathbf{S}^{-1})x \end{aligned} \quad \square$$

2.2.4 Properties of Relations

Definition 2.2.11 (Reflexive). Let \mathbf{R} be a binary relation on \mathbf{A} . Then \mathbf{R} is *reflexive* on \mathbf{A} iff $\forall x \in \mathbf{A}.(x, x) \in \mathbf{R}$.

Proposition Schema 2.2.12 (S without Foundation). *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem:*

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

PROOF:

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

$\langle 1 \rangle 2.$ $x\mathbf{R}x$

PROOF: Since \mathbf{R} is reflexive.

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

□

Definition 2.2.13 (Irreflexive). A relation \mathbf{R} is *irreflexive* iff there is no x such that $(x, x) \in \mathbf{R}$.

Definition 2.2.14 (Symmetric). A relation \mathbf{R} is *symmetric* iff, whenever $x\mathbf{R}y$, then $y\mathbf{R}x$.

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

Proposition Schema 2.2.16 (S without Foundation). *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1.$ ASSUME: $x\mathbf{R}^{-1}y$ and $y\mathbf{R}^{-1}x$

$\langle 1 \rangle 2.$ $y\mathbf{R}x$ and $x\mathbf{R}y$

$\langle 1 \rangle 3.$ $x = y$

PROOF: Since \mathbf{R} is antisymmetric.

□

Definition 2.2.17 (Transitive). A relation \mathbf{R} is *transitive* iff, whenever $x\mathbf{R}y$ and $y\mathbf{R}z$, then $x\mathbf{R}z$.

Proposition Schema 2.2.18 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{R} , the following is a theorem:*

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

PROOF:

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

$\langle 1 \rangle 2.$ $(y, x), (z, y) \in \mathbf{R}$

$\langle 1 \rangle 3.$ $(z, x) \in \mathbf{R}$

$\langle 1 \rangle 4.$ $(x, z) \in \mathbf{R}^{-1}$

□

Proposition 2.2.19 (S without Foundation). *For any relation R on a set A , there exists a smallest transitive relation on A that includes R .*

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

Definition 2.2.20 (Transitive Closure). For any relation R on a set A , the *transitive closure* of R is the smallest transitive relation that includes R .

Definition 2.2.21 (Minimal). Let \mathbf{R} be a relation on \mathbf{A} . An element $m \in \mathbf{A}$ is *minimal* iff there is no $x \in \mathbf{A}$ such that $x\mathbf{R}m$.

Definition 2.2.22 (Maximal). Let \mathbf{R} be a relation on \mathbf{A} . An element $m \in \mathbf{A}$ is *maximal* iff there is no $x \in \mathbf{A}$ such that $m\mathbf{R}x$.

2.3 n-ary Relations

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

$$(a_1) := a_1$$

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

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 Well Founded Relations

Definition 2.4.1 (Well Founded). A relation \mathbf{R} is *well founded* iff:

- Every nonempty set has an \mathbf{R} -minimal element.
- For every set x , there exists a set u such that $x \subseteq u$ and, for all w, y , if $y \in u$ and $w\mathbf{R}y$ then $w \in u$.

Proposition Schema 2.4.2 (S without Foundation). *For any class \mathbf{R} , the following is a theorem:*

Assume \mathbf{R} is a well founded relation. For any set a , the class $\{x \mid x\mathbf{R}a\}$ is a set.

PROOF:

$\langle 1 \rangle 1$. PICK a set u such that $\{a\} \subseteq u$ and, for all w, y , if $y \in u$ and $w\mathbf{R}y$ then $w \in u$.

$\langle 1 \rangle 2$. $\{x \mid x\mathbf{R}a\} \subseteq u$

□

Proposition Schema 2.4.3 (S without Foundation). *For any classes \mathbf{A}, \mathbf{B} and \mathbf{R} , the following is a theorem:*

Assume \mathbf{R} is a well founded relation on \mathbf{A} and $\mathbf{B} \subseteq \mathbf{A}$ is nonempty. Then \mathbf{B} has an \mathbf{R} -minimal element.

PROOF:

$\langle 1 \rangle 1$. PICK $b \in \mathbf{B}$

$\langle 1 \rangle 2$. LET: $S = \{x \in \mathbf{B} \mid x\mathbf{R}b\}$

$\langle 1 \rangle 3$. CASE: $S = \emptyset$

PROOF: In this case b is an \mathbf{R} -minimal element of \mathbf{B} .

$\langle 1 \rangle 4$. CASE: $S \neq \emptyset$

PROOF: In this cases S has an \mathbf{R} -minimal element, which is an \mathbf{R} -minimal element of \mathbf{B} .

□

Proposition Schema 2.4.4 (FOL). *For any classes \mathbf{R} and \mathbf{S} , the following is a theorem:*

Assume \mathbf{R} is a relation. If \mathbf{S} is a well-founded relation and $\mathbf{R} \subseteq \mathbf{S}$ then \mathbf{R} is a well founded relation.

PROOF: Immediate from definitions. □

Theorem Schema 2.4.5 (Transfinite Induction Principle (S without Foundation)). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{R} , the following is a theorem:*

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

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

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

PROOF:

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

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

PROOF: Proposition 2.4.3.

$\langle 1 \rangle 3$. $\{x \in \mathbf{A} \mid x\mathbf{R}m\} \subseteq \mathbf{B}$

PROOF: By minimality of m .

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

$\langle 1 \rangle 5$. Q.E.D.

PROOF: This is a contradiction.

□

Theorem 2.4.6 (S without Foundation). *The transitive closure of a well founded relation on a set is well founded.*

PROOF:

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

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

$\langle 1 \rangle 3$. For any $x, y \in A$, if $xR^t y$ then there exists $z \in A$ such that zRy .

PROOF: $\{(x, y) \in A^2 \mid \exists z \in A. zRy\}$ is a transitive relation on A that includes R .

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

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

$\langle 1 \rangle 6$. b is R^t -minimal in B .

PROOF: If there exists x such that $xR^t b$ then there exists z such that zRb by $\langle 1 \rangle 3$.

□

Definition 2.4.7 (Initial Segment). Let \mathbf{R} be a relation on \mathbf{A} and $a \in \mathbf{A}$. The *initial segment* up to a is

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

Chapter 3

Functions

3.1 Functions

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

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

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

Proposition 3.1.3 (S without Foundation). *For any class \mathbf{A} , the following is a theorem:*

$$\text{id}_{\mathbf{A}} : \mathbf{A} \rightarrow \mathbf{A}$$

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

Proposition Schema 3.1.4 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{F} and \mathbf{G} , the following is a theorem:*

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

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

PROOF:

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

PROOF: Because $(x, \mathbf{F}(x)) \in \mathbf{F}$ and $(\mathbf{F}(x), \mathbf{G}(\mathbf{F}(x))) \in \mathbf{G}$.

$\langle 1 \rangle 2. \text{ If } (x, z) \in \mathbf{F} \circ \mathbf{G} \text{ then } z = \mathbf{G}(\mathbf{F}(x))$

$\langle 2 \rangle 1. \text{ PICK } y \in \mathbf{B} \text{ such that } x\mathbf{F}y \text{ and } y\mathbf{G}z$

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

$\langle 2 \rangle 3. z = \mathbf{G}(y)$

$\langle 2 \rangle 4. z = \mathbf{G}(\mathbf{F}(x))$

\square

Proposition 3.1.5 (SC without Foundation). *For any set A there exists a function $F : \mathcal{P}A - \{\emptyset\} \rightarrow A$ (a choice function for A) such that, for every nonempty $B \subseteq A$, we have $F(B) \in B$.*

PROOF:

$\langle 1 \rangle 1$. LET: A be a set.

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

$\langle 1 \rangle 3$. Every member of \mathcal{A} is nonempty.

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

$\langle 1 \rangle 5$. PICK a set C such that, for all $X \in \mathcal{A}$, we have $C \cap X$ is a singleton.

PROOF: Axiom of Choice.

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

$\langle 1 \rangle 7$. $F : \mathcal{P}A - \{\emptyset\} \rightarrow A$

$\langle 2 \rangle 1$. F is a function.

$\langle 3 \rangle 1$. LET: $(B, b), (B, b') \in F$

$\langle 3 \rangle 2$. $(B, b), (B, b') \in \{B\} \times B$

PROOF: Since $(B, b), (B, b') \in \bigcup \mathcal{A}$.

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

$\langle 3 \rangle 4$. $(B, b) = (B, b')$

PROOF: From $\langle 1 \rangle 5$.

$\langle 3 \rangle 5$. $b = b'$

$\langle 2 \rangle 2$. $\text{dom } F = \mathcal{P}A - \{\emptyset\}$

PROOF:

$$B \in \text{dom } F$$

$$\Leftrightarrow \exists b. (B, b) \in F$$

$$\Leftrightarrow \exists b. ((B, b) \in \bigcup \mathcal{A} \wedge (B, b) \in C)$$

$$\Leftrightarrow \exists b. \exists B' \in \mathcal{P}A - \{\emptyset\}. ((B, b) \in \{B'\} \times B' \wedge (B, b) \in C)$$

$$\Leftrightarrow B \in \mathcal{P}A - \{\emptyset\} \wedge \exists b \in B. (B, b) \in C$$

$$\Leftrightarrow B \in \mathcal{P}A - \{\emptyset\} \quad (\langle 1 \rangle 5)$$

$\langle 2 \rangle 3$. $\text{ran } F \subseteq A$

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

□

Proposition 3.1.6 (SC without Foundation). *For any relation R between A and B , there exists a function $H : A \rightarrow B$ such that $H \subseteq R$ (i.e. $\forall x \in A. xRH(x)$).*

PROOF:

$\langle 1 \rangle 1$. LET: R be a relation between A and B .

$\langle 1 \rangle 2$. PICK a choice function G for B .

$\langle 1 \rangle 3$. Define $H : A \rightarrow B$ by $H(x) = G(\{y \mid xRy\})$

$\langle 1 \rangle 4$. $H \subseteq R$

□

3.1.1 Injective Functions

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

Proposition 3.1.8 (S without Foundation). *For any class \mathbf{A} , the following is a theorem:*

$\text{id}_{\mathbf{A}} : \mathbf{A} \rightarrow \mathbf{A}$ is injective.

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

Proposition Schema 3.1.9 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{F} , \mathbf{G} , the following is a theorem:*

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

PROOF:

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

$\langle 1 \rangle 2$. ASSUME: $(\mathbf{G} \circ \mathbf{F})(x) = (\mathbf{G} \circ \mathbf{F})(y)$

$\langle 1 \rangle 3$. $\mathbf{G}(\mathbf{F}(x)) = \mathbf{G}(\mathbf{F}(y))$

$\langle 1 \rangle 4$. $\mathbf{F}(x) = \mathbf{F}(y)$

PROOF: Since \mathbf{G} is injective.

$\langle 1 \rangle 5$. $x = y$

PROOF: Since \mathbf{F} is injective.

\square

Proposition 3.1.10 (S without Foundation). *Let $F : A \rightarrow B$ where A is nonempty. There exists $G : B \rightarrow A$ (a left inverse) such that $G \circ F = \text{id}_A$ if and only if F is one-to-one.*

PROOF:

$\langle 1 \rangle 1$. If there exists $G : B \rightarrow A$ such that $G \circ F = \text{id}_A$ then F is one-to-one.

$\langle 2 \rangle 1$. ASSUME: $G : B \rightarrow A$ and $G \circ F = I_A$

$\langle 2 \rangle 2$. LET: $x, y \in A$

$\langle 2 \rangle 3$. ASSUME: $F(x) = F(y)$

$\langle 2 \rangle 4$. $x = y$

PROOF: $x = G(F(x)) = G(F(y)) = y$

$\langle 1 \rangle 2$. If F is one-to-one then there exists $G : B \rightarrow A$ such that $G \circ F = I_A$.

$\langle 2 \rangle 1$. ASSUME: F is one-to-one.

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

$\langle 2 \rangle 3$. LET: $G : B \rightarrow A$ be the function defined by: $G(b)$ is the (unique) $x \in A$ such that $F(x) = b$ if there exists such an x , $G(b) = a$ otherwise.

$\langle 2 \rangle 4$. For all $x \in A$ we have $G(F(x)) = x$.

\square

3.1.2 Surjective Functions

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

Proposition Schema 3.1.12 (S without Foundation). *For any class \mathbf{A} , the following is a theorem:*

$\text{id}_{\mathbf{A}} : \mathbf{A} \rightarrow \mathbf{A}$ is surjective.

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

Proposition Schema 3.1.13 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{F} and \mathbf{G} , the following is a theorem:*

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

PROOF:

- $\langle 1 \rangle 1$. LET: $c \in \mathbf{C}$
- $\langle 1 \rangle 2$. PICK $b \in \mathbf{B}$ such that $\mathbf{G}(b) = c$.
- $\langle 1 \rangle 3$. PICK $a \in \mathbf{A}$ such that $\mathbf{F}(a) = b$.
- $\langle 1 \rangle 4$. $(\mathbf{G} \circ \mathbf{F})(a) = c$

\square

Proposition 3.1.14 (SC without Foundation). *Let $F : A \rightarrow B$. There exists $H : B \rightarrow A$ (a right inverse) such that $F \circ H = \text{id}_B$ if and only if F maps A onto B .*

PROOF:

- $\langle 1 \rangle 1$. If F has a right inverse then F is surjective.
 - $\langle 2 \rangle 1$. ASSUME: F has a right inverse $H : B \rightarrow A$.
 - $\langle 2 \rangle 2$. LET: $y \in B$
 - $\langle 2 \rangle 3$. $F(H(y)) = y$
 - $\langle 2 \rangle 4$. There exists $x \in A$ such that $F(x) = y$
- $\langle 1 \rangle 2$. If F is surjective then F has a right inverse.
 - $\langle 2 \rangle 1$. ASSUME: F is surjective.
 - $\langle 2 \rangle 2$. PICK a function $H : B \rightarrow A$ such that $H \subseteq F^{-1}$
 - PROOF: Proposition 3.1.6.
 - $\langle 2 \rangle 3$. $F \circ H = \text{id}_B$
 - $\langle 3 \rangle 1$. LET: $y \in B$
 - $\langle 3 \rangle 2$. $(y, H(y)) \in F^{-1}$
 - $\langle 3 \rangle 3$. $F(H(y)) = y$

\square

3.1.3 Bijections

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

Proposition Schema 3.1.16 (S without Foundation). *For any class \mathbf{A} , the following is a theorem:*

The identity function $\text{id}_{\mathbf{A}} : \mathbf{A} \approx \mathbf{A}$ is a bijection.

PROOF: Proposition 3.1.8 and 3.1.12. \square

Proposition Schema 3.1.17 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{F} , the following is a theorem:*

If $\mathbf{F} : \mathbf{A} \approx \mathbf{B}$ then $\mathbf{F}^{-1} : \mathbf{B} \approx \mathbf{A}$.

PROOF:

$\langle 1 \rangle 1.$ $\mathbf{F}^{-1} : \mathbf{B} \rightarrow \mathbf{A}$

$\langle 2 \rangle 1.$ LET: $b \in \mathbf{B}$

$\langle 2 \rangle 2.$ PICK $a \in \mathbf{A}$ such that $\mathbf{F}(a) = b$.

PROOF: Since \mathbf{F} is surjective.

$\langle 2 \rangle 3.$ $(b, a) \in \mathbf{F}^{-1}$

$\langle 2 \rangle 4.$ If $(b, a') \in \mathbf{F}^{-1}$ then $a' = a$.

$\langle 3 \rangle 1.$ LET: $a' \in \mathbf{A}$ such that $(b, a') \in \mathbf{F}^{-1}$

$\langle 3 \rangle 2.$ $\mathbf{F}(a') = \mathbf{F}(a)$

$\langle 3 \rangle 3.$ $a' = a$

PROOF: Since \mathbf{F} is injective.

$\langle 1 \rangle 2.$ \mathbf{F}^{-1} is injective.

$\langle 2 \rangle 1.$ LET: $x, y \in \mathbf{B}$

$\langle 2 \rangle 2.$ ASSUME: $\mathbf{F}^{-1}(x) = \mathbf{F}^{-1}(y)$

$\langle 2 \rangle 3.$ $x = y$

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

$\langle 1 \rangle 3.$ \mathbf{F}^{-1} is surjective.

PROOF: For all $a \in \mathbf{A}$ we have $\mathbf{F}^{-1}(\mathbf{F}(a)) = a$.

□

Proposition Schema 3.1.18 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{F} and \mathbf{G} , the following is a theorem:*

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

PROOF: Propositions 3.1.9 and 3.1.13. □

3.1.4 Restrictions

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

$$\begin{aligned} \mathbf{F} \upharpoonright \mathbf{C} : \mathbf{C} &\rightarrow \mathbf{B} \\ (\mathbf{F} \upharpoonright \mathbf{C})(x) &= \mathbf{F}(x) \quad (x \in \mathbf{C}) \end{aligned}$$

3.1.5 Images

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

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

Proposition Schema 3.1.21 (S without Foundation). *For any classes \mathbf{F} , \mathbf{A} and \mathbf{B} , the following is a theorem.*

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

PROOF: By an Axiom of Replacement. \square

Proposition Schema 3.1.22 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} and \mathbf{F} , the following is a theorem:*

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

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

PROOF:

$$\begin{aligned} y \in \mathbf{F}\left(\bigcup \mathbf{C}\right) &\Leftrightarrow \exists x \in \bigcup \mathbf{C}. y = \mathbf{F}(x) \\ &\Leftrightarrow \exists x. \exists X. X \in \mathbf{C} \wedge x \in X \wedge y = \mathbf{F}(x) \\ &\Leftrightarrow \exists X \in \mathbf{C}. y \in \mathbf{F}(X) \end{aligned} \quad \square$$

Proposition Schema 3.1.23 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{D} and \mathbf{F} , the following is a theorem:*

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

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

PROOF:

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

Proposition 3.1.24 (S without Foundation). *For any classes \mathbf{F} , \mathbf{A} , \mathbf{B} , \mathbf{C} and \mathbf{D} , the following is a theorem:*

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

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

Equality holds if \mathbf{F} is injective.

PROOF:

- $\langle 1 \rangle 1. \mathbf{F}(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$
 - $\langle 2 \rangle 1. \text{ LET: } y \in \mathbf{F}(\mathbf{A} \cap \mathbf{B})$
 - $\langle 2 \rangle 2. \text{ PICK } x \in \mathbf{A} \cap \mathbf{B} \text{ such that } y = \mathbf{F}(x)$
 - $\langle 2 \rangle 3. y \in \mathbf{F}(\mathbf{A})$
 - PROOF: Since $x \in \mathbf{A}$.
 - $\langle 2 \rangle 4. y \in \mathbf{F}(\mathbf{B})$
 - PROOF: Since $x \in \mathbf{B}$.
- $\langle 1 \rangle 2. \text{ If } \mathbf{F} \text{ is injective then } \mathbf{F}(\mathbf{A} \cap \mathbf{B}) = \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B}).$
 - $\langle 2 \rangle 1. \text{ ASSUME: } \mathbf{F} \text{ is injective.}$
 - $\langle 2 \rangle 2. \text{ LET: } y \in \mathbf{F}(\mathbf{A}) \cap \mathbf{F}(\mathbf{B})$
 - $\langle 2 \rangle 3. \text{ PICK } x \in \mathbf{A} \text{ such that } y = \mathbf{F}(x)$
 - $\langle 2 \rangle 4. \text{ PICK } x' \in \mathbf{B} \text{ such that } y = \mathbf{F}(x')$
 - $\langle 2 \rangle 5. x = x'$
 - PROOF: $\langle 2 \rangle 1$

- ⟨2⟩6. $x \in \mathbf{A} \cap \mathbf{B}$
- ⟨2⟩7. $y \in \mathbf{F}(\mathbf{A} \cap \mathbf{B})$

□

Proposition Schema 3.1.25 (S without Foundation). *For any classes \mathbf{F} , \mathbf{A} , \mathbf{B} , and \mathbf{C} , the following is a theorem:*

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

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

Equality holds if \mathbf{F} is injective 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 $y = \mathbf{F}(x)$
 - ⟨2⟩3. LET: $X \in \mathbf{A}$
 - ⟨2⟩4. $x \in X$
 - ⟨2⟩5. $y \in \mathbf{F}(X)$
- ⟨1⟩2. If \mathbf{F} is injective then $\mathbf{F}(\bigcap \mathbf{A}) = \bigcap \{\mathbf{F}(X) \mid X \in \mathbf{A}\}$
 - ⟨2⟩1. ASSUME: \mathbf{F} is injective.
 - ⟨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 3.1.26 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{D} and \mathbf{F} , the following is a theorem:*

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

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

Equality holds if \mathbf{F} is injective.

PROOF:

- ⟨1⟩1. $\mathbf{F}(\mathbf{C}) - \mathbf{F}(\mathbf{D}) \subseteq \mathbf{F}(\mathbf{A} - \mathbf{B})$
 - ⟨2⟩1. LET: $y \in \mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B})$
 - ⟨2⟩2. PICK $x \in \mathbf{A}$ such that $y = \mathbf{F}(x)$
 - ⟨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 injective then $\mathbf{F}(\mathbf{A}) - \mathbf{F}(\mathbf{B}) = \mathbf{F}(\mathbf{A} - \mathbf{B})$
 ⟨2⟩1. ASSUME: \mathbf{F} is injective.
 ⟨2⟩2. LET: $y \in \mathbf{F}(\mathbf{A} - \mathbf{B})$
 ⟨2⟩3. PICK $x \in \mathbf{A} - \mathbf{B}$ such that $y = \mathbf{F}(x)$
 ⟨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 $y = \mathbf{F}(x')$
 ⟨3⟩3. $x = x'$
 PROOF: ⟨2⟩1
 ⟨3⟩4. $x \in \mathbf{B}$
 ⟨3⟩5. Q.E.D.
 PROOF: This contradicts ⟨2⟩3.

□

3.1.6 Inverse Images

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

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

Proposition Schema 3.1.28 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} and \mathbf{F} , the following is a theorem:*

Assume $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$ and $\mathbf{C} \subseteq \mathcal{PB}$. Then

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

PROOF:

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

Proposition Schema 3.1.29 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{D} and \mathbf{F} , the following is a theorem:*

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

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

PROOF:

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

3.1.7 Function Sets

Proposition 3.1.30 (SF without Foundation). *For any classes \mathbf{B} and \mathbf{F} , the following is a theorem:*

Let A be a set. If $\mathbf{F} : A \rightarrow \mathbf{B}$ then \mathbf{F} is a set.

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

Definition 3.1.31 (Dependent Product Class). Let I be a set and let $\mathbf{H}(i)$ be a class for all $i \in I$. We write $\prod_{i \in I} \mathbf{H}(i)$ for the class of all functions $f : I \rightarrow \bigcup_{i \in I} \mathbf{H}(i)$ such that $\forall i \in I. f(i) \in \mathbf{H}(i)$.

We write \mathbf{B}^I for $\prod_{i \in I} \mathbf{B}$ where \mathbf{B} does not depend on I .

Proposition Schema 3.1.32 (SF without Foundation). *Let I be a set. Let $H(i)$ be a set for every $i \in I$. Then $\prod_{i \in I} H(i)$ is a set.*

PROOF:

$\langle 1 \rangle 1$. $\{\mathbf{H}(i) \mid i \in I\}$ is a set.

PROOF: By an Axiom of Replacement.

$\langle 1 \rangle 2$. $\bigcup_{i \in I} \mathbf{H}(i)$ is a set.

$\langle 1 \rangle 3$. $\prod_{i \in I} \mathbf{H}(i)$ is a set.

PROOF: It is a subset of $\mathcal{P}(I \times \bigcup_{i \in I} \mathbf{H}(i))$.

\square

Proposition 3.1.33 (SFC without Foundation). *Let I be a set. Let $H(i)$ be a set for all $i \in I$. If $\forall i \in I. H(i) \neq \emptyset$ then $\prod_{i \in I} H(i) \neq \emptyset$.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: $\forall i \in I. H(i) \neq \emptyset$

$\langle 1 \rangle 2$. LET: $R = \{(i, x) \mid i \in I, x \in H(i)\}$

$\langle 1 \rangle 3$. PICK a function $f : I \rightarrow \bigcup_{i \in I} H(i)$ such that $f \subseteq R$

PROOF: Proposition 3.1.6.

$\langle 1 \rangle 4$. $f \in \prod_{i \in I} H(i)$

\square

3.2 Equinumerosity

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

Proposition 3.2.2 (S without Foundation). *Let 2 be any set of the form $\{a, b\}$ where $a \neq b$. For any set A we have $\mathcal{P}A \approx 2^A$.*

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

3.3 Domination

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

Proposition 3.3.2 (SC without Foundation). *Given sets A and B , if $A \neq \emptyset$ or $B = \emptyset$, then we have $A \preceq B$ iff there exists a surjective function $B \rightarrow A$.*

PROOF:

- $\langle 1 \rangle 1$. If $A \preceq B$ and $A \neq \emptyset$ then there exists a surjective function $B \rightarrow A$.
 - $\langle 2 \rangle 1$. ASSUME: $f : A \rightarrow B$ be injective.
 - $\langle 2 \rangle 2$. PICK $a \in A$
 - $\langle 2 \rangle 3$. LET: $g : B \rightarrow A$ be the function defined by $g(b) = f^{-1}(b)$ if $b \in \text{ran } f$, and $g(b) = a$ otherwise.
 - $\langle 2 \rangle 4$. g is surjective.
- $\langle 1 \rangle 2$. If there exists a surjective function $B \rightarrow A$ then $A \preceq B$.
 - $\langle 2 \rangle 1$. ASSUME: there exists a surjective function $g : B \rightarrow A$
 - $\langle 2 \rangle 2$. $\forall a \in A. \exists b \in B. g(b) = a$
 - $\langle 2 \rangle 3$. Choose a function $f : A \rightarrow B$ such that $\forall a \in A. g(f(a)) = a$
 - $\langle 2 \rangle 4$. f is injective.

□

3.4 Transfinite Recursion

Theorem Schema 3.4.1 (Transfinite Recursion Theorem Schema (SF without Foundation)). *For any classes \mathbf{A} , \mathbf{R} and any property $G[x, y, z]$, there exists a class \mathbf{F} such that, for any class \mathbf{F}' the following is a theorem:*

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

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

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

PROOF:

- $\langle 1 \rangle 1$. For B a subset of \mathbf{A} , let us say a function $v : B \rightarrow \mathbf{V}$ is *acceptable* iff, for all $x \in B$, we have $\text{seg } x \subseteq B$ and $G[v \upharpoonright \text{seg } x, x, v(x)]$
- $\langle 1 \rangle 2$. LET: \mathbf{K} be the class of all acceptable functions.
- $\langle 1 \rangle 3$. LET: $\mathbf{F} = \bigcup \mathbf{K}$
- $\langle 1 \rangle 4$. For all $B, C \subseteq \mathbf{A}$, given $v_1 : B \rightarrow \mathbf{V}$ and $v_2 : C \rightarrow \mathbf{V}$ acceptable and $x \in B \cap C$, we have $v_1(x) = v_2(x)$
 - $\langle 2 \rangle 1$. ASSUME: as transfinite induction hypothesis $\forall y \mathbf{R} x. y \in B \cap C \Rightarrow v_1(y) = v_2(y)$
 - $\langle 2 \rangle 2$. $v_1 \upharpoonright \text{seg } x = v_2 \upharpoonright \text{seg } x$
 - $\langle 2 \rangle 3$. $G[v_1 \upharpoonright \text{seg } x, x, v_1(x)]$

- (2)4. $G[v_2 \upharpoonright \text{seg } x, v_2(x)]$
 - (2)5. $v_1(x) = v_2(x)$
 - (1)5. **F** is a function.
 - (2)1. ASSUME: $(x, y), (x, z) \in \mathbf{F}$
 - (2)2. PICK acceptable $v_1 : B \rightarrow \mathbf{V}$ and $v_2 : C \rightarrow \mathbf{V}$ such that $v_1(x) = y$ and $v_2(x) = z$
 - (2)3. $y = z$
- PROOF: By (1)4.
- (1)6. For all $t \in \text{dom } \mathbf{F}$, we have $\mathbf{F} \upharpoonright \text{seg } t$ is a set and $G[\mathbf{F} \upharpoonright \text{seg } t, t, \mathbf{F}(t)]$
- (2)1. LET: $t \in \text{dom } \mathbf{F}$
 - (2)2. PICK an acceptable $v : A \rightarrow \mathbf{V}$ such that $t \in A$
 - (2)3. For all $y \mathbf{R} x$ we have $v(y) = \mathbf{F}(y)$
 - (2)4. $\mathbf{F} \upharpoonright \text{seg } x = v \upharpoonright \text{seg } x$
 - (2)5. $G[v \upharpoonright \text{seg } x, x, v(x)]$
 - (2)6. $G[\mathbf{F} \upharpoonright \text{seg } x, x, \mathbf{F}(x)]$
- (1)7. $\text{dom } \mathbf{F} = \mathbf{A}$
- (2)1. LET: $x \in \mathbf{A}$
 - (2)2. ASSUME: as transfinite induction hypothesis $\forall y \mathbf{R} x. y \in \mathbf{A}$
 - (2)3. ASSUME: for a contradiction $x \notin \text{dom } \mathbf{F}$
 - (2)4. $\mathbf{F} \upharpoonright \text{seg } x$ is a set
- PROOF: Axiom of Replacement, Proposition 2.4.2.
- (2)5. $\mathbf{F} \upharpoonright \text{seg } x$ is acceptable
- (2)6. LET: y be the unique object such that $G[\mathbf{F} \upharpoonright \text{seg } x, x, y]$
- (2)7. $\mathbf{F} \upharpoonright \text{seg } x \cup \{(x, y)\}$ is acceptable
- (2)8. $x \in \text{dom } \mathbf{F}$
- (2)9. Q.E.D.
- PROOF: This is a contradiction.
- (1)8. If $\mathbf{F}' : \mathbf{A} \rightarrow \mathbf{V}$ satisfies the theorem, then $\mathbf{F}' = \mathbf{F}$.
- (2)1. LET: $x \in \mathbf{A}$
 - PROVE: $\mathbf{F}'(x) = \mathbf{F}(x)$
 - (2)2. ASSUME: as transfinite induction hypothesis $\forall y \mathbf{R} x. \mathbf{F}'(y) = \mathbf{F}(y)$
 - (2)3. $\mathbf{F} \upharpoonright x = \mathbf{F}' \upharpoonright x$
 - (2)4. $G[\mathbf{F} \upharpoonright x, x, \mathbf{F}(x)]$
 - (2)5. $G[\mathbf{F}' \upharpoonright x, x, \mathbf{F}'(x)]$
 - (2)6. $\mathbf{F}(x) = \mathbf{F}'(x)$

1

Chapter 4

Category Theory

4.1 Categories

Definition 4.1.1 (Category). A *category* \mathbf{C} consists of:

- a class of *objects*;
- for any objects X, Y , a set $\mathbf{C}(X, Y)$ whose elements are called *morphisms*. We write $f : X \rightarrow Y$ for $f \in \mathbf{C}(X, Y)$.
- for any morphisms $f : X \rightarrow Y$ and $g : Y \rightarrow Z$, a morphism $gf : X \rightarrow Z$

such that:

- For all $f : X \rightarrow Y, g : Y \rightarrow Z, h : Z \rightarrow W$, we have $h(gf) = (hg)f$.
- For every object X , there exists a morphism $\text{id}_X : X \rightarrow X$ such that:
 - for any object Y and morphism $f : X \rightarrow Y$ we have $f\text{id}_X = f$.
 - for any object Y and morphism $f : Y \rightarrow X$ we have $\text{id}_X f = f$.

Definition 4.1.2 (Category of Sets). Let Set be the category of sets and functions.

Definition 4.1.3 (Category of Pointed Sets). The *category of pointed sets* Set_* has:

- objects all pairs (A, a) where A is a set and $a \in A$;
- morphisms $f : (A, a) \rightarrow (B, b)$ all functions $f : A \rightarrow B$ such that $f(a) = b$.

Definition 4.1.4 (Opposite Category). For any category \mathbf{C} , the *opposite category* \mathbf{C}^{op} is the category with the same objects as \mathbf{C} and $\mathbf{C}^{\text{op}}(X, Y) = \mathbf{C}(Y, X)$.

4.2 Invertible Morphisms

Definition 4.2.1 (Left Inverse, Right Inverse). In any category, let $f : A \rightarrow B$ and $g : B \rightarrow A$. Then g is a *left inverse* of f , and f is a *right inverse* of f , iff $gf = \text{id}_A$.

Proposition 4.2.2 (FOL). Let $f : A \rightarrow B$ and $g, h : B \rightarrow A$. If g is a left inverse to f and h is a right inverse to f then $g = h$.

PROOF: Since $g = g\text{id}_B = gfh = \text{id}_Ah = h$. \square

Definition 4.2.3 (Isomorphism). A morphism $f : A \rightarrow B$ is an *isomorphism*, $f : A \cong B$, iff it has both a left and a right inverse. In this case, its unique inverse is denoted f^{-1} .

Two objects A and B are *isomorphic*, $A \cong B$, iff there exists an isomorphism between them.

Proposition 4.2.4 (S without Foundation). A function is an isomorphism in *Set* iff it is a bijection.

Proposition 4.2.5 (S without Foundation). Let $f : A \rightarrow B$ in the category **C**. Then the following are equivalent.

1. f is an isomorphism.
2. For every object X , the function $\mathbf{C}(X, f) : \mathbf{C}(X, A) \rightarrow \mathbf{C}(X, B)$ is a bijection.
3. For every object X , the function $\mathbf{C}(f, X) : \mathbf{C}(B, X) \rightarrow \mathbf{C}(A, X)$ is a bijection.

Chapter 5

Equivalence Relations

Definition 5.0.1 (Equivalence Relation). An *equivalence relation* on a class \mathbf{A} is a binary relation on \mathbf{A} that is reflexive, symmetric and transitive.

Proposition 5.0.2 (S without Foundation). *Equinumerosity is an equivalence relation on the class of all sets.*

PROOF: Propositions 3.1.16, 3.1.17, 3.1.18. \square

Definition 5.0.3 (Respects). Let \mathbf{R} be an equivalence relation on \mathbf{A} and $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$. Then \mathbf{F} *respects* \mathbf{A} iff, whenever $(x, y) \in \mathbf{R}$, then $\mathbf{F}(x) = \mathbf{F}(y)$.

Definition 5.0.4 (Equivalence Class). Let \mathbf{R} be an equivalence relation on \mathbf{A} and $a \in \mathbf{A}$. The *equivalence class* of a modulo \mathbf{R} is

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

Proposition Schema 5.0.5 (S without Foundation). *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem.*

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

PROOF:

$\langle 1 \rangle 1$. If $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$ then $a\mathbf{R}b$.

$\langle 2 \rangle 1$. ASSUME: $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$

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

PROOF: Reflexivity

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

$\langle 2 \rangle 4$. $b \in [a]_{\mathbf{R}}$

$\langle 2 \rangle 5$. $a\mathbf{R}b$

$\langle 1 \rangle 2$. If $a\mathbf{R}b$ then $[a]_{\mathbf{R}} = [b]_{\mathbf{R}}$.

$\langle 2 \rangle 1$. For all $x, y \in \mathbf{A}$, if $x\mathbf{R}y$ then $[y]_{\mathbf{R}} \subseteq [x]_{\mathbf{R}}$

$\langle 3 \rangle 1$. LET: $x, y \in \mathbf{A}$

$\langle 3 \rangle 2$. ASSUME: $x\mathbf{R}y$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

Definition 5.0.6 (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 5.0.7. Let R be an equivalence relation on a set A . The *quotient set* A/R is the set of all equivalence classes.

Theorem 5.0.8 (S without Foundation). *Let A be a set and \mathbf{B} a class. Let R be an equivalence relation on A and $F : A \rightarrow \mathbf{B}$. Then F respects R if and only if there exists $\hat{F} : A/R \rightarrow \mathbf{B}$ such that*

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

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

PROOF:

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

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

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

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

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

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

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

PROOF: Proposition 5.0.5.

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

PROOF: $\langle 2 \rangle 1$

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

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

- $\langle 2 \rangle 6.$ $\forall a \in A. \hat{F}([a]_R) = F(a)$
 $\langle 1 \rangle 2.$ If there exists $\hat{F} : A/R \rightarrow \mathbf{B}$ such that $\forall a \in A. \hat{F}([a]_R) = F(a)$ then F respects R .
 $\langle 2 \rangle 1.$ ASSUME: $\hat{F} : A/R \rightarrow \mathbf{B}$ and $\forall a \in A. \hat{F}([a]_R) = F(a)$
 $\langle 2 \rangle 2.$ LET: $a, a' \in A$
 $\langle 2 \rangle 3.$ ASSUME: $(a, a') \in R$
 $\langle 2 \rangle 4.$ $[a]_R = [a']_R$
 PROOF: Proposition 5.0.5.
 $\langle 2 \rangle 5.$ $F(a) = F(a')$
 PROOF: $\langle 2 \rangle 1$
 $\langle 1 \rangle 3.$ If $G, H : A/R \rightarrow \mathbf{B}$ and $\forall a \in A. G([a]_R) = H([a]_R)$ then $G = H$.
 \square

Proposition 5.0.9 (S without Foundation). *Let R be an equivalence relation on a set A . Then A/R is a partition of A .*

PROOF:

- $\langle 1 \rangle 1.$ Every member of A/R is nonempty.
 PROOF: Since $a \in [a]_R$ by reflexivity.
 $\langle 1 \rangle 2.$ No two different sets in A/R have any common elements.
 $\langle 2 \rangle 1.$ LET: $[a]_R, [b]_R \in A/R$
 $\langle 2 \rangle 2.$ LET: $c \in [a]_R \cap [b]_R$
 PROVE: $[a]_R = [b]_R$
 $\langle 2 \rangle 3.$ aRc
 PROOF: $\langle 2 \rangle 2$
 $\langle 2 \rangle 4.$ bRc
 PROOF: $\langle 2 \rangle 2$
 $\langle 2 \rangle 5.$ cRb
 PROOF: Symmetry, $\langle 2 \rangle 4$
 $\langle 2 \rangle 6.$ aRb
 PROOF: Transitivity, $\langle 2 \rangle 3$, $\langle 2 \rangle 5$
 $\langle 2 \rangle 7.$ $[a]_R = [b]_R$
 PROOF: Proposition 5.0.5, $\langle 2 \rangle 6$
 $\langle 1 \rangle 3.$ Each element of A is in some set in A/R .
 PROOF: Since $a \in [a]_R$ by reflexivity.
 \square

Proposition 5.0.10 (S without Foundation). *For any partition P of a set A , there exists a unique equivalence relation R on A such that $A/R = P$, namely xRy iff $\exists X \in P (x \in X \wedge y \in X)$.*

PROOF: Easy. \square

Definition 5.0.11 (Natural Map). Let A be a set and R an equivalence relation on A . The *natural map* $A \rightarrow A/R$ is the function that maps $a \in A$ to $[a]_R$.

Chapter 6

Ordering Relations

6.1 Partial Orders

Definition 6.1.1 (Partial Ordering). Let \mathbf{A} be a class. A *partial ordering* on \mathbf{A} is a relation \mathbf{R} on \mathbf{A} that is reflexive, antisymmetric and transitive.

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

Proposition Schema 6.1.2 (S without Foundation). *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1.$ \mathbf{R}^{-1} is reflexive.

PROOF: Proposition 2.2.12.

$\langle 1 \rangle 2.$ \mathbf{R}^{-1} is antisymmetric.

PROOF: Proposition 2.2.16.

$\langle 1 \rangle 3.$ \mathbf{R}^{-1} is transitive.

$\langle 2 \rangle 1.$ ASSUME: $x\mathbf{R}^{-1}y$ and $y\mathbf{R}^{-1}z$

$\langle 2 \rangle 2.$ $y\mathbf{R}x$ and $z\mathbf{R}y$

$\langle 2 \rangle 3.$ $z\mathbf{R}x$

PROOF: Since \mathbf{R} is transitive.

$\langle 2 \rangle 4.$ $x\mathbf{R}^{-1}z$

□

Proposition Schema 6.1.3 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{F} and \mathbf{R} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1.$ \mathbf{S} is reflexive.

PROOF: For any $x \in \mathbf{A}$ we have $\mathbf{F}(x)\mathbf{R}\mathbf{F}(x)$.

- $\langle 1 \rangle 2$. **S** is antisymmetric.
 $\langle 2 \rangle 1$. LET: $x, y \in \mathbf{A}$
 $\langle 2 \rangle 2$. ASSUME: $x\mathbf{S}y$ and $y\mathbf{S}x$
 $\langle 2 \rangle 3$. $\mathbf{F}(x)\mathbf{R}\mathbf{F}(y)$ and $\mathbf{F}(y)\mathbf{R}\mathbf{F}(x)$
 $\langle 2 \rangle 4$. $\mathbf{F}(x) = \mathbf{F}(y)$
 PROOF: **R** is antisymmetric.
 $\langle 2 \rangle 5$. $x = y$
 $\langle 1 \rangle 3$. **S** is transitive.
 \square

Corollary Schema 6.1.3.1 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and **R**, the following is a theorem:*

*Assume **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} .*

Definition 6.1.4 (Partially Ordered Set). A *partially ordered set* or *poset* is a pair (A, \leq) where A is a set and \leq is a partial ordering on A . We often write just A for (A, \leq) .

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

Definition 6.1.5 (Strictly Monotone). Let $(A, <_A)$ and $(B, <_B)$ be posets. A function $f : A \rightarrow B$ is *strictly monotone* iff, whenever $x <_A y$, then $f(x) <_B f(y)$.

Definition 6.1.6 (Least). Let \leq be a partial order on \mathbf{A} . An element $m \in \mathbf{A}$ is *least* iff for all $x \in \mathbf{A}$ we have $m \leq x$.

Proposition 6.1.7 (S without Foundation). *A partial order has at most one least element.*

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

Definition 6.1.8 (Greatest). Let \leq be a partial order on \mathbf{A} . An element $m \in \mathbf{A}$ is *greatest* iff for all $x \in \mathbf{A}$ we have $x \leq m$.

Proposition 6.1.9 (S without Foundation). *A poset has at most one greatest element.*

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

Definition 6.1.10 (Upper Bound). Let \leq 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 6.1.11 (Lower Bound). Let \leq 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 6.1.12 (Bounded Above). Let \leq 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 6.1.13 (Bounded Below). Let \leq 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 6.1.14 (Least Upper Bound). Let \leq 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 6.1.15 (Greatest Lower Bound). Let \leq 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 6.1.16 (Complete). A partial order is *complete* iff every nonempty subset bounded above has a supremum, and every nonempty subset bounded below has an infimum.

Definition 6.1.17 (Order Isomorphism). Let A and B be posets. An *order isomorphism* between A and B , $f : A \cong B$, is a bijection $f : A \approx B$ such that f and f^{-1} are monotone.

Theorem 6.1.18 (Knaster Fixed-Point Theorem (S without Foundation)). *Let A be a complete poset with a greatest and least element. Let $\phi : A \rightarrow A$ 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 6.1.19 (Dense). Let \leq be a partial order on \mathbf{A} and $\mathbf{B} \subseteq \mathbf{A}$. Then \mathbf{B} is *dense* iff, for all $x, y \in \mathbf{A}$, if $x < y$ then there exists $z \in \mathbf{B}$ such that $x < z < y$.

Proposition 6.1.20 (S without Foundation). *Let A be a complete poset with no least element. Let $B \subseteq A$ be dense. Let $\theta : A \rightarrow A$ be a monotone map that is the identity on B . Then $\theta = \text{id}_A$.*

PROOF:

$\langle 1 \rangle 1$. LET: $a \in A$

PROVE: $\theta(a) = a$

- ⟨1⟩2. LET: $S(a) = \{b \in B \mid b < a\}$
- ⟨1⟩3. $S(a)$ is nonempty and bounded above.
 - ⟨2⟩1. $S(a)$ is nonempty.
 - ⟨3⟩1. PICK $a_1 < a$
 - PROOF: Since a is not least.
 - ⟨3⟩2. There exists $b \in B$ such that $a_1 < b < a$.
 - ⟨2⟩2. $S(a)$ is bounded above by a .
- ⟨1⟩4. $\sup S(a) \leq a$
- ⟨1⟩5. $\sup S(a) = a$
 - ⟨2⟩1. ASSUME: for a contradiction $\sup S(a) < a$
 - ⟨2⟩2. PICK $b \in B$ such that $\sup S(a) < b < a$
 - ⟨2⟩3. $b \in S(a)$
 - ⟨2⟩4. Q.E.D.
- PROOF: This contradicts the fact that $\sup S(a) < b$.
- ⟨1⟩6. For all $b \in S(a)$ we have $b \leq \theta(a)$
 - ⟨2⟩1. LET: $b \in S(a)$
 - ⟨2⟩2. $b < a$
 - ⟨2⟩3. $\theta(b) \leq \theta(a)$
 - ⟨2⟩4. $b \leq \theta(a)$
 - PROOF: $\theta(b) = b$
- ⟨1⟩7. $a \leq \theta(a)$
 - PROOF: Since $a = \sup S(a)$ and $\theta(a)$ is an upper bound for $S(a)$.
- ⟨1⟩8. $a \not\leq \theta(a)$
 - ⟨2⟩1. ASSUME: for a contradiction $a < \theta(a)$.
 - ⟨2⟩2. PICK $b \in B$ such that $a < b < \theta(a)$
 - ⟨2⟩3. $\theta(a) \leq \theta(b) = b$
 - ⟨2⟩4. Q.E.D.
 - PROOF: This contradicts the fact that $b < \theta(a)$.
- ⟨1⟩9. $\theta(a) = a$

□

Theorem 6.1.21 (S without Foundation). *Let A and P be complete posets with no least or greatest element. Let B be dense in A and Q be dense in P . Every order isomorphism $\phi : B \cong Q$ extends uniquely to an order isomorphism $A \cong P$.*

PROOF:

- ⟨1⟩1. For $a \in A$, let $S(a) = \{b \in B \mid b < a\}$.
- ⟨1⟩2. Define $\bar{\phi} : A \rightarrow P$ by $\bar{\phi}(a) = \sup \phi(S(a))$.
 - ⟨2⟩1. $\phi(S(a))$ is nonempty.
 - ⟨3⟩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.

Definition 6.1.23 (Lexicographic Ordering). Let \mathbf{R} be a partial order on \mathbf{A} and \mathbf{S} a partial order on \mathbf{B} . The *lexicographic ordering* \leq on $\mathbf{A} \times \mathbf{B}$ is defined by:

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

Proposition Schema 6.1.24 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{R} and \mathbf{S} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1$. LET: \leq be the lexicographic ordering on $\mathbf{A} \times \mathbf{B}$

$\langle 1 \rangle 2$. \leq is reflexive.

PROOF: For any $a \in \mathbf{A}$ and $b \in \mathbf{B}$ we have $a = a$ and $b\mathbf{S}b$, so $(a, b) \leq (a, b)$.

$\langle 1 \rangle 3$. \leq is antisymmetric.

$\langle 2 \rangle 1$. ASSUME: $(a, b) \leq (a', b')$ and $(a', b') \leq (a, b)$

$\langle 2 \rangle 2$. $(a\mathbf{R}a' \wedge a \neq a') \vee (a = a' \wedge b\mathbf{S}b')$

$\langle 2 \rangle 3$. $(a'\mathbf{R}a \wedge a' \neq a) \vee (a' = a \wedge b\mathbf{S}b')$

$\langle 2 \rangle 4$. CASE: $a = a'$

PROOF: Then $b\mathbf{S}b'$ and $b'\mathbf{S}b$ hence $b = b'$ and $(a, b) = (a', b')$.

$\langle 2 \rangle 5$. CASE: $a \neq a'$

PROOF: Then $a\mathbf{R}a'$ and $a'\mathbf{R}a$ hence $a = a'$ which is a contradiction.

$\langle 1 \rangle 4$. \leq is transitive.

$\langle 2 \rangle 1$. ASSUME: $(a_1, b_1) \leq (a_2, b_2) \leq (a_3, b_3)$

$\langle 2 \rangle 2$. $(a_1\mathbf{R}a_2 \wedge a_1 \neq a_2) \vee (a_1 = a_2 \wedge b_1\mathbf{S}b_2)$

$\langle 2 \rangle 3$. $(a_2\mathbf{R}a_3 \wedge a_2 \neq a_3) \vee (a_2 = a_3 \wedge b_2\mathbf{S}b_3)$

$\langle 2 \rangle 4$. CASE: $a_1\mathbf{R}a_2, a_1 \neq a_2, a_2\mathbf{R}a_3, a_2 \neq a_3$

$\langle 3 \rangle 1$. $a_1\mathbf{R}a_3$

PROOF: Since \mathbf{R} is transitive.

$\langle 3 \rangle 2$. $a_1 \neq a_3$

PROOF: If $a_1 = a_3$ then $a_1\mathbf{R}a_2$ and $a_2\mathbf{R}a_1$ so $a_1 = a_2$ which is a contradiction.

$\langle 2 \rangle 5$. CASE: $a_1\mathbf{R}a_2, a_1 \neq a_2, a_2 = a_3, b_2\mathbf{S}b_3$

PROOF: Then $a_1\mathbf{R}a_3$ and $a_1 \neq a_3$.

$\langle 2 \rangle 6$. CASE: $a_1 = a_2, b_1\mathbf{S}b_2, a_2\mathbf{R}a_3, a_2 \neq a_3$

PROOF: Then $a_1\mathbf{R}a_3$ and $a_1 \neq a_3$.

$\langle 2 \rangle 7$. CASE: $a_1 = a_2, b_1\mathbf{S}b_2, a_2 = a_3, b_2\mathbf{S}b_3$

PROOF: Then $a_1 = a_3$ and $b_1\mathbf{S}b_3$.

□

6.2 Linear Orders

Definition 6.2.1 (Linear Ordering). Let \mathbf{A} be a class. A *linear ordering* or *total ordering* on \mathbf{A} is a partial ordering \leq on \mathbf{A} that is *total*, i.e.

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

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

Proposition Schema 6.2.2 (Trichotomy (S without Foundation)). *For any classes \mathbf{A} and \leq , the following is a theorem:*

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

PROOF: Immediate from definitions. \square

Proposition Schema 6.2.3 (S without Foundation). *For any classes \mathbf{A} and $<$, the following is a theorem:*

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

PROOF:

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

PROOF: By definition we have $\forall x \in \mathbf{A}. x \leq x$.

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

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

$\langle 2 \rangle 2.$ $x < y$ or $x = y$

$\langle 2 \rangle 3.$ $y < x$ or $y = x$

$\langle 2 \rangle 4.$ We cannot have $x < y$ and $y < x$

PROOF: Trichotomy.

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

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

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

$\langle 2 \rangle 2.$ $x < y$ or $x = y$

$\langle 2 \rangle 3.$ $y < z$ or $y = z$

$\langle 2 \rangle 4.$ CASE: $x < y$ and $y < z$

PROOF: Then $x < z$ by transitivity, so $x \leq z$.

$\langle 2 \rangle 5.$ CASE: $x = y$

PROOF: Then we have $y \leq z$ and so $x \leq z$.

$\langle 2 \rangle 6.$ CASE: $y = z$

PROOF: Then we have $x \leq y$ and so $x \leq z$.

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

PROOF: Immediate from trichotomy.

\square

Proposition Schema 6.2.4 (S without Foundation). *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1.$ \mathbf{R}^{-1} is a partial order on \mathbf{A} .

PROOF: Proposition 6.1.2.

$\langle 1 \rangle 2.$ \mathbf{R}^{-1} is total.

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

□

Proposition Schema 6.2.5 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{F} , \mathbf{R} , \mathbf{S} , the following is a theorem:*

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

PROOF:

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

□

Proposition Schema 6.2.6 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \leq , \preceq and \mathbf{F} , the following is a theorem:*

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

PROOF:

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

□

Corollary Schema 6.2.6.1 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \leq , \preceq and \mathbf{F} , the following is a theorem:*

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

Proposition Schema 6.2.7 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{F} and \mathbf{S} , the following is a theorem:*

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

PROOF:

- ⟨1⟩1. \mathbf{R} is a partial order on \mathbf{A} .
 PROOF: Proposition 6.1.3.

$\langle 1 \rangle 2$. \mathbf{R} is total.

PROOF: For all $x, y \in \mathbf{A}$ we have $\mathbf{F}(x)\mathbf{SF}(y)$ or $\mathbf{F}(y)\mathbf{SF}(x)$.

□

Corollary Schema 6.2.7.1 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{R} , the following is a theorem:*

Assume \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} .

Proposition Schema 6.2.8 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{R} and \mathbf{S} , the following is a theorem:*

Assume \mathbf{R} is a linear order on \mathbf{A} and \mathbf{S} is a linear order on \mathbf{B} . Then the lexicographic ordering is a linear order on $\mathbf{A} \times \mathbf{B}$.

PROOF:

$\langle 1 \rangle 1$. LET: \leq be the lexicographic order on $\mathbf{A} \times \mathbf{B}$

$\langle 1 \rangle 2$. \leq is a partial order.

PROOF: Proposition 6.1.24.

$\langle 1 \rangle 3$. \leq is total.

$\langle 2 \rangle 1$. LET: $a, a' \in \mathbf{A}$ and $b, b' \in \mathbf{B}$

$\langle 2 \rangle 2$. CASE: $a\mathbf{R}a'$ and $a \neq a'$

PROOF: Then $(a, b) \leq (a', b')$.

$\langle 2 \rangle 3$. CASE: $a = a'$

PROOF: We have $b\mathbf{S}b'$ or $b'\mathbf{S}b$, so $(a, b) \leq (a', b')$ or $(a', b') \leq (a, b)$.

$\langle 2 \rangle 4$. CASE: $a'\mathbf{R}a$ and $a \neq a'$

PROOF: Then $(a', b') \leq (a, b)$.

□

6.3 Well Orderings

Definition 6.3.1 (Well Ordering). A *well ordering* on a class \mathbf{A} is a well-founded linear ordering on \mathbf{A} .

Proposition 6.3.2 (S without Foundation). *Let S be a well ordering of the set B and $f : A \rightarrow B$ a function. Define R on A by xRy if and only if $F(x)\mathbf{S}F(y)$. Then R well orders A .*

PROOF:

$\langle 1 \rangle 1$. R linearly orders A .

PROOF: Proposition 6.2.7.

$\langle 1 \rangle 2$. Every nonempty subset of A has a least element.

$\langle 2 \rangle 1$. LET: C be a nonempty subset of A .

$\langle 2 \rangle 2$. LET: y be the least element of $f(C)$.

$\langle 2 \rangle 3$. PICK $x \in C$ such that $f(x) = y$.

$\langle 2 \rangle 4$. x is least in C .

□

Proposition Schema 6.3.3 (S without Foundation). *For any classes \mathbf{A} , \mathbf{B} and \mathbf{R} , the following is a theorem:*

Assume \mathbf{R} well orders \mathbf{B} and $\mathbf{A} \subseteq \mathbf{B}$. Then $\mathbf{R} \cap \mathbf{A}^2$ well orders \mathbf{A} .

PROOF:

$\langle 1 \rangle 1$. LET: $\mathbf{R}' = \mathbf{R} \cap \mathbf{A}^2$

$\langle 1 \rangle 2$. \mathbf{R}' linearly orders \mathbf{A} .

PROOF: Corollary 6.2.7.1.

$\langle 1 \rangle 3$. \mathbf{R}' is well founded.

PROOF: Proposition 2.4.4.

□

Proposition Schema 6.3.4 (SF without Foundation). *For any classes \mathbf{A} , \mathbf{B} , \mathbf{F} and \mathbf{S} , the following is a theorem:*

Assume \mathbf{S} well orders \mathbf{B} and $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$. Define \mathbf{R} on \mathbf{A} by $x\mathbf{R}y$ if and only if $\mathbf{F}(x)\mathbf{S}\mathbf{F}(y)$. Then \mathbf{R} well orders \mathbf{A} .

PROOF:

$\langle 1 \rangle 1$. \mathbf{R} linearly orders \mathbf{A} .

PROOF: Proposition 6.2.7.

$\langle 1 \rangle 2$. For all $t \in \mathbf{A}$ we have $\{x \in \mathbf{A} \mid x\mathbf{R}t \wedge x \neq t\}$ is a set.

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

$\langle 2 \rangle 2$. LET: $S = \{y \in \mathbf{B} \mid y\mathbf{S}\mathbf{F}(t) \wedge y \neq \mathbf{F}(t)\}$

$\langle 2 \rangle 3$. LET: $P(x, y)$ be the property $\mathbf{F}(y) = x$

$\langle 2 \rangle 4$. For all $x \in S$ there exists at most one y such that $P(x, y)$

PROOF: \mathbf{F} is injective.

$\langle 2 \rangle 5$. LET: $T = \{y \mid \exists x \in S. P(x, y)\}$

PROOF: Axiom of Replacement.

$\langle 2 \rangle 6$. $T = \{x \in \mathbf{A} \mid x\mathbf{R}t \wedge x \neq t\}$

$\langle 1 \rangle 3$. Every nonempty subset of \mathbf{A} has a least element.

$\langle 2 \rangle 1$. LET: S be a nonempty subset of \mathbf{A} .

$\langle 2 \rangle 2$. $\mathbf{F}(S)$ is a nonempty subset of \mathbf{B}

PROOF: Axiom of Replacement.

$\langle 2 \rangle 3$. LET: y be the least element of $\mathbf{F}(S)$.

$\langle 2 \rangle 4$. PICK $x \in S$ such that $\mathbf{F}(x) = y$.

$\langle 2 \rangle 5$. x is least in S .

□

Proposition 6.3.5 (S without Foundation). *For any well ordered sets A and B , the lexicographic order well orders $A \times B$.*

PROOF:

$\langle 1 \rangle 1$. $A \times B$ is linearly ordered.

PROOF: Proposition 6.2.8.

$\langle 1 \rangle 2$. Every nonempty subset of $A \times B$ has a least element.

$\langle 2 \rangle 1$. LET: S be a nonempty subset of $A \times B$.

$\langle 2 \rangle 2$. LET: a be the least element of $\{x \in A \mid \exists y \in B. (x, y) \in S\}$.

$\langle 2 \rangle 3$. LET: b be the least element of $\{y \in B \mid (a, y) \in S\}$.

⟨2⟩4. (a, b) is least in S .
 \square

Definition 6.3.6 (End Extension). Let A and B be well ordered sets. Then B is an *end extension* of A iff $A \subseteq B$ and:

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

Theorem 6.3.7 (S without Foundation). Let \leq be a linear ordering on A . Assume that, for any $B \subseteq A$ such that $\forall t \in A. \text{seg } t \subseteq B \Rightarrow t \in B$, we have $B = A$. Then \leq is a well ordering on A .

PROOF:

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

Proposition Schema 6.3.8 (S without Foundation). For any classes $\mathbf{A}, \mathbf{B}, \mathbf{F}, \mathbf{G}, \leq$ and \preceq , the following is a theorem:

Assume \leq well orders \mathbf{A} and \preceq well orders \mathbf{B} . Assume \mathbf{F} and \mathbf{G} are order isomorphisms between \mathbf{A} and \mathbf{B} . Then $\mathbf{F} = \mathbf{G}$.

PROOF:

- ⟨1⟩1. For all $x \in \mathbf{A}$, if $\forall t < x. \mathbf{F}(t) = \mathbf{G}(t)$, then $\mathbf{F}(x) = \mathbf{G}(x)$
 ⟨2⟩1. LET: $x \in \mathbf{A}$
 ⟨2⟩2. ASSUME: $\forall t < x. \mathbf{F}(t) = \mathbf{G}(t)$
 ⟨2⟩3. $\mathbf{F}(\text{seg } x) = \mathbf{G}(\text{seg } x)$
 ⟨2⟩4. $\mathbf{F}(x)$ is the least element of $\mathbf{B} - \mathbf{F}(\text{seg } x)$
 ⟨2⟩5. $\mathbf{G}(x)$ is the least element of $\mathbf{B} - \mathbf{G}(\text{seg } x)$
 ⟨2⟩6. $\mathbf{F}(x) = \mathbf{G}(x)$
 ⟨1⟩2. $\forall x \in \mathbf{A}. \mathbf{F}(x) = \mathbf{G}(x)$

PROOF: Transfinite induction.

\square

Theorem 6.3.9 (ZF without Foundation). Let A and B be well ordered sets. Then one of the following holds: $A \cong B$; there exists $b \in B$ such that $A \cong \text{seg } b$; there exists $a \in A$ such that $\text{seg } a \cong B$.

PROOF:

- ⟨1⟩1. PICK e that is not in A or B .
 ⟨1⟩2. LET: $F : A \rightarrow B \cup \{e\}$ be the function defined by transfinite recursion thus:

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

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

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

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

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

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

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

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

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

1

Chapter 7

Ordinal Numbers

7.1 Ordinals

Definition 7.1.1 (Ordinal). A set α is an *ordinal (number)* iff:

- α is a transitive set
- $\{(x, y) \in \alpha^2 \mid x \in y\}$ is a strict well ordering of α .

Given ordinals α, β , we write $\alpha < \beta$ iff $\alpha \in \beta$, and $\alpha \leq \beta$ iff $\alpha \in \beta$ or $\alpha = \beta$.
Let **On** be the class of ordinals.

Proposition 7.1.2 (S). *Let α be a set. Then α is an ordinal if and only if α is a transitive set and, for all $x, y \in \alpha$, we have $x \in y$ or $x = y$ or $y \in x$.*

PROOF:

$\langle 1 \rangle 1$. LET: α be a set.

$\langle 1 \rangle 2$. If α is an ordinal then α is a transitive set and, for all $x, y \in \alpha$, we have $x \in y$ or $x = y$ or $y \in x$.

PROOF: Immediate from definitions.

$\langle 1 \rangle 3$. If α is a transitive set and $\forall x, y \in \alpha (x \in y \vee x = y \vee y \in x)$, then α is an ordinal.

$\langle 2 \rangle 1$. ASSUME: α is a transitive set.

$\langle 2 \rangle 2$. ASSUME: $\forall x, y \in \alpha (x \in y \vee x = y \vee y \in x)$

$\langle 2 \rangle 3$. Every nonempty subset of α has an \in -least element.

PROOF: Axiom of Foundation.

□

Proposition 7.1.3 (S without Foundation). **On** is a transitive class. That is, if β is an ordinal and $\alpha \in \beta$ then α is an ordinal.

PROOF:

$\langle 1 \rangle 1$. LET: β be an ordinal.

$\langle 1 \rangle 2$. LET: $\alpha \in \beta$

- $\langle 1 \rangle 3.$ α is a transitive set.
 $\langle 2 \rangle 1.$ LET: $x \in y \in \alpha$
 $\langle 2 \rangle 2.$ $y \in \beta$
 PROOF: β is a transitive set.
 $\langle 2 \rangle 3.$ $x \in \beta$
 PROOF: β is a transitive set.
 $\langle 2 \rangle 4.$ $x \in \alpha$ or $x = \alpha$ or $\alpha \in x$
 $\langle 2 \rangle 5.$ $x \neq \alpha$
 PROOF: We cannot have $x \in y \in x$ since β is well-ordered by \in .
 $\langle 2 \rangle 6.$ $\alpha \notin x$
 PROOF: We cannot have $x \in y \in \alpha \in x$ since β is well-ordered by \in .
 $\langle 2 \rangle 7.$ $x \in \alpha$
 $\langle 1 \rangle 4.$ α is well-ordered by \in
 PROOF: This holds because $\alpha \subseteq \beta$ since β is a transitive set.

□

Proposition 7.1.4 (S without Foundation). *For ordinals α and β , we have $\alpha \subseteq \beta$ if and only if $\alpha \leq \beta$.*

PROOF:

- $\langle 1 \rangle 1.$ If $\alpha \leq \beta$ then $\alpha \subseteq \beta$.
 PROOF: Since β is a transitive set.
 $\langle 1 \rangle 2.$ If $\alpha \subseteq \beta$ then $\alpha \leq \beta$.
 $\langle 2 \rangle 1.$ ASSUME: $\alpha \subsetneq \beta$
 PROVE: $\alpha \in \beta$
 $\langle 2 \rangle 2.$ LET: u be the \in -least element of $\beta - \alpha$
 $\langle 2 \rangle 3.$ $u \in \beta$
 $\langle 2 \rangle 4.$ $u \notin \alpha$
 $\langle 2 \rangle 5.$ For all $v \in \beta$, if $v \notin \alpha$ then $v \notin u$
 PROOF: From $\langle 2 \rangle 2$
 $\langle 2 \rangle 6.$ For all $v \in u$ we have $v \in \alpha$
 $\langle 2 \rangle 7.$ For all $w \in \alpha$ we have $w \in u$
 $\langle 3 \rangle 1.$ LET: $w \in \alpha$
 $\langle 3 \rangle 2.$ $w \in \beta$
 PROOF: $\langle 2 \rangle 1$
 $\langle 3 \rangle 3.$ $w \in u$ or $w = u$ or $u \in w$
 PROOF: β is an ordinal, $\langle 2 \rangle 3$, $\langle 3 \rangle 2$
 $\langle 3 \rangle 4.$ $w \neq u$
 PROOF: $\langle 2 \rangle 4$, $\langle 3 \rangle 1$
 $\langle 3 \rangle 5.$ $u \notin w$
 PROOF: $\langle 2 \rangle 4$, $\langle 3 \rangle 1$, α is a transitive set.
 $\langle 3 \rangle 6.$ $w \in u$
 PROOF: $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$
 $\langle 2 \rangle 8.$ $u = \alpha$
 PROOF: $\langle 2 \rangle 6$, $\langle 2 \rangle 7$, Axiom of Extensionality.
 $\langle 2 \rangle 9.$ $\alpha \in \beta$
 PROOF: $\langle 2 \rangle 3$, $\langle 2 \rangle 8$

□

Proposition 7.1.5 (S without Foundation). *The intersection of any nonempty set of ordinals is an ordinal.*

PROOF:

⟨1⟩1. LET: x be a nonempty set of ordinals.

⟨1⟩2. $\bigcap x$ is a transitive set.

PROOF: Proposition 1.6.6.

⟨1⟩3. $\bigcap x$ is well ordered by \in

⟨2⟩1. PICK $\alpha \in x$

⟨2⟩2. α is well ordered by \in .

⟨2⟩3. $\bigcap x \subseteq \alpha$

□

Theorem 7.1.6 (S without Foundation). *For any ordinals α and β , we have $\alpha < \beta$ or $\alpha = \beta$ or $\beta < \alpha$.*

PROOF:

⟨1⟩1. LET: α and β be ordinals.

⟨1⟩2. CASE: $\alpha \cap \beta = \alpha$ or $\alpha \cap \beta = \beta$

⟨2⟩1. ASSUME: for a contradiction $\alpha \cap \beta \subsetneq \alpha$ and $\alpha \cap \beta \subsetneq \beta$

⟨2⟩2. $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$

PROOF: Propositions 7.1.4, 7.1.5.

⟨2⟩3. $\alpha \cap \beta \in \alpha \cap \beta$

⟨2⟩4. Q.E.D.

PROOF: This contradicts the fact that α is well ordered by \in .

⟨1⟩3. $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$

⟨1⟩4. $\alpha \in \beta$ or $\alpha = \beta$ or $\beta \in \alpha$

PROOF: Proposition 7.1.4.

□

Corollary 7.1.6.1 (S without Foundation). *The class **On** is well ordered by $<$.*

PROOF:

⟨1⟩1. For ordinals α, β, γ , if $\alpha < \beta < \gamma$ then $\alpha < \gamma$.

PROOF: Because γ is a transitive set.

⟨1⟩2. Any nonempty set of ordinals has an \in -least element.

⟨2⟩1. LET: S be a nonempty set of ordinals.

⟨2⟩2. PICK $\alpha \in S$

⟨2⟩3. ASSUME: w.l.o.g. α is not least in S .

⟨2⟩4. $\alpha \cap S$ is a nonempty subset of α .

⟨2⟩5. LET: β be the least element of $\alpha \cap S$.

⟨2⟩6. β is least in S .

□

Corollary 7.1.6.2 (Burali-Forti Paradox (S without Foundation)). *The class **On** is a proper class.*

PROOF: If \mathbf{On} is a set then it is an ordinal by Proposition 7.1.3 and the previous Corollary, hence $\mathbf{On} \in \mathbf{On}$ contradicting the fact that every ordinal is well ordered by \in . \square

Corollary 7.1.6.3 (S without Foundation). *A set is an ordinal if and only if it is a transitive set of ordinals.*

Proposition 7.1.7 (S without Foundation). *For any nonempty set of ordinals x , we have $\bigcap x$ is the infimum of x in \mathbf{On} .*

PROOF: It is an ordinal by Proposition 7.1.5. The fact it is the infimum is immediate from definitions. \square

Proposition 7.1.8 (S without Foundation). *For any nonempty set of ordinals x , we have $\bigcup x$ is the supremum of x in \mathbf{On} .*

PROOF:

$\langle 1 \rangle 1$. $\bigcup x$ is an ordinal.

$\langle 2 \rangle 1$. $\bigcup x$ is a transitive set.

PROOF: Proposition 1.6.3.

$\langle 2 \rangle 2$. $\bigcup x$ is a set of ordinals.

\square

Proposition 7.1.9 (S). *For any set α , we have α is an ordinal if and only if α is a transitive set of transitive sets.*

PROOF:

$\langle 1 \rangle 1$. If α is an ordinal then α is a transitive set of transitive sets.

PROOF: Proposition 7.1.3.

$\langle 1 \rangle 2$. If α is a transitive set of transitive sets then α is an ordinal.

$\langle 2 \rangle 1$. ASSUME: α is a transitive set of transitive sets.

$\langle 2 \rangle 2$. ASSUME: for a contradiction there exist $x, y \in \alpha$ such that $x \notin y$ and $x \neq y$ and $y \notin x$

$\langle 2 \rangle 3$. $S = \{x \in \alpha \mid \exists y \in \alpha. x \notin y \wedge x \neq y \wedge y \notin x\}$ is nonempty

$\langle 2 \rangle 4$. PICK $x \in S$ such that $x \cap S = \emptyset$

PROOF: Axiom of Foundation.

$\langle 2 \rangle 5$. $T = \{y \in \alpha \mid x \notin y \wedge x \neq y \wedge y \notin x\}$ is nonempty.

$\langle 2 \rangle 6$. PICK $y \in T$ such that $y \cap T = \emptyset$

PROOF: Axiom of Foundation.

$\langle 2 \rangle 7$. $x \subseteq y$

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

$\langle 3 \rangle 2$. $z \notin S$

PROOF: $\langle 2 \rangle 4$

$\langle 3 \rangle 3$. $z \in y$ or $z = y$ or $y \in z$

$\langle 3 \rangle 4$. $z \neq y$

PROOF: Since $y \notin x$ ($\langle 2 \rangle 6$).

$\langle 3 \rangle 5$. $y \notin z$

PROOF: Since x is transitive and $y \notin x$.

1

PROOF: Vacuous. \square

$$0 := \emptyset$$
$$\alpha^+ := \alpha \cup \{\alpha\} \text{ .}$$

PROOF:

$\langle 1 \rangle$ 2. α^+ is a transitive set.

$\langle 2 \rangle 2. y \in \alpha$ or $y = \alpha$

PROOF: If $y \in \alpha$ then this follows because α is a transitive set. If $y = \alpha$ this follows immediately.

$\langle 2 \rangle 4. x \in \alpha^+$

PROOF:

$\langle 1 \rangle 2.$ $\beta \in \alpha$ or $\beta = \alpha$.

$\langle 1 \rangle 3$. CASE: $\beta \in \alpha$

PROOF: We have $\alpha \in \beta \in \alpha$ contradicting the Axiom of Foundation.

$\langle 1 \rangle 4$. CASE: $\beta = \alpha$

PROOF: We have $\alpha \in \alpha$ contradicting the Axiom of Foundation.

□

Proposition 7.1.15 (S without Foundation). *For ordinals α and β , if $\alpha^+ = \beta^+$ then $\alpha = \beta$.*

PROOF: If $\alpha^+ = \beta^+$ then $\alpha = \bigcup(\alpha^+) = \bigcup(\beta^+) = \beta$. □

Proposition 7.1.16 (S without Foundation). *For ordinals α and β , we have $\alpha < \beta$ if and only if $\alpha^+ < \beta^+$.*

PROOF:

$$\begin{aligned} \alpha < \beta &\Leftrightarrow \alpha^+ \leq \beta \\ &\Leftrightarrow \alpha^+ < \beta^+ \end{aligned} \quad \square$$

Definition 7.1.17 (Successor Ordinal). An ordinal α is a *successor ordinal* iff there exists an ordinal β such that $\alpha = \beta^+$.

Definition 7.1.18 (Limit Ordinal). An ordinal is a *limit ordinal* iff it is neither 0 nor a successor ordinal.

Proposition 7.1.19 (S without Foundation). *The relation $\{(\alpha, \beta) \in \mathbf{On}^2 \mid \alpha < \beta\}$ is well founded.*

PROOF:

$\langle 1 \rangle 1$. Any nonempty set has an \in -minimal element.

PROOF: Since \mathbf{On} is well ordered by \in .

$\langle 1 \rangle 2$. For any set x , there exists a set u such that $x \in u$ and for all ordinals α , β , if $\beta \in u$ and $\alpha < \beta$ then $\alpha \in u$.

$\langle 2 \rangle 1$. LET: x be a set.

$\langle 2 \rangle 2$. LET: $u = \{x\}$ if x is not an ordinal, x^+ if x is an ordinal.

$\langle 2 \rangle 3$. $x \in u$

$\langle 2 \rangle 4$. LET: α, β be ordinals.

$\langle 2 \rangle 5$. ASSUME: $\beta \in u$

$\langle 2 \rangle 6$. ASSUME: $\alpha < \beta$

$\langle 2 \rangle 7$. x is an ordinal

$\langle 2 \rangle 8$. $\alpha < \beta \leq x$

$\langle 2 \rangle 9$. $\alpha \in x^+ = u$

□

Proposition 7.1.20 (S without Foundation). *If λ is a limit ordinal and $\beta < \lambda$ then $\beta^+ < \lambda$.*

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

Proposition 7.1.21 (S without Foundation). *For any ordinal numbers α and β , if $(\alpha, \in) \cong (\beta, \in)$ then $\alpha = \beta$.*

PROOF:

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

Theorem 7.1.22 (SF without Foundation). *Every well-ordered set is isomorphic to a unique ordinal.*

PROOF:

- ⟨1⟩1. For any well-ordered set A , there exists an ordinal α such that $A \cong \alpha$.
- ⟨2⟩1. LET: A be a well-ordered set.
- ⟨2⟩2. Define the function E on A by transfinite recursion thus:

$$E(t) = \{E(x) \mid x < t\} \quad (t \in A) .$$
- ⟨2⟩3. LET: $\alpha = \{E(x) \mid x \in A\}$
- ⟨2⟩4. α is an ordinal.
 - ⟨3⟩1. α is a transitive set.
 - ⟨4⟩1. LET: $x \in y \in \alpha$
 - ⟨4⟩2. PICK $t \in A$ such that $y = E(t)$
 - ⟨4⟩3. $x \in E(t) = \{E(s) \mid s < t\}$
 - ⟨4⟩4. PICK $s < t$ such that $x = E(s)$
 - ⟨4⟩5. $x \in \alpha$
 - ⟨3⟩2. For all $x, y \in \alpha$ we have $x \in y$ or $x = y$ or $y \in x$
 - ⟨4⟩1. LET: $x, y \in \alpha$
 - ⟨4⟩2. PICK $a, b \in A$ such that $E(a) = x$ and $E(b) = y$
 - ⟨4⟩3. $a < b$ or $a = b$ or $b < a$
 - ⟨4⟩4. $x \in y$ or $x = y$ or $y \in x$

- ⟨3⟩3. Every nonempty subset of α has a least element.
- ⟨4⟩1. LET: S be a nonempty subset of α
- ⟨4⟩2. LET: $T = \{x \in A \mid E(x) \in S\}$
- ⟨4⟩3. LET: t be the least element of T .
PROVE: $E(t)$ is least in S
- ⟨4⟩4. LET: $y \in S$
- ⟨4⟩5. PICK $s \in T$ such that $E(s) = y$
- ⟨4⟩6. $t \leq s$
- ⟨4⟩7. $x \leq y$
- ⟨2⟩5. E is surjective.
PROOF: By definition of α .
- ⟨2⟩6. E is strictly monotone.
PROOF: If $s < t$ then $E(s) \in E(t)$ by definition of $E(t)$.
- ⟨2⟩7. Q.E.D.
PROOF: Corollary 6.2.6.1.
- ⟨1⟩2. For any ordinals α and β , if $\alpha \cong \beta$ then $\alpha = \beta$.
PROOF: Proposition 7.1.21.

□

Proposition 7.1.23 (SF without Foundation). *Let α be an ordinal and $S \subseteq \alpha$. Then S is well-ordered by \in and the ordinal of (S, \in) is $\leq \alpha$.*

PROOF:

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

□

Lemma 7.1.24 (SF without Foundation). *Let A and B be well-ordered sets. If B is an end extension of A then the ordinal of A is \leq the ordinal of B .*

PROOF:

- ⟨1⟩1. LET: α be the ordinal of A and β the ordinal of B .
- ⟨1⟩2. LET: $E_A : A \cong \alpha$ and $E_B : B \cong \beta$ be the canonical isomorphisms.
- ⟨1⟩3. $\forall a \in A. E_A(a) = E_B(a)$
 - ⟨2⟩1. LET: $a \in A$

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

Lemma 7.1.25 (SF without Foundation). *Let \mathcal{C} be a set of well ordered sets such that, for any $A, B \in \mathcal{C}$, we have that one of A and B is an end extension of the other. Let $W = \bigcup \mathcal{C}$ under $x \leq y$ iff there exists $A \in W$ such that $x, y \in A$ and $x \leq y$. Then W is a well ordered set whose ordinal is the supremum of the ordinals of the members of \mathcal{C} .*

PROOF:

- ⟨1⟩1. \leq is reflexive on W .
 - ⟨2⟩1. LET: $x \in W$
 - ⟨2⟩2. PICK $A \in W$ such that $x \in A$.
 - ⟨2⟩3. $x \leq x$
- ⟨1⟩2. \leq is antisymmetric on W .
 - ⟨2⟩1. LET: $x, y \in W$
 - ⟨2⟩2. ASSUME: $x \leq y$ and $y \leq x$
 - ⟨2⟩3. PICK $A \in W$ such that $x, y \in A$ and $x \leq_A y$, and $B \in W$ such that $x, y \in B$ and $y \leq_B x$
 - ⟨2⟩4. ASSUME: w.l.o.g. B is an end extension of A
 - ⟨2⟩5. $x \leq_B y$ and $y \leq_B x$
 - ⟨2⟩6. $x = y$
- ⟨1⟩3. \leq is transitive on W .
 - ⟨2⟩1. ASSUME: $x \leq y \leq z$
 - ⟨2⟩2. PICK $A, B \in W$ such that $x \leq_A y$ and $y \leq_B z$
 - ⟨2⟩3. CASE: A is an end extension of B .
 - ⟨3⟩1. $x \leq_A y$ and $y \leq_A z$
 - ⟨3⟩2. $x \leq_A z$
 - ⟨3⟩3. $x \leq z$
 - ⟨2⟩4. CASE: B is an end extension of A .

PROOF: Similar.
- ⟨1⟩4. \leq is total on W .
 - ⟨2⟩1. LET: $x, y \in W$
 - ⟨2⟩2. PICK $A, B \in \mathcal{C}$ such that $x \in A$ and $y \in B$
 - ⟨2⟩3. ASSUME: w.l.o.g. B is an end extension of A
 - ⟨2⟩4. $x \leq_B y$ or $y \leq_B x$
 - ⟨2⟩5. $x \leq_W y$ or $y \leq_W x$
- ⟨1⟩5. Every nonempty subset of W has a least element.
 - ⟨2⟩1. LET: S be a nonempty subset of W
 - ⟨2⟩2. PICK $s \in S$
 - ⟨2⟩3. PICK $A \in \mathcal{C}$ such that $s \in A$

- (2)4. LET: a be the \leq_A -least element of $S \cap A$
PROVE: a is least in S
 - (2)5. LET: $x \in S$
PROVE: $a \leq x$
 - (2)6. PICK $B \in \mathcal{C}$ such that $x \in B$
 - (2)7. CASE: A is an end extension of B
 - (3)1. $a \leq_A x$
 - (3)2. $a \leq x$
 - (2)8. CASE: B is an end extension of A
 - (3)1. CASE: $x \in A$
 - (4)1. $a \leq_A x$
 - (4)2. $a \leq x$
 - (3)2. CASE: $x \in B - A$
 - (4)1. $a \leq_B x$
 - (4)2. $a \leq x$
- (1)6. For all $A \in \mathcal{C}$, W is an end extension of A .
 - (2)1. For all $x, y \in A$, we have $x \leq_A y$ if and only if $x \leq_W y$
 - (3)1. LET: $x, y \in A$
 - (3)2. If $x \leq_A y$ then $x \leq_W y$
PROOF: Immediate from definitions.
 - (3)3. If $x \leq_W y$ then $x \leq_A y$
 - (4)1. ASSUME: $x \not\leq_W y$
 - (4)2. PICK $B \in \mathcal{C}$ such that $x \leq_B y$
 - (4)3. CASE: A is an end extension of B
PROOF: Then $x \leq_A y$.
 - (4)4. CASE: B is an end extension of A
PROOF: Then $x \leq_A y$.
 - (2)2. For all $x \in A$ and $y \in W - A$ we have $x < y$
 - (3)1. LET: $x \in A$ and $y \in W - A$
 - (3)2. PICK $B \in \mathcal{C}$ such that $y \in B$
 - (3)3. B is an end extension of A
 - (3)4. $x <_B y$
 - (3)5. $x <_W y$
- (1)7. For all $A \in \mathcal{C}$, the ordinal of A is \leq the ordinal of W .
PROOF: Lemma 7.1.24.
- (1)8. For any ordinal α , if for all $A \in \mathcal{C}$ the ordinal of A is $\leq \alpha$, then the ordinal of W is $\leq \alpha$.
 - (2)1. LET: α be an ordinal.
 - (2)2. ASSUME: for all $A \in \mathcal{C}$, the ordinal of A is $\leq \alpha$
 - (2)3. LET: β be the ordinal of W
 - (2)4. LET: $E : W \approx \beta$ be the canonical isomorphism.
 - (2)5. ASSUME: for a contradiction $\alpha < \beta$
 - (2)6. LET: $a \in W$ be the element with $E(a) = \alpha$
 - (2)7. PICK $A \in \mathcal{C}$ such that $a \in A$
 - (2)8. LET: γ be the ordinal of A and $E_A : A \cong \gamma$ be the canonical isomorphism.

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

PROOF: Transfinite induction on x .

$\langle 2 \rangle 10$. $E_A(a) = \alpha$

$\langle 2 \rangle 11$. $\alpha < \gamma$

$\langle 2 \rangle 12$. Q.E.D.

PROOF: This contradicts $\langle 2 \rangle 2$.

□

7.2 Natural Numbers

Definition 7.2.1 (Natural Number). An ordinal n is a *natural number* iff either it is 0, or it is a successor ordinal and every element of n is either 0 or a successor ordinal.

We write ω or \mathbb{N} for the class of natural numbers.

Theorem Schema 7.2.2 (Mathematical Induction (S without Foundation)).

For any predicate $P(x)$, the following is a theorem:

Assume $P(0)$. Assume that, for any ordinal α , if $P(\alpha)$ then $P(\alpha^+)$. Then, for every natural number n , we have $P(n)$.

PROOF:

$\langle 1 \rangle 1$. ASSUME: n is a natural number such that $\neg P(n)$

$\langle 1 \rangle 2$. LET: $y = \{\gamma \in n^+ \mid \neg P(\gamma)\}$

$\langle 1 \rangle 3$. $y \neq \emptyset$

$\langle 1 \rangle 4$. PICK $\gamma_0 \in y$ such that $y \cap \gamma_0 = \emptyset$

$\langle 1 \rangle 5$. CASE: $\gamma_0 = 0$

PROOF: Then $\neg P(0)$

$\langle 1 \rangle 6$. CASE: $\gamma_0 \neq 0$

$\langle 2 \rangle 1$. PICK γ_1 such that $\gamma_0 = \gamma_1^+$

PROOF: Either $\gamma_0 = n$ or $\gamma_0 \in n$, and in either case γ_0 is a successor because n is a natural number.

$\langle 2 \rangle 2$. $\gamma_1 \notin y$

PROOF: From $\langle 1 \rangle 4$ since $\gamma_1 \in \gamma_0$.

$\langle 2 \rangle 3$. $\gamma_1 \in n^+$

PROOF: Since $\gamma_1 \in \gamma_0 \in n^+$ and n^+ is a transitive set.

$\langle 2 \rangle 4$. $P(\gamma_1)$ and $\neg P(\gamma_1^+)$

PROOF: $\langle 1 \rangle 2$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$

□

Theorem 7.2.3 (Z without Foundation). The class of natural numbers ω is a set.

PROOF:

$\langle 1 \rangle 1$. PICK a set I such that $\emptyset \in I$ and $\forall x \in I. x \cup \{x\} \in I$.

PROOF: Axiom of Infinity.

$\langle 1 \rangle 2$. Every natural number is in I .

PROOF: By induction.

$\langle 1 \rangle 3$. Q.E.D.

PROOF: By an Axiom of Comprehension.

□

Theorem 7.2.4 (Z without Foundation). *ω is a limit ordinal.*

PROOF:

$\langle 1 \rangle 1$. ω is a transitive set.

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

PROVE: m is a natural number.

$\langle 2 \rangle 2$. ASSUME: $m \neq 0$

$\langle 2 \rangle 3$. m is a successor ordinal.

PROOF: Since $m \in n$ and n is a natural number.

$\langle 2 \rangle 4$. Every element of m is either 0 or a successor ordinal.

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

$\langle 3 \rangle 2$. $x \in n$

PROOF: Since n is a transitive set.

$\langle 3 \rangle 3$. $x = 0$ or x is a successor ordinal.

$\langle 1 \rangle 2$. ω is a set of ordinals.

$\langle 1 \rangle 3$. $\omega \neq 0$

PROOF: Since $0 \in \omega$.

$\langle 1 \rangle 4$. ω is not a successor ordinal.

$\langle 2 \rangle 1$. ASSUME: for a contradiction $\omega = n^+$

$\langle 2 \rangle 2$. n is a natural number.

$\langle 2 \rangle 3$. ω is a natural number.

$\langle 2 \rangle 4$. $\omega \in \omega$

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

PROOF: This contradicts the Axiom of Foundation.

□

7.3 Transitive Closure of a Set

Definition 7.3.1 (Transitive Closure). Let x be a set. The *transitive closure* of x is the class

$$\text{TC}(x) = \bigcap \{y \mid y \text{ is a transitive set} \wedge x \in y\} .$$

Theorem 7.3.2 (ZF without Foundation). *For any set x , the transitive closure $\text{TC}(x)$ is a set.*

PROOF:

$\langle 1 \rangle 1$. LET: $E(n, y, x)$ be the predicate: There exists a function $f : n^+ \rightarrow \mathbf{V}$ such that $f(0) = y$ and $f(n) = x$ and $\forall m \in n. f(m) \in f(m^+)$

$\langle 1 \rangle 2$. $\forall x, y. E(0, y, x) \Leftrightarrow y = x$

$\langle 1 \rangle 3$. LET: x be a set.

$\langle 1 \rangle 4$. LET: $\mathbf{W} = \{y \mid \exists n \in \mathbb{N}. E(n, y, x)\}$

$\langle 1 \rangle 5$. \mathbf{W} is a set.

- ⟨2⟩1. For $n \in \mathbb{N}$,
 LET: $\mathbf{W}_n = \{y \mid E(n, y, x)\}$
- ⟨2⟩2. For all $n \in \mathbb{N}$, \mathbf{W}_n is a set.
- ⟨3⟩1. \mathbf{W}_0 is a set.
 PROOF: $\mathbf{W}_0 = \{x\}$.
- ⟨3⟩2. For all $n \in \mathbb{N}$, if \mathbf{W}_n is a set then \mathbf{W}_{n+} is a set.
- ⟨4⟩1. $\mathbf{W}_{n+} = \bigcup \mathbf{W}_n$
- ⟨5⟩1. $\mathbf{W}_{n+} \subseteq \bigcup \mathbf{W}_n$
 - ⟨6⟩1. LET: $y \in \mathbf{W}_{n+}$
 - ⟨6⟩2. $E(n^+, y, x)$
 - ⟨6⟩3. PICK $f : n^{++} \rightarrow \mathbf{V}$ such that $f(0) = y$ and $f(n^+) = x$ and
 $\forall m \in n^+. f(m) \in f(m^+)$
 - ⟨6⟩4. $y \in f(1)$ and $E(n, f(1), x)$
 PROOF: Define $g : n^+ \rightarrow \mathbf{V}$ by $g(m) = f(m^+)$. Then $g(0) = f(1)$
 and $g(n) = x$ and $\forall m \in n. g(m) \in g(m^+)$.
 - ⟨6⟩5. $y \in f(1) \in \mathbf{W}_n$
- ⟨5⟩2. $\bigcup \mathbf{W}_n \subseteq \mathbf{W}_{n+}$
 - ⟨6⟩1. LET: $y \in z \in \mathbf{W}_n$
 - ⟨6⟩2. PICK $f : n^+ \rightarrow \mathbf{V}$ such that $f(0) = z$ and $f(n) = x$ and
 $\forall m \in n. f(m) \in f(m^+)$
 - ⟨6⟩3. LET: $g : n^{++} \rightarrow \mathbf{V}$ be the function defined by $g(0) = y$,
 $g(m^+) = f(m)$
 - ⟨6⟩4. $g(0) = y$ and $g(n^+) = x$ and $\forall m \in n^+. f(m) \in f(m^+)$
 - ⟨6⟩5. $E(n^+, y, x)$
- ⟨2⟩3. $\mathbf{W} = \bigcup \{\mathbf{W}_n \mid n \in \mathbb{N}\}$
- ⟨2⟩4. $\{\mathbf{W}_n \mid n \in \mathbb{N}\}$ is a set.
 PROOF: Axiom of Replacement.
- ⟨2⟩5. \mathbf{W} is a set.
 PROOF: Axiom of Union.
- ⟨1⟩6. \mathbf{W} is a transitive set.
- ⟨2⟩1. LET: $y \in z \in \mathbf{W}$
- ⟨2⟩2. PICK $n \in \mathbb{N}$ and $f : n^+ \rightarrow \mathbf{V}$ such that $f(0) = z$, $f(n) = x$ and
 $\forall m \in n. f(m^+) \in f(m)$
- ⟨2⟩3. LET: $g : n^{++} \rightarrow \mathbf{V}$ be the function with $g(0) = y$ and $g(m^+) = f(m)$
 for $m \in n$
- ⟨2⟩4. $g(0) = y$ and $g(n^+) = x$ and $\forall m \in n^{++}. g(m^+) \in g(m)$
- ⟨2⟩5. $y \in \mathbf{W}$
- ⟨1⟩7. $x \in \mathbf{W}$
 - ⟨2⟩1. LET: $f : 0^+ \rightarrow \mathbf{V}$ be the function $f = \{(0, x)\}$
 - ⟨2⟩2. $f(0) = x$ and $f(0) = x$ and vacuously $\forall m \in 0. f(m) \in f(m^+)$
 - ⟨2⟩3. $E(0, x, x)$
- ⟨1⟩8. For any set w' , if w' is a transitive set that contains x then $\mathbf{W} \subseteq w'$
 - ⟨2⟩1. LET: w' be a transitive set that contains x
 - ⟨2⟩2. $\forall n \in \mathbb{N}. \forall y. E(n, y, x) \Rightarrow y \in w'$
 - ⟨3⟩1. $\forall y. E(0, y, x) \Rightarrow y \in w'$
 - ⟨4⟩1. LET: y be a set.

- $\langle 4 \rangle 2$. ASSUME: $E(0, y, x)$
 $\langle 4 \rangle 3$. PICK a function $f : 0^+ \rightarrow \mathbf{V}$ such that $f(0) = y$ and $f(0) = x$ and
 $\forall m \in 0. f(m) \in f(m^+)$
 $\langle 4 \rangle 4$. $x = y$
 PROOF: $x = f(0) = y$
 $\langle 4 \rangle 5$. $y \in w'$
 PROOF: $\langle 2 \rangle 1$
 $\langle 3 \rangle 2$. For all $n \in \mathbb{N}$, if $\forall y. E(n, y, x) \Rightarrow y \in w'$, then $\forall y. E(n^+, y, x) \Rightarrow y \in w'$
 $\langle 4 \rangle 1$. LET: $n \in \mathbb{N}$
 $\langle 4 \rangle 2$. ASSUME: $\forall y. E(n, y, x) \Rightarrow y \in w'$
 $\langle 4 \rangle 3$. LET: y be a set.
 $\langle 4 \rangle 4$. ASSUME: $E(n^+, y, x)$
 $\langle 4 \rangle 5$. PICK $f : n^{++} \rightarrow \mathbf{V}$ such that $f(0) = y$ and $f(n^+) = x$ and
 $\forall m \in n^+. f(m) \in f(m^+)$
 $\langle 4 \rangle 6$. LET: $g : n^+ \rightarrow \mathbf{V}$ be the function $g(m) = f(m^+)$
 $\langle 4 \rangle 7$. $g(0) = f(0^+)$ and $g(n) = x$ and $\forall m \in n. g(m) \in g(m^+)$
 $\langle 4 \rangle 8$. $E(n, f(0^+), x)$
 $\langle 4 \rangle 9$. $f(0^+) \in w'$
 PROOF: $\langle 4 \rangle 5$
 $\langle 4 \rangle 10$. $y \in f(0^+)$
 PROOF: $y = f(0) \in f(0^+)$ by $\langle 4 \rangle 5$.
 $\langle 4 \rangle 11$. $y \in w'$
 PROOF: From $\langle 3 \rangle 2$ and $\langle 4 \rangle 10$ since w' is transitive ($\langle 2 \rangle 1$).
 $\langle 2 \rangle 3$. $\mathbf{W} \subseteq w'$
 \square

Proposition 7.3.3 (S without Foundation). *The transitive closure of an ordinal α is α^+ .*

PROOF:

- $\langle 1 \rangle 1$. α^+ is a transitive set that contains α .
 $\langle 1 \rangle 2$. For any transitive set x , if $\alpha \in x$ then $\alpha^+ \subseteq x$.
 \square

7.4 The Well-Ordering Theorem and Zorn's Lemma

Theorem 7.4.1 (Hartogs (SF without Foundation)). *For any set A , there exists an ordinal not dominated by A .*

PROOF:

- $\langle 1 \rangle 1$. LET: α be the class of all ordinals β such that $\beta \preccurlyeq A$
 PROVE: α is a set.
 $\langle 1 \rangle 2$. LET: $W = \{(B, R) \mid B \subseteq A, R \text{ is a well ordering on } B\}$
 $\langle 1 \rangle 3$. α is the class of the ordinals of the elements of W .
 $\langle 2 \rangle 1$. For all $(B, R) \in W$, the ordinal of (B, R) is in α .
 $\langle 3 \rangle 1$. 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 $\beta \rightarrow A$
 - ⟨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 $f : \beta \rightarrow A$
 - ⟨3⟩3. Define \leq on $\text{ran } f$ by $f(x) \leq f(y)$ iff $x \leq y$
 - ⟨3⟩4. $(\text{ran } f, \leq) \in W$
 - ⟨3⟩5. β is the ordinal number of $(\text{ran } f, \leq)$
 - ⟨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. $\alpha \not\approx A$
 - PROOF: Since $\alpha \notin \alpha$.
-

Theorem 7.4.2 (Numeration Theorem (SFC without Foundation)). *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: $F : \alpha \rightarrow A \cup \{e\}$ 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. $e \in \text{ran } F$
- ⟨2⟩1. ASSUME: for a contradiction $e \notin \text{ran } F$
- ⟨2⟩2. F is an injection $\alpha \rightarrow A$.
- ⟨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. $F \upharpoonright \delta : \delta \approx A$

Theorem 7.4.3 (Well-Ordering Theorem (SFC without Foundation)). *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 .

□

Theorem 7.4.4 (Zorn's Lemma (SFC without Foundation)). *Let \mathcal{A} be a set such that, for every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$. Then \mathcal{A} has a maximal element.*

PROOF:

- ⟨1⟩1. PICK a well ordering $<$ on \mathcal{A} .
- ⟨1⟩2. LET: $F : \mathcal{A} \rightarrow 2$ be the function defined by transfinite recursion by:

$$F(A) = \begin{cases} 1 & \text{if } A \text{ includes every set } B < A \text{ for which } F(B) = 1 \\ 0 & \text{otherwise} \end{cases}$$
- ⟨1⟩3. LET: $\mathcal{C} = \{A \in \mathcal{A} \mid F(A) = 1\}$
- PROVE: $\bigcup \mathcal{C}$ is a maximal element of \mathcal{A}
- ⟨1⟩4. For all $A \in \mathcal{A}$, we have $A \in \mathcal{C}$ iff $\forall B < A. B \in \mathcal{C} \Rightarrow B \subseteq A$
- ⟨1⟩5. \mathcal{C} is a chain.
 - ⟨2⟩1. LET: $A, A' \in \mathcal{C}$
 - ⟨2⟩2. ASSUME: w.l.o.g. $A \leq A'$
 - ⟨2⟩3. $A \subseteq A'$

PROOF: By ⟨1⟩4

- ⟨1⟩6. $\bigcup \mathcal{C} \in \mathcal{A}$
- ⟨1⟩7. $\bigcup \mathcal{C}$ is maximal in \mathcal{A} .
 - ⟨2⟩1. LET: $A \in \mathcal{A}$ and $\bigcup \mathcal{C} \subseteq A$
 - ⟨2⟩2. $A \in \mathcal{C}$
 - PROOF: By ⟨1⟩4 since $\forall B \in \mathcal{C}. B \subseteq A$.
 - ⟨2⟩3. $A \subseteq \bigcup \mathcal{C}$
 - ⟨2⟩4. $A = \bigcup \mathcal{C}$

□

Proposition 7.4.5 (Teichmüller-Tukey Lemma (SFC without Foundation)). *Let \mathcal{A} be a nonempty set such that, for every B , we have $B \in \mathcal{A}$ if and only if every finite subset of B is a member of \mathcal{A} . Then \mathcal{A} has a maximal element.*

PROOF:

- ⟨1⟩1. For every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$
 - ⟨2⟩1. LET: $\mathcal{B} \subseteq \mathcal{A}$ be a chain.
 - ⟨2⟩2. Every finite subset of $\bigcup \mathcal{B}$ is a member of \mathcal{A} .
 - ⟨3⟩1. LET: C be a finite subset of $\bigcup \mathcal{B}$.
 - ⟨3⟩2. PICK $B \in \mathcal{B}$ such that $C \subseteq B$.
 - ⟨3⟩3. $B \in \mathcal{A}$
 - ⟨3⟩4. Every finite subset of B is in \mathcal{A} .
 - ⟨3⟩5. $C \in \mathcal{A}$
 - ⟨2⟩3. $\bigcup \mathcal{B} \in \mathcal{A}$.
- ⟨1⟩2. Q.E.D.

PROOF: Zorn's lemma.

□

Theorem Schema 7.4.6 (SF without Foundation). *For any class \mathbf{A} , there exists a class \mathbf{F} such that the following is a theorem:*

If \mathbf{A} is a proper class of ordinals, then $\mathbf{F} : \mathbf{On} \rightarrow \mathbf{A}$ is an order isomorphism.

PROOF:

$\langle 1 \rangle 1$. Define $\mathbf{F} : \mathbf{On} \rightarrow \mathbf{A}$ by transfinite recursion as follows: $\mathbf{F}(\alpha)$ is the least element of \mathbf{A} that is different from $\mathbf{F}(\beta)$ for all $\beta < \alpha$.

$\langle 1 \rangle 2$. For all $\alpha, \beta \in \mathbf{On}$, if $\alpha < \beta$ then $\mathbf{F}(\alpha) < \mathbf{F}(\beta)$

PROOF: We have $\mathbf{F}(\alpha) \neq \mathbf{F}(\beta)$ by the definition of $\mathbf{F}(\beta)$, and $\mathbf{F}(\beta) \not< \mathbf{F}(\alpha)$ by the leastness of $\mathbf{F}(\alpha)$.

$\langle 1 \rangle 3$. \mathbf{F} is surjective.

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

$\langle 2 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall \beta \in \mathbf{A}$, if $\beta < \alpha$ then there exists γ such that $\beta = \mathbf{F}(\gamma)$.

$\langle 2 \rangle 3$. LET: $\gamma = \{\delta \in \mathbf{On} \mid \mathbf{F}(\delta) < \alpha\}$

$\langle 2 \rangle 4$. γ is a set.

PROOF: Axiom of Replacement applied to α .

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

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

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

PROOF: Corollary 7.1.6.3.

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

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

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

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

□

7.5 Ordinal Operations

Definition 7.5.1 (Ordinal Operation). An *ordinal operation* is a function $\mathbf{On} \rightarrow \mathbf{On}$.

Definition 7.5.2 (Continuous). An ordinal operation $\mathbf{T} : \mathbf{On} \rightarrow \mathbf{On}$ is *continuous* iff, for every limit ordinal λ , we have $\mathbf{T}(\lambda) = \bigcup_{\alpha < \lambda} \mathbf{T}(\alpha)$.

Definition 7.5.3 (Normal). An ordinal operation is *normal* iff it is continuous and strictly monotone.

Proposition Schema 7.5.4 (S without Foundation). *For any class \mathbf{T} , the following is a theorem.*

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

PROOF:

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

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

PROOF: Vacuous.

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

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

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

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

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

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

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

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

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

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

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

PROOF:

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

□

Proposition Schema 7.5.5 (S without Foundation). *For any class \mathbf{T} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1$. LET: γ be an ordinal.

$\langle 1 \rangle 2$. ASSUME: as induction hypothesis $\forall \delta < \gamma. \mathbf{T}(\delta) \geq \delta$

$\langle 1 \rangle 3$. For all $\delta < \gamma$ we have $\delta < \mathbf{T}(\gamma)$

PROOF: \mathbf{T} is strictly monotone.

$\langle 1 \rangle 4$. $\gamma \leq \mathbf{T}(\gamma)$

□

Proposition Schema 7.5.6 (S without Foundation). *For any class \mathbf{T} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1$. There exists γ such that $\mathbf{T}(\gamma) > \beta$

$\langle 2 \rangle 1$. For all γ we have $\mathbf{T}(\gamma) \geq \gamma$

PROOF: Proposition 7.5.5.

$\langle 2 \rangle 2$. $\mathbf{T}(\beta^+) > \beta$

$\langle 1 \rangle 2$. LET: δ be least such that $\mathbf{T}(\delta) > \beta$

$\langle 1 \rangle 3$. δ is a successor ordinal.

$\langle 2 \rangle 1. \delta \neq 0$

PROOF: Since $\mathbf{T}(0) \leq \beta$.

$\langle 2 \rangle 2. \delta$ is not a limit ordinal.

$\langle 3 \rangle 1.$ ASSUME: for a contradiction δ is a limit ordinal.

$\langle 3 \rangle 2. \beta < \bigcup_{\epsilon < \delta} \mathbf{T}(\epsilon)$

PROOF: \mathbf{T} is continuous.

$\langle 3 \rangle 3.$ There exists $\epsilon < \delta$ such that $\beta < \mathbf{T}(\epsilon)$

$\langle 3 \rangle 4.$ Q.E.D.

PROOF: This contradicts the minimality of δ .

$\langle 1 \rangle 4.$ LET: $\delta = \gamma^+$

$\langle 1 \rangle 5.$ γ is greatest such that $\mathbf{T}(\gamma) \leq \beta$

□

Theorem Schema 7.5.7 (S without Foundation). *For any class \mathbf{T} , the following is a theorem:*

Assume that \mathbf{T} is a normal ordinal operation. For any nonempty set of ordinals S , we have

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

PROOF:

$\langle 1 \rangle 1. \forall \alpha \in S. \mathbf{T}(\alpha) \leq \mathbf{T}(\sup S)$

PROOF: Since \mathbf{T} is monotone.

$\langle 1 \rangle 2.$ For any ordinal β , if $\forall \alpha \in S. \mathbf{T}(\alpha) \leq \beta$, then $\mathbf{T}(\sup S) \leq \beta$

$\langle 2 \rangle 1.$ LET: β be an ordinal.

$\langle 2 \rangle 2.$ LET: $\gamma = \sup S$

$\langle 2 \rangle 3.$ ASSUME: $\forall \alpha \in S. \mathbf{T}(\alpha) \leq \beta$

$\langle 2 \rangle 4.$ CASE: γ is 0 or a successor ordinal

PROOF: Then we must have $\gamma \in S$ so $\mathbf{T}(\gamma) \leq \beta$ from $\langle 2 \rangle 3$.

$\langle 2 \rangle 5.$ CASE: γ is a limit ordinal

$\langle 3 \rangle 1. \mathbf{T}(\gamma) = \sup_{\alpha < \gamma} \mathbf{T}(\alpha)$

PROOF: \mathbf{T} is continuous.

$\langle 3 \rangle 2.$ ASSUME: for a contradiction $\beta < \mathbf{T}(\gamma)$

$\langle 3 \rangle 3.$ PICK $\alpha < \gamma$ such that $\beta < \mathbf{T}(\alpha)$

PROOF: $\langle 3 \rangle 1, \langle 3 \rangle 2$

$\langle 3 \rangle 4.$ PICK $\alpha' \in S$ such that $\alpha < \alpha'$

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

$\langle 3 \rangle 5. \beta < \mathbf{T}(\alpha') \leq \beta$

PROOF: \mathbf{T} is strictly monotone, $\langle 3 \rangle 3, \langle 3 \rangle 4, \langle 2 \rangle 3$.

$\langle 3 \rangle 6.$ Q.E.D.

PROOF: This is a contradiction.

□

Proposition 7.5.8 (SF without Foundation). *For any classes \mathbf{A} and \mathbf{T} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1$. \mathbf{T} is strictly monotone.

PROOF: Since it is an order isomorphism.

$\langle 1 \rangle 2$. \mathbf{T} is continuous.

$\langle 2 \rangle 1$. LET: λ be a limit ordinal.

$\langle 2 \rangle 2$. $\mathbf{T}'(\lambda)$ is the least member of \mathbf{A} that is greater than $\mathbf{T}'(\alpha)$ for all $\alpha < \lambda$

$\langle 2 \rangle 3$. $\mathbf{T}'(\lambda) = \sup_{\alpha < \lambda} \mathbf{T}'(\alpha)$

□

Proposition Schema 7.5.9 (S without Foundation). *For any class \mathbf{T} , the following is a theorem:*

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

PROOF:

$\langle 1 \rangle 1$. $\mathbf{T}(\lambda) \neq 0$

PROOF: Since $0 \leq \mathbf{T}(0) < \mathbf{T}(\lambda)$.

$\langle 1 \rangle 2$. $\mathbf{T}(\lambda)$ is not a successor ordinal.

$\langle 2 \rangle 1$. ASSUME: for a contradiction $\mathbf{T}(\lambda) = \alpha^+$

$\langle 2 \rangle 2$. $\alpha < \mathbf{T}(\lambda) = \sup_{\beta < \lambda} \mathbf{T}(\beta)$

$\langle 2 \rangle 3$. PICK $\beta < \lambda$ such that $\alpha < \mathbf{T}(\beta)$

$\langle 2 \rangle 4$. $\alpha^+ \leq \mathbf{T}(\beta) < \mathbf{T}(\lambda)$

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

PROOF: This is a contradiction.

□

7.6 Ordinal Arithmetic

7.6.1 Addition

Definition 7.6.1. Let A and B be disjoint well-ordered sets. The *concatenation* of A and B is the set $A \cup B$ under the relation:

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

Proposition 7.6.2 (S without Foundation). *If A and B are disjoint well-ordered sets, then their concatenation is well-ordered.*

PROOF:

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

PROOF: For all $a \in A$ we have $a \leq a$, and for all $b \in B$ we have $b \leq b$.

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

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

$\langle 2 \rangle 2$. CASE: $x, y \in A$

PROOF: Then $x = y$ since the order on A is antisymmetric.

$\langle 2 \rangle 3$. CASE: $x \in A$ and $y \in B$

PROOF: This is impossible as it would imply $y \not\leq x$.

$\langle 2 \rangle 4$. CASE: $x \in B$ and $y \in A$

PROOF: This is impossible as it would imply $x \not\leq y$.

$\langle 2 \rangle 5$. CASE: $x, y \in B$

PROOF: Then $x = y$ since the order on B is antisymmetric.

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

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

$\langle 2 \rangle 2$. CASE: $x, z \in A$

PROOF: In this case $y \in A$ since $y \leq z$, and so $x \leq z$ since the order on A is transitive.

$\langle 2 \rangle 3$. CASE: $x \in A$ and $z \in B$

PROOF: Then $x \leq z$ immediately.

$\langle 2 \rangle 4$. CASE: $x \in B$ and $z \in A$

PROOF: This is impossible because we have $y \notin A$ since $x \leq y$ and $y \notin B$ since $y \leq z$.

$\langle 2 \rangle 5$. CASE: $x, z \in B$

PROOF: In this case $y \in B$ since $x \leq y$, and so $x \leq z$ since the order on B is transitive.

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

$\langle 2 \rangle 1$. LET: $x, y \in A \cup B$

$\langle 2 \rangle 2$. CASE: $x, y \in A$

PROOF: Then $x \leq y$ or $y \leq x$ because the order on A is total.

$\langle 2 \rangle 3$. CASE: $x \in A$ and $y \in B$

PROOF: Then $x \leq y$.

$\langle 2 \rangle 4$. CASE: $x \in B$ and $y \in A$

PROOF: Then $y \leq x$.

$\langle 2 \rangle 5$. CASE: $x, y \in B$

PROOF: Then $x \leq y$ or $y \leq x$ because the order on B is total.

$\langle 1 \rangle 5$. Every nonempty subset of $A \cup B$ has a least element.

$\langle 2 \rangle 1$. LET: S be a nonempty subset of $A \cup B$

$\langle 2 \rangle 2$. CASE: $S \cap A = \emptyset$

PROOF: Then $S \subseteq B$ and so S has a least element.

$\langle 2 \rangle 3$. CASE: $S \cap A \neq \emptyset$

PROOF: The least element of $S \cap A$ is the least element of S .

□

Definition 7.6.3 (Ordinal Addition (SF without Foundation)). Let α and β be ordinal numbers. Then $\alpha + \beta$ is the ordinal number of the concatenation of A and B , where A is any well ordered set with ordinal α and B is any well ordered set with ordinal β .

Theorem 7.6.4 (Associative Law for Addition (SF without Foundation)). For any ordinals ρ , σ and τ , we have

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

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

Theorem 7.6.5 (SF without Foundation). *For any ordinal ρ we have*

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

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

Theorem 7.6.6 (SF without Foundation). *For any ordinal α we have $\alpha + 1 = \alpha^+$.*

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

Theorem 7.6.7 (SF without Foundation). *For any ordinal α , the operation that maps β to $\alpha + \beta$ is normal.*

PROOF:

$\langle 1 \rangle 1$. For any limit ordinal λ , we have $\alpha + \lambda = \sup_{\beta < \lambda} (\alpha + \beta)$.

$\langle 2 \rangle 1$. LET: λ be a limit ordinal.

$\langle 2 \rangle 2$. $(\{0\} \times \alpha) \cup (\{1\} \times \lambda) = \bigcup_{\beta \in \lambda} ((\{0\} \times \alpha) \cup (\{1\} \times \beta))$, where the order on the right hand side is as in Lemma 7.1.25.

PROOF:

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

$\langle 1 \rangle 2$. For any ordinal β we have $\alpha + \beta < \alpha + \beta^+$

PROOF: Since $\alpha + \beta^+ = \alpha + \beta + 1 = (\alpha + \beta)^+$.

\square

Corollary 7.6.7.1 (SF without Foundation). *For any ordinals α , β , γ , we have $\beta < \gamma$ if and only if $\alpha + \beta < \alpha + \gamma$.*

Corollary 7.6.7.2 (Left Cancellation for Addition (SF without Foundation)). *For any ordinals α , β and γ , if $\alpha + \beta = \alpha + \gamma$ then $\beta = \gamma$.*

Theorem 7.6.8 (SF without Foundation). *For any ordinals α , β , γ , if $\beta \leq \gamma$ then $\beta + \alpha \leq \gamma + \alpha$.*

PROOF: Transfinite induction on α . \square

Theorem 7.6.9 (Subtraction Theorem (SF without Foundation)). *Let α and β be ordinals with $\alpha \leq \beta$. Then there exists a unique ordinal δ such that $\alpha + \delta = \beta$.*

PROOF:

(1)1. For all ordinals α and β with $\alpha \leq \beta$, there exists δ such that $\alpha + \delta = \beta$

(2)1. LET: α and β be ordinals with $\alpha \leq \beta$

(2)2. LET: δ be the greatest ordinal such that $\alpha + \delta \leq \beta$

PROOF: Proposition 7.5.6.

(2)3. $\alpha + \delta = \beta$

PROOF: If $\alpha + \delta < \beta$ then $\alpha + \delta + 1 \leq \beta$ contradicting the greatestness of δ .

(1)2. Q.E.D.

PROOF: Uniqueness follows from the Left Cancellation Law.

□

7.6.2 Multiplication

Definition 7.6.10 (Ordinal Multiplication (SF without Foundation)). Let α and β be ordinal numbers. Then $\alpha\beta$ is the ordinal number of $A \times B$ under the lexicographic order, where A is any well ordered set with ordinal α and B is any well ordered set with ordinal β .

This is well defined by Proposition 6.3.5.

Theorem 7.6.11 (Associative Law (SF without Foundation)). *For any ordinals ρ , σ and τ , we have*

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

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

Theorem 7.6.12 (Left Distributive Law (SF without Foundation)). *For any ordinals ρ , σ and τ , we have*

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

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

Theorem 7.6.13 (SF without Foundation). *For any ordinal ρ we have $\rho 0 = 0\rho = 0$.*

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

Theorem 7.6.14 (SF without Foundation). *For any ordinal ρ we have $\rho 1 = 1\rho = \rho$.*

PROOF: Easy. □

Theorem 7.6.15 (SF without Foundation). *For any ordinals ρ and σ , if $\rho\sigma = 0$ then $\rho = 0$ or $\sigma = 0$.*

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

Theorem 7.6.16 (SF without Foundation). *For any non-zero ordinal α , the operation that maps β to $\alpha\beta$ is normal.*

PROOF:

$\langle 1 \rangle 1$. For any limit ordinal λ , we have $\alpha\lambda = \bigcup_{\beta < \lambda} \alpha\beta$

$\langle 2 \rangle 1$. LET: λ be a limit ordinal

$\langle 2 \rangle 2$. $\alpha \times \lambda = \bigcup_{\beta < \lambda} (\alpha \times \beta)$ as well-ordered sets

$\langle 1 \rangle 2$. For any ordinal β we have $\alpha\beta < \alpha\beta^+$

PROOF: $\alpha\beta^+ = \alpha\beta + \alpha > \alpha\beta$

□

Corollary 7.6.16.1 (SF without Foundation). *For any ordinals α, β, γ , if $\alpha \neq 0$ then $\beta < \gamma$ if and only if $\alpha\beta < \alpha\gamma$.*

Corollary 7.6.16.2 (Left Cancellation for Multiplication (SF without Foundation)). *For any ordinals α, β, γ , if $\alpha \neq 0$ and $\alpha\beta = \alpha\gamma$ then $\beta = \gamma$.*

Theorem 7.6.17 (SF without Foundation). *For any ordinals α, β and γ , if $\beta \leq \gamma$ then $\beta\alpha \leq \gamma\alpha$.*

PROOF: Transfinite induction on α . □

Theorem 7.6.18 (Division Theorem (SF without Foundation)). *Let α and δ be ordinal numbers with $\delta \neq 0$. Then there exist unique ordinals β and γ with $\gamma < \delta$ and*

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

PROOF:

$\langle 1 \rangle 1$. For any ordinal numbers α and δ with $\delta \neq 0$, there exist ordinals β and γ such that $\gamma < \delta$ and $\alpha = \delta\beta + \gamma$

$\langle 2 \rangle 1$. LET: α and δ be ordinals with $\delta \neq 0$

$\langle 2 \rangle 2$. LET: β be the greatest ordinal such that $\delta\beta \leq \alpha$

PROOF: Proposition 7.5.6.

$\langle 2 \rangle 3$. There exists an ordinal γ such that $\alpha = \delta\beta + \gamma$

PROOF: Subtraction Theorem

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

$\langle 2 \rangle 1$. LET: $\delta, \beta, \beta', \gamma, \gamma'$ be ordinals.

$\langle 2 \rangle 2$. ASSUME: $\delta \neq 0$ and $\delta\beta + \gamma = \delta\beta' + \gamma'$

$\langle 2 \rangle 3$. $\beta = \beta'$

$\langle 3 \rangle 1$. $\beta \not\leq \beta'$

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

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

$\langle 3 \rangle 2$. $\beta' \not\leq \beta$

PROOF: Similar.

$\langle 2 \rangle 4. \gamma = \gamma'$

PROOF: By Cancellation.

□

7.6.3 Exponentiation

Definition 7.6.19 (SF without Foundation). Given ordinals α and β , define the ordinal α^β as follows:

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

Theorem 7.6.20 (SF without Foundation). *Let α be an ordinal ≥ 2 . The operation that maps β to α^β is normal.*

PROOF:

$\langle 1 \rangle 1.$ For λ a limit ordinal we have $\alpha^\lambda = \sup_{\beta < \lambda} \alpha^\beta$

PROOF: By definition.

$\langle 1 \rangle 2.$ For any ordinal β we have $\alpha^\beta < \alpha^{\beta^+}$

PROOF: We have $\alpha^{\beta^+} = \alpha^\beta \alpha > \alpha^\beta$ by Theorem 7.6.16 since $\alpha > 1$ and $\alpha^\beta \neq 0$.

□

Corollary 7.6.20.1 (SF without Foundation). *For any ordinals α, β, γ , if $\alpha \geq 2$ then $\beta < \gamma$ if and only if $\alpha^\beta < \alpha^\gamma$.*

Corollary 7.6.20.2 (Cancellation for Exponentiation (SF without Foundation)). *For any ordinals α, β, γ , if $\alpha \geq 2$ and $\alpha^\beta = \alpha^\gamma$ then $\beta = \gamma$.*

Theorem 7.6.21 (SF without Foundation). *For any ordinals α, β and γ , if $\beta \leq \gamma$ then $\beta^\alpha \leq \gamma^\alpha$.*

PROOF: Transfinite induction on α .

Theorem 7.6.22 (Logarithm Theorem (SF without Foundation)). *Let α and β be ordinal numbers with $\alpha \neq 0$ and $\beta > 1$. Then there exist unique ordinals γ, δ and ρ such that*

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

PROOF:

$\langle 1 \rangle 1.$ For any ordinals α and β with $\alpha \neq 0$ and $\beta > 1$, there exist ordinals γ, δ, ρ such that

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

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

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

PROOF: Proposition 7.5.6.

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

PROOF: By the Division Theorem.

⟨2⟩4. $\delta \neq 0$

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

⟨2⟩5. $\delta < \beta$

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

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

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

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

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

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

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

⟨2⟩6. $\gamma = \gamma'$

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

PROOF: By the Division Theorem.

□

Theorem 7.6.23 (SF without Foundation). *For any ordinal numbers α , β , γ , we have*

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

PROOF:

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

⟨1⟩2. $P[0]$

PROOF:

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

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

PROOF:

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

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

⟨2⟩1. LET: λ be a limit ordinal

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

⟨2⟩3. LET: α and β be any ordinals.

⟨2⟩4. CASE: $\alpha = 0$

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

⟨2⟩5. CASE: $\alpha = 1$

PROOF: We have $\alpha^{\beta+\lambda} = \alpha^\beta \alpha^\lambda = 1$.

$\langle 2 \rangle 6$. CASE: $\alpha > 1$

PROOF:

$$\begin{aligned}
 \alpha^{\beta+\lambda} &= \alpha^{\sup_{\gamma < \lambda} (\beta+\gamma)} \\
 &= \sup_{\gamma < \lambda} \alpha^{\beta+\gamma} && \text{(Theorem 7.5.7)} \\
 &= \sup_{\gamma < \lambda} \alpha^\beta \alpha^\gamma && (\langle 2 \rangle 2) \\
 &= \alpha^\beta \sup_{\gamma < \lambda} \alpha^\gamma && \text{(Theorem 7.5.7)} \\
 &= \alpha^\beta \alpha^\lambda
 \end{aligned}$$

□

Theorem 7.6.24 (SF without Foundation). *For any ordinal numbers α , β and γ , we have*

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

PROOF:

$\langle 1 \rangle 1$. LET: $P[\gamma]$ be the property: For any ordinals α and β , we have $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$

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

PROOF:

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

$\langle 1 \rangle 3$. $\forall \gamma \in \mathbf{On}. P[\gamma] \Rightarrow P[\gamma + 1]$

PROOF:

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

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

$\langle 2 \rangle 1$. LET: λ be a limit ordinal.

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

$\langle 2 \rangle 3$. LET: α and β be any ordinals.

$\langle 2 \rangle 4$. CASE: $\alpha = 0$ and $\beta = 0$

PROOF:

$$\begin{aligned}
 (0^\beta)^\lambda &= 1^\lambda \\
 &= 1 \\
 &= 0^0 \\
 &= 0^{0\lambda}
 \end{aligned}$$

$\langle 2 \rangle 5$. CASE: $\alpha = 0$ and $\beta \neq 0$

PROOF: $(0^\beta)^\lambda = 0^{\beta\lambda} = 0$.

$\langle 2 \rangle 6$. CASE: $\alpha = 1$

PROOF: $(1^\beta)^\lambda = 1^{\beta\lambda} = 1$

⟨2⟩7. CASE: $\alpha > 1$

PROOF:

$$\begin{aligned}
 (\alpha^\beta)^\lambda &= \sup_{\gamma < \lambda} (\alpha^\beta)^\gamma \\
 &= \sup_{\gamma < \lambda} \alpha^{\beta\gamma} \\
 &= \alpha^{\sup_{\gamma < \lambda} \beta\gamma} \\
 &= \alpha^{\beta\lambda}
 \end{aligned}$$

□

7.7 Sequences

i

Definition 7.7.1 (Sequence). Given an ordinal α and class \mathbf{A} , an α -sequence in \mathbf{A} is a function $a : \alpha \rightarrow \mathbf{A}$. We write a_β for $a(\beta)$, and $(a_\beta)_{\beta < \alpha}$ for a .

Definition 7.7.2 (Strictly Increasing). A sequence (a_β) of ordinals is *strictly increasing* iff, whenever $\beta < \gamma$, then $a_\beta < a_\gamma$.

Definition 7.7.3 (Subsequence). Let $(a_\beta)_{\beta < \gamma}$ be a sequence in \mathbf{A} . A *subsequence* of (a_β) is a sequence of the form $(a_{\beta_\xi})_{\xi < \delta}$ where $(\beta_\xi)_{\xi < \delta}$ is a strictly increasing sequence in γ .

Definition 7.7.4 (Convergence). Let $(a_\beta)_{\beta < \gamma}$ be a sequence of ordinals and λ an ordinal. Then (a_β) *converges* to the *limit* λ iff $\lambda = \sup_{\beta < \gamma} a_\beta$.

Lemma 7.7.5. Let $(a_\beta)_{\beta < \gamma}$ be a sequence of ordinals. Then there is a strictly increasing subsequence $(a_{\beta_\xi})_{\xi < \delta}$ such that $\sup_{\xi < \delta} a_{\beta_\xi} = \sup_{\beta < \gamma} a_\beta$.

PROOF: Define β_ξ by transfinite recursion as follows. β_ξ is the least β such that $a_\beta > a_{\beta_\zeta}$ for all $\zeta < \xi$ if there is such an a_β ; if not, the sequence ends. □

7.8 Strict Supremum

Definition 7.8.1 (Strict Supremum). For any set S of ordinals, define the *strict supremum* of S , $\text{ssup } S$, to be the least ordinal greater than every member of S .

Chapter 8

Cardinal Numbers

8.1 Cardinal Numbers

Definition 8.1.1 (Cardinality). For any set A , the *cardinality* or *cardinal number* $|A|$ of A is the least ordinal equinumerous with A .

Let **Card** be the class of all cardinal numbers.

Proposition 8.1.2. For any sets A and B , we have $A \approx B$ iff $|A| = |B|$.

PROOF: Easy. \square

Definition 8.1.3 (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 $A \cup B \rightarrow A' \cup B'$ that maps $a \in A$ to $f(a)$ and $b \in B$ to $g(b)$ is a bijection.

\square

Proposition 8.1.4. 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 8.1.5 (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 8.1.6. For any cardinal numbers κ and λ we have $\kappa + \lambda = \lambda + \kappa$.

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

Definition 8.1.7 (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 $A \times B \approx A' \times B'$. \square

Proposition 8.1.8. For any cardinal number κ we have $\kappa \cdot 0 = 0$.

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

Proposition 8.1.9. For any cardinal number κ we have $\kappa \cdot 1 = \kappa$.

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

Theorem 8.1.10 (Distributive Law). For any cardinal numbers κ , λ and μ , we have $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$.

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

Theorem 8.1.11 (Associative Law for Multiplication). For any cardinal numbers κ , λ and μ , we have $\kappa(\lambda\mu) = (\kappa\lambda)\mu$.

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

Theorem 8.1.12 (Commutative Law for Multiplication). For any cardinal numbers κ and λ , we have $\kappa\lambda = \lambda\kappa$.

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

Theorem 8.1.13. 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 $B = \emptyset$. \square

Definition 8.1.14 (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 $h : B \rightarrow A$ to $f \circ h \circ g^{-1}$ is a bijection $A^B \approx A'^{B'}$. \square

Proposition 8.1.15. For any cardinal numbers κ , λ and μ ,

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

PROOF: The function that maps $f : A \times B \rightarrow C$ to $\lambda a \in A. \lambda b \in B. f(a, b)$ is a bijection $A^{B \times C} \approx (A^B)^C$. \square

Proposition 8.1.16. For any cardinal numbers κ , λ and μ ,

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

PROOF: The function $f : A^C \times B^C \rightarrow (A \times B)^C$ with $f(g, h)(c) = (g(c), h(c))$ is a bijection. \square

Proposition 8.1.17. *For any cardinal numbers κ , λ and μ , we have*

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

PROOF: If $B \cap C = \emptyset$, then $f : A^B \times A^C \rightarrow A^{B \cup C}$ given by $f(g, h)(b) = g(b)$ and $f(g, h)(c) = h(c)$ is a bijection. \square

Proposition 8.1.18. *For any cardinal number κ , we have $\kappa^0 = 1$.*

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

Proposition 8.1.19. *For any cardinal number κ , we have $\kappa^1 = \kappa$.*

PROOF: For any sets A and B , if $B = \{b\}$ then the function $f : A \rightarrow A^B$ with $f(a)(b) = a$ is a bijection. \square

Proposition 8.1.20. *For any non-zero cardinal number κ we have $0^\kappa = 0$.*

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

Proposition 8.1.21. *For any set A we have $|\mathcal{P}A| = 2^{|A|}$.*

PROOF: The function $f : \mathcal{P}A \rightarrow 2^A$ where $f(X)(a) = 0$ if $a \notin X$ and $f(X)(a) = 1$ if $a \in X$. \square

Theorem 8.1.22 (König). *Let I be a set. Let $\{A_i\}_{i \in I}$ and $\{B_i\}_{i \in I}$ be families of sets. Assume that $\forall i \in I. |A_i| < |B_i|$. Then $|\bigcup_{i \in I} A_i| < |\prod_{i \in I} B_i|$.*

PROOF:

$\langle 1 \rangle 1$. For all $i \in I$, choose an injection $f_i : A_i \rightarrow B_i$

$\langle 1 \rangle 2$. For all $i \in I$, choose $b_i \in B_i - f_i(A_i)$

$\langle 1 \rangle 3$. $|\bigcup_{i \in I} A_i| \leq |\prod_{i \in I} B_i|$

$\langle 2 \rangle 1$. Define $g : \bigcup_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$ by

$$g(i, a)(j) = \begin{cases} f_i(a) & \text{if } i = j \\ b_j & \text{otherwise} \end{cases}$$

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

$\langle 1 \rangle 4$. $|\bigcup_{i \in I} A_i| \neq |\prod_{i \in I} B_i|$

$\langle 2 \rangle 1$. LET: $h : \bigcup_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$

PROVE: h is not surjective.

$\langle 2 \rangle 2$. For $i \in I$, PICK $c_i \in B_i - \{h(i, a)(i) \mid i \in I\}$

$\langle 2 \rangle 3$. $c \in \prod_{i \in I} B_i$

$\langle 2 \rangle 4$. $c \notin \text{ran } h$

\square

Corollary 8.1.22.1. *For any cardinal number κ we have $\kappa < 2^\kappa$.*

8.2 Ordering on Cardinal Numbers

Definition 8.2.1. Given cardinal numbers κ and λ , we have $\kappa \leq \lambda$ iff $A \preccurlyeq B$, where $|A| = \kappa$ and $|B| = \lambda$.

PROOF:

$\langle 1 \rangle 1$. LET: $|A| = \kappa$ and $|B| = \lambda$

$\langle 1 \rangle 2$. PICK bijections $f : A \approx \kappa$ and $g : B \approx \lambda$

$\langle 1 \rangle 3$. If $\kappa \leq \lambda$ then $A \preccurlyeq B$

PROOF: Let $i : \kappa \hookrightarrow \lambda$ be the inclusion. Then $g^{-1} \circ i \circ f$ is an injection $A \rightarrow B$.

$\langle 1 \rangle 4$. If $A \preccurlyeq B$ then $\kappa \leq \lambda$

$\langle 2 \rangle 1$. ASSUME: $A \preccurlyeq B$

$\langle 2 \rangle 2$. PICK an injection $h : A \hookrightarrow B$

$\langle 2 \rangle 3$. $g(h(A)) \subseteq B$ is well-ordered by \in

$\langle 2 \rangle 4$. LET: γ be the ordinal number of $(g(h(A)), \in)$

$\langle 2 \rangle 5$. $\gamma \leq \lambda$

PROOF: Proposition 7.1.23.

$\langle 2 \rangle 6$. $\kappa \leq \gamma$

PROOF: By the leastness of κ , since A is equinumerous with γ .

$\langle 2 \rangle 7$. $\kappa \leq \lambda$

□

Corollary 8.2.1.1. *There is no largest cardinal number.*

Proposition 8.2.2. *For any cardinal numbers κ , λ , μ , if $\kappa \leq \lambda$ then $\kappa + \mu \leq \lambda + \mu$.*

PROOF: If $f : A \rightarrow B$ is injective, and $A \cap C = B \cap C = \emptyset$, then the function $A \cup C \rightarrow B \cup C$ that maps a to $f(a)$ and maps c to c is an injection. □

Proposition 8.2.3. *For any cardinal numbers κ , λ , μ , if $\kappa \leq \lambda$ then $\kappa\mu \leq \lambda\mu$.*

PROOF: If $f : A \rightarrow B$ is injective, then the function $A \times C \rightarrow B \times C$ that maps (a, c) to $(f(a), c)$ is injective. □

Proposition 8.2.4. *For any cardinal numbers κ , λ , μ , if $\kappa \leq \lambda$ then $\kappa^\mu \leq \lambda^\mu$.*

PROOF: Given an injection $f : A \rightarrow B$, the function that maps $A^C \rightarrow B^C$ that maps g to $f \circ g$ is an injection. □

Proposition 8.2.5. *For any cardinal numbers κ , λ , μ , if $\kappa \leq \lambda$ and μ and κ are not both 0, then $\mu^\kappa \leq \mu^\lambda$.*

PROOF:

$\langle 1 \rangle 1$. LET: A , B and C be sets with A and C not both empty.

$\langle 1 \rangle 2$. LET: $f : A \rightarrow B$ be an injection.

PROVE: $C^A \preccurlyeq C^B$

$\langle 1 \rangle 3$. CASE: $C = \emptyset$

PROOF: Then $A \neq \emptyset$ so $C^A = \emptyset \preccurlyeq C^B$.

$\langle 1 \rangle 4$. CASE: $C \neq \emptyset$

- ⟨2⟩1. PICK $c \in C$
 ⟨2⟩2. LET: $g : C^A \rightarrow C^B$ be the function $g(h)(f(a)) = h(a)$, $g(h)(b) = c$ if $b \notin f(A)$
 ⟨2⟩3. g is an injection.
 □

Proposition 8.2.6. *Let \mathcal{A} be a set such that $\forall X \in \mathcal{A}. |X| \leq \kappa$. Then*

$$\left| \bigcup \mathcal{A} \right| \leq |\mathcal{A}| \kappa .$$

PROOF:

- ⟨1⟩1. For $X \in \mathcal{A}$, choose a surjection $f_X : \kappa \rightarrow X$.
 ⟨1⟩2. Define $g : \mathcal{A} \times \kappa \rightarrow \bigcup \mathcal{A}$ by $g(X, \alpha) = f_X(\alpha)$
 ⟨1⟩3. g is surjective.
 □

Lemma 8.2.7. *The union of a set of cardinal numbers is a cardinal number.*

PROOF:

- ⟨1⟩1. LET: A be a set of cardinal numbers.
 PROVE: $\bigcup A$ is the smallest ordinal equinumerous with $\bigcup A$
 ⟨1⟩2. LET: $\alpha < \bigcup A$
 PROVE: $\alpha \not\approx \bigcup A$
 ⟨1⟩3. PICK $\kappa \in A$ such that $\alpha < \kappa$
 ⟨1⟩4. $\alpha \prec \kappa$
 ⟨1⟩5. $\alpha \prec \bigcup A$
 □

Chapter 9

Natural Numbers

9.1 Inductive Sets

Definition 9.1.1 (Inductive). A set I is *inductive* iff $0 \in I$ and $\forall x \in I. x^+ \in I$.

Definition 9.1.2 (Natural Number). A *natural number* is a set that belongs to every inductive set.

Theorem 9.1.3. *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 9.1.4. *\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 9.1.4.1 (Induction Principle for \mathbb{N}). *Any inductive subset of \mathbb{N} coincides with \mathbb{N} .*

Theorem 9.1.5. *Every natural number except 0 is the successor of some natural number.*

PROOF: Trivially by induction. \square

Proposition 9.1.6. *Every natural number is an ordinal.*

PROOF: By induction. \square

Proposition 9.1.7. *\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.

\square

Corollary 9.1.7.1. *\mathbb{N} is an ordinal.*

Definition 9.1.8. We define $\omega = \mathbb{N}$.

Proposition 9.1.9 (Dependent Choice). *Let A be a nonempty set and R a relation on A such that $\forall x \in A. \exists y \in A. (y, x) \in R$. Then there exists a function $f : \mathbb{N} \rightarrow A$ such that $\forall n \in \mathbb{N}. (f(n+1), f(n)) \in R$.*

PROOF:

$\langle 1 \rangle 1.$ PICK a choice function F for A .

$\langle 1 \rangle 2.$ PICK $a \in A$

$\langle 1 \rangle 3.$ Define $f : \mathbb{N} \rightarrow A$ by $f(0) = a$ and $f(n+1) = F(\{y \in A \mid (y, f(n)) \in R\})$.

\square

Theorem Schema 9.1.10. *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem:*

Assume \mathbf{R} is a relation on \mathbf{A} and, for all $a \in \mathbf{A}$, the class $\{x \in \mathbf{A} \mid x\mathbf{R}a\}$ is a set. Then \mathbf{R} is well founded if and only if there does not exist a function $f : \mathbb{N} \rightarrow \mathbf{A}$ such that $\forall n \in \mathbb{N}. f(n+1)\mathbf{R}f(n)$.

PROOF:

$\langle 1 \rangle 1.$ If there exists a function $f : \mathbb{N} \rightarrow \mathbf{A}$ such that $\forall n \in \mathbb{N}. f(n+1)\mathbf{R}f(n)$ then \mathbf{R} is not well founded.

PROOF: $f(\mathbb{N})$ is a nonempty subset of \mathbf{A} with no \mathbf{R} -minimal element.

$\langle 1 \rangle 2.$ If \mathbf{R} is not well founded then there exists a function $f : \mathbb{N} \rightarrow \mathbf{A}$ such that $\forall n \in \mathbb{N}. f(n+1)\mathbf{R}f(n)$.

$\langle 2 \rangle 1.$ ASSUME: \mathbf{R} is not well founded.

$\langle 2 \rangle 2.$ PICK a nonempty subset $B \subseteq \mathbf{A}$ that has no \mathbf{R} -minimal element.

$\langle 2 \rangle 3.$ $\forall x \in B. \exists y \in B. y\mathbf{R}x$

- ⟨2⟩4. Choose a function $g : B \rightarrow B$ such that $\forall x \in B. g(x) \mathbf{R} x$
- ⟨2⟩5. PICK $b \in B$
- ⟨2⟩6. Define $f : \mathbb{N} \rightarrow \mathbf{A}$ recursively by $f(0) = b$ and $\forall n \in \mathbb{N}. f(n+1) = g(f(n))$
- ⟨2⟩7. $\forall n \in \mathbb{N}. f(n+1) \mathbf{R} f(n)$

□

9.2 Cardinality

Definition 9.2.1 (Finite). A set is *finite* iff it is equinumerous to some natural number; otherwise it is *infinite*.

Theorem 9.2.2 (Pigeonhole Principle). *No natural number is equinumerous to a proper subset of itself.*

PROOF:

⟨1⟩1. LET: $P(n)$ be the property: any one-to-one function $n \rightarrow n$ is surjective.

⟨1⟩2. $P(0)$

PROOF: The only function $0 \rightarrow 0$ is injective.

⟨1⟩3. For every natural number n , if $P(n)$ then $P(n+1)$.

⟨2⟩1. ASSUME: $P(n)$

⟨2⟩2. LET: f be a one-to-one function $n+1 \rightarrow n+1$

⟨2⟩3. $f \upharpoonright n$ is a one-to-one function $n \rightarrow n+1$

⟨2⟩4. CASE: $n \notin \text{ran } f$

⟨3⟩1. $f \upharpoonright n : n \rightarrow n$

⟨3⟩2. $\text{ran}(f \upharpoonright n) = n$

⟨3⟩3. $f(n) = n$

PROOF: ⟨2⟩1.

⟨3⟩4. $\text{ran } f = n+1$

⟨2⟩5. CASE: $n \in \text{ran } f$

⟨3⟩1. PICK $p \in n$ such that $f(p) = n$

⟨3⟩2. LET: $\hat{f} : n \rightarrow n$ be the function

$$\hat{f}(p) = f(n)$$

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

⟨3⟩3. \hat{f} is one-to-one

⟨3⟩4. $\text{ran } \hat{f} = n$

PROOF: ⟨2⟩1

⟨3⟩5. $\text{ran } f = n+1$

⟨1⟩4. For every natural number n , $P(n)$.

□

Corollary 9.2.2.1. *No finite set is equinumerous to a proper subset of itself.*

Corollary 9.2.2.2. *Every natural number is a cardinal number.*

PROOF: For any natural number n , we have that n is the least ordinal such that $n \approx n$. □

Corollary 9.2.2.3. \mathbb{N} is a cardinal number.

Corollary 9.2.2.4. \mathbb{N} is infinite.

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

Corollary 9.2.2.5. If C is a proper subset of a natural number n , then there exists $m < n$ such that $C \approx m$.

PROOF: By Proposition 7.1.23. \square

Corollary 9.2.2.6. Any subset of a finite set is finite.

Proposition 9.2.3. For any natural numbers m and n we have $m+n$ (cardinal addition) is a natural number.

PROOF: Induction on n . \square

Corollary 9.2.3.1. The union of two finite sets is finite.

Corollary 9.2.3.2. The union of a finite set of finite sets is finite.

PROOF: By induction on the number of elements. \square

Proposition 9.2.4. For natural numbers m and n , the cardinal sum $m+n$ is equal to the ordinal sum $m+n$.

PROOF: Induction on n . \square

Proposition 9.2.5. For any natural numbers m and n , we have mn (cardinal multiplication) is a natural number.

Corollary 9.2.5.1. If A and B are finite sets then $A \times B$ is finite.

Proposition 9.2.6. For natural numbers m and n , the cardinal product mn is equal to the ordinal product mn .

PROOF: Induction on n . \square

Proposition 9.2.7. For any natural numbers m and n we have m^n (cardinal exponentiation) is a natural number.

PROOF: Induction on n .

Corollary 9.2.7.1. If A and B are finite sets then A^B are finite.

Proposition 9.2.8. For natural numbers m and n , the cardinal exponentiation m^n and the ordinal exponentiation m^n agree.

PROOF: Induction on n . \square

Proposition 9.2.9. $\mathbb{N}^2 \approx \mathbb{N}$

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

Proposition 9.2.10. *For any infinite cardinal κ we have $\aleph_0 \leq \kappa$.*

PROOF:

$\langle 1 \rangle 1$. LET: A be an infinite set.

PROVE: $\aleph_0 \leq A$

$\langle 1 \rangle 2$. PICK a choice function F for A .

$\langle 1 \rangle 3$. Define $h : \mathbb{N} \rightarrow \{X \in \mathcal{P}A \mid X \text{ is finite}\}$ by

$$h(0) = \emptyset$$

$$h(n+1) = h(n) \cup \{F(A - \{h(m) \mid m < n\})\}$$

$\langle 1 \rangle 4$. Define $g : \mathbb{N} \rightarrow A$ by $g(n) = F(A - \{h(m) \mid m < n\})$

$\langle 1 \rangle 5$. g is injective.

PROOF: If $m < n$ then $g(m) \neq g(n)$.

\square

Theorem Schema 9.2.11 (König's Lemma). *For any classes \mathbf{A} and \mathbf{R} , the following is a theorem:*

Assume \mathbf{R} is a well founded relation on \mathbf{A} such that, for all $y \in \mathbf{A}$, the class $\{x \in \mathbf{A} \mid x\mathbf{R}y\}$ is a finite set. Let \mathbf{R}^t be the transitive closure of \mathbf{R} . Then, for all $y \in \mathbf{A}$, the class $\{x \in \mathbf{A} \mid x\mathbf{R}^ty\}$ is a finite set.

PROOF:

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

$\langle 1 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall x\mathbf{R}y. \{z \in \mathbf{A} \mid z\mathbf{R}^tx\}$ is a finite set.

$\langle 1 \rangle 3$. $\{x \mid x\mathbf{R}^ty\} = \bigcup_{x\mathbf{R}y} (\{x\} \cup \{z \mid z\mathbf{R}^tx\})$

$\langle 1 \rangle 4$. $\{x \mid x\mathbf{R}^ty\}$ is finite.

PROOF: Corollary 9.2.3.2.

\square

9.3 Countable Sets

Definition 9.3.1 (Countable). A set A is *countable* iff $|A| \leq \aleph_0$.

Theorem 9.3.2. *The union of a countable set of countable sets is countable.*

PROOF: Proposition 8.2.6. \square

9.4 Arithmetic

Definition 9.4.1 (Even). A natural number n is *even* iff there exists $m \in \mathbb{N}$ such that $n = 2m$.

Definition 9.4.2 (Odd). A natural number n is *odd* iff there exists $p \in \mathbb{N}$ such that $n = 2p + 1$.

Proposition 9.4.3. *Every natural number is either even or odd.*

PROOF:

$\langle 1 \rangle 1$. 0 is even.

PROOF: $0 = 2 \times 0$.

$\langle 1 \rangle 2$. For any natural number n , if n is either even or odd then n^+ is either even or odd.

PROOF:

$\langle 2 \rangle 1$. LET: $n \in \mathbb{N}$

$\langle 2 \rangle 2$. If n is even then n^+ is odd.

PROOF: If $n = 2p$ then $n^+ = 2p + 1$.

$\langle 2 \rangle 3$. If n is odd then n^+ is even.

PROOF: If $n = 2p + 1$ then $n^+ = 2(p + 1)$.

□

Proposition 9.4.4. *No natural number is both even and odd.*

PROOF:

$\langle 1 \rangle 1$. 0 is not odd.

PROOF: For any p we have $2p + 1 = (2p)^+ \neq 0$.

$\langle 1 \rangle 2$. For any natural number n , if n is not both even and odd, then n^+ is not both even and odd.

$\langle 2 \rangle 1$. LET: n be a natural number.

$\langle 2 \rangle 2$. If n^+ is even then n is odd.

$\langle 3 \rangle 1$. ASSUME: n^+ is even.

$\langle 3 \rangle 2$. PICK p such that $n^+ = 2p$

$\langle 3 \rangle 3$. $p \neq 0$

PROOF: Since $n^+ \neq 0$.

$\langle 3 \rangle 4$. PICK q such that $p = q^+$

PROOF: Theorem 9.1.5.

$\langle 3 \rangle 5$. $n^+ = 2q + 2$

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

$\langle 3 \rangle 6$. $n = 2q + 1$

PROOF: Proposition 7.1.15, $\langle 3 \rangle 5$

$\langle 3 \rangle 7$. n is odd.

$\langle 2 \rangle 3$. If n^+ is odd then n is even.

$\langle 3 \rangle 1$. ASSUME: n^+ is odd.

$\langle 3 \rangle 2$. PICK p such that $n^+ = 2p + 1$

$\langle 3 \rangle 3$. $n = 2p$

PROOF: Proposition 7.1.15, $\langle 3 \rangle 2$

$\langle 3 \rangle 4$. n is even.

□

Proposition 9.4.5. *Let m, n, p, q be natural numbers. Assume $m + n = p + q$. Then $m < p$ if and only if $q < n$.*

PROOF:

$\langle 1 \rangle 1$. If $m < p$ then $q < n$.

PROOF: If $m < p$ and $n \leq q$ then $m + n < p + q$.

(1)2. If $q < n$ then $m < p$.

PROOF: Similar.

□

Proposition 9.4.6. *Let m, n, p and q be natural numbers. Assume $n < m$ and $q < p$. Then*

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

PROOF:

(1)1. PICK positive natural numbers a and b such that $m = n + a$ and $p = q + b$.

(1)2. $mp + nq > mq + np$

PROOF:

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

□

9.5 Sequences

Definition 9.5.1 (Sequence). Let A be a set. A *finite sequence* in A is a function $a : n \rightarrow A$ for some natural number n ; we write it as $(a(0), a(1), \dots, a(n - 1))$. An *(infinite) sequence* in A is a function $\mathbb{N} \rightarrow A$.

We write A^* for the set of all finite sequences in A .

Proposition 9.5.2. *If A is countable then A^* is countable.*

PROOF: For any n , the set A^n is countable, and A^* is equinumerous with $\bigcup_n A^n$.

□

9.6 Transitive Closure of a Set

Proposition 9.6.1. *For any set A , there exists a unique transitive set C such that:*

- $A \subseteq C$
- For any transitive set X , if $A \subseteq X$ then $C \subseteq X$

PROOF:

(1)1. Define a function $F : \mathbb{N} \rightarrow \mathbf{V}$ by

$$F(0) = A$$

$$F(n + 1) = A \cup \bigcup (F(0) \cup \dots \cup F(n))$$

- ⟨1⟩2. For all $n \in \mathbb{N}$ and $a \in F(n)$ we have $a \subseteq F(n+1)$
 PROOF: $a \in F(0) \cup \dots \cup F(n)$ so $a \subseteq \bigcup(F(0) \cup \dots \cup F(n)) \subseteq F(n+1)$.
 ⟨1⟩3. LET: $C = \bigcup_{n \in \mathbb{N}} F(n)$
 ⟨1⟩4. C is transitive.
 ⟨2⟩1. LET: $x \in y \in C$
 ⟨2⟩2. PICK $n \in \mathbb{N}$ such that $y \in F(n)$
 ⟨2⟩3. $y \subseteq F(n+1)$
 PROOF: ⟨1⟩2
 ⟨2⟩4. $x \in F(n+1)$
 ⟨2⟩5. $x \in C$
 ⟨1⟩5. $A \subseteq C$
 PROOF: Since $F(0) = A$.
 ⟨1⟩6. For any transitive set X , if $A \subseteq X$ then $C \subseteq X$
 ⟨2⟩1. LET: X be a transitive set
 ⟨2⟩2. ASSUME: $A \subseteq X$
 ⟨2⟩3. For all $n \in \mathbb{N}$ we have $F(n) \subseteq X$.
 ⟨3⟩1. $F(0) \subseteq X$
 PROOF: ⟨2⟩2
 ⟨3⟩2. For all $n \in \mathbb{N}$, if $F(n) \subseteq X$, then $F(n+1) \subseteq X$.
 ⟨4⟩1. LET: $n \in \mathbb{N}$
 ⟨4⟩2. ASSUME: $\forall m < n. F(m) \subseteq X$
 ⟨4⟩3. $F(0) \cup \dots \cup F(n) \subseteq X$
 ⟨4⟩4. $\bigcup(F(0) \cup \dots \cup F(n)) \subseteq X$
 PROOF: Since X is transitive.
 ⟨4⟩5. $F(n+1) \subseteq X$
 ⟨2⟩4. $C \subseteq X$
 ⟨1⟩7. Let D be a transitive set such that $A \subseteq D$ and, for any transitive set X ,
 if $A \subseteq X$ then $D \subseteq X$. Then $D = C$.
 PROOF: We have $C \subseteq D$ and $D \subseteq C$.
 □

Proposition 9.6.2 (ZF). *For any class \mathbf{A} , the relation $\mathbf{E} = \{(x, y) \in \mathbf{A}^2 \mid x \in y\}$ is well founded.*

PROOF:

- ⟨1⟩1. Every nonempty set has an \mathbf{E} -minimal element.
 PROOF: Axiom of Regularity.
 ⟨1⟩2. For every set x , there exists a set u such that $x \subseteq u$ and, for all w, y , if
 $y \in u$ and $w \mathbf{E} y$ then $w \in u$.
 PROOF: Take u to be the transitive closure of x .
 □

9.7 The Veblen Fixed Point Theorem

Theorem Schema 9.7.1 (Veblen Fixed Point Theorem). *For any class \mathbf{T} , the following is a theorem:*

Assume \mathbf{T} is a normal ordinal operation. For every ordinal β , there exists $\gamma \geq \beta$ such that $\mathbf{T}(\gamma) = \gamma$.

PROOF:

$\langle 1 \rangle 1$. LET: β be an ordinal.

$\langle 1 \rangle 2$. ASSUME: w.l.o.g. $\beta < \mathbf{T}(\beta)$

PROOF: We have $\beta \leq \mathbf{T}(\beta)$ by Proposition 7.5.5, and if $\beta = \mathbf{T}(\beta)$ we take $\gamma := \beta$.

$\langle 1 \rangle 3$. Define $f : \mathbb{N} \rightarrow \mathbf{On}$ by recursion thus:

$$f(0) = \beta$$

$$f(n^+) = \mathbf{T}(f(n))$$

$\langle 1 \rangle 4$. LET: $\gamma = \sup_{n \in \mathbb{N}} f(n)$

$\langle 1 \rangle 5$. $\beta \leq \gamma$

PROOF: Since $\beta = f(0)$.

$\langle 1 \rangle 6$. $\mathbf{T}(\gamma) = \gamma$

$\langle 2 \rangle 1$. $\mathbf{T}(\gamma) \leq \gamma$

PROOF:

$$\mathbf{T}(\gamma) = \sup_{n \in \mathbb{N}} \mathbf{T}(f(n)) \quad (\text{Theorem 7.5.7})$$

$$= \sup_{n \in \mathbb{N}} f(n^+) \quad (\langle 1 \rangle 3)$$

$$\leq \sup_{n \in \mathbb{N}} f(n)$$

$$= \gamma$$

$\langle 2 \rangle 2$. $\gamma \leq \mathbf{T}(\gamma)$

PROOF: Proposition 7.5.5.

□

Definition 9.7.2 (Derived Operation). Let \mathbf{T} be a normal ordinal operation. The *derived* operation $\mathbf{T}' : \mathbf{On} \rightarrow \mathbf{V}$ is the unique order isomorphism between \mathbf{On} and the fixed points of \mathbf{T} .

Proposition Schema 9.7.3. For any class \mathbf{T} , the following is a theorem:

If \mathbf{T} is a normal ordinal operation, then the derived operation is normal.

PROOF:

$\langle 1 \rangle 1$. For any set S of fixed points of \mathbf{T} , we have $\bigcup S$ is a fixed point of \mathbf{T}

$\langle 2 \rangle 1$. LET: S be a set of fixed points of \mathbf{T} .

$\langle 2 \rangle 2$. $\mathbf{T}(\sup S) = \sup S$

PROOF:

$$\mathbf{T}(\sup S) = \sup_{\alpha \in S} \mathbf{T}(\alpha) \quad (\text{Theorem 7.5.7})$$

$$= \sup_{\alpha \in S} \alpha \quad (\langle 2 \rangle 1)$$

$$= \sup S$$

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

PROOF: Proposition 7.5.8.

□

9.8 Cantor Normal Form

Theorem 9.8.1. *For any ordinal α , there exist a unique sequence of nonzero natural numbers (n_1, \dots, n_k) and sequence of ordinals $(\gamma_1, \dots, \gamma_k)$ such that*

$$\gamma_k < \gamma_{k-1} < \dots < \gamma_1$$

and

$$\alpha = \omega^{\gamma_1} n_1 + \omega^{\gamma_2} n_2 + \dots + \omega^{\gamma_k} n_k .$$

PROOF:

$\langle 1 \rangle 1$. For any ordinal α , there exist a sequence of nonzero natural numbers (n_1, \dots, n_k) and sequence of ordinals $(\gamma_1, \dots, \gamma_k)$ such that

$$\gamma_k < \gamma_{k-1} < \dots < \gamma_1$$

and

$$\alpha = \omega^{\gamma_1} n_1 + \omega^{\gamma_2} n_2 + \dots + \omega^{\gamma_k} n_k .$$

$\langle 2 \rangle 1$. LET: α be an ordinal

$\langle 2 \rangle 2$. ASSUME: as an induction hypothesis that, for all $\beta < \alpha$, the theorem holds.

$\langle 2 \rangle 3$. ASSUME: w.l.o.g. $\alpha \neq 0$

$\langle 2 \rangle 4$. LET: γ_1, n_1, ρ_1 be the unique ordinals such that $0 \neq n_1 < \omega$, $\rho_1 < \omega^{\gamma_1}$, and $\alpha = \omega^{\gamma_1} n_1 + \rho_1$

$\langle 2 \rangle 5$. LET: $(\gamma_2, \dots, \gamma_k)$ and (n_2, \dots, n_k) be sequences such that $\gamma_k < \gamma_{k-1} < \dots < \gamma_2$ and $\rho_1 = \omega^{\gamma_2} n_2 + \dots + \omega^{\gamma_k} n_k$

$\langle 2 \rangle 6$. $\gamma_2 < \gamma_1$

PROOF: Since $\omega^{\gamma_2} \leq \rho_1 < \omega^{\gamma_1}$

$\langle 1 \rangle 2$. If

$$\begin{aligned} \gamma_k &< \gamma_{k-1} < \dots < \gamma_1 \\ \gamma'_k &< \gamma'_{k-1} < \dots < \gamma'_1 \end{aligned}$$

and

$$\omega^{\gamma_1} n_1 + \omega^{\gamma_2} n_2 + \dots + \omega^{\gamma_k} n_k = \omega^{\gamma'_1} n'_1 + \omega^{\gamma'_2} n'_2 + \dots + \omega^{\gamma'_k} n'_k$$

then $\gamma_i = \gamma'_i$ for all i and $n_i = n'_i$ for all i

PROOF: Prove by induction on i using the Logarithm Theorem.

□

Definition 9.8.2 (Cantor Normal Form). For any ordinal α , the *Cantor normal form* of α is the expression $\alpha = \omega^{\gamma_1} n_1 + \dots + \omega^{\gamma_k} n_k$ such that n_1, \dots, n_k are nonzero natural numbers and $\gamma_k < \gamma_{k-1} < \dots < \gamma_1$.

Chapter 10

The Cumulative Hierarchy

Definition 10.0.1 (Cumulative Hierarchy (ZF)). Define the function $V : \mathbf{On} \rightarrow \mathbf{V}$ by transfinite recursion thus:

$$V_\alpha = \bigcup_{\beta < \alpha} \mathcal{P}V_\beta$$

Proposition 10.0.2 (ZF). *For all $\alpha \in \mathbf{On}$, V_α is a transitive set.*

PROOF:

$\langle 1 \rangle 1$. LET: $\alpha \in \mathbf{On}$

$\langle 1 \rangle 2$. ASSUME: as transfinite induction hypothesis $\forall \beta < \alpha. V_\beta$ is a transitive set.

$\langle 1 \rangle 3$. For all $\beta < \alpha$, $\mathcal{P}V_\beta$ is a transitive set.

PROOF: Proposition 1.6.4.

$\langle 1 \rangle 4$. V_α is a transitive set.

PROOF: Proposition 1.6.3.

□

Proposition 10.0.3 (ZF). *For any ordinals α and β , if $\beta < \alpha$ then $V_\beta \subseteq V_\alpha$.*

PROOF: Since $V_\beta \in \mathcal{P}V_\beta \subseteq V_\alpha$ and V_α is a transitive set. □

Theorem 10.0.4 (ZF).

1. $V_0 = \emptyset$

2. $\forall \alpha \in \mathbf{On}. V_{\alpha+} = \mathcal{P}V_\alpha$

3. For any limit ordinal λ , $V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha$.

PROOF:

$\langle 1 \rangle 1$. $V_0 = \emptyset$

PROOF: Immediate from definition.

$\langle 1 \rangle 2$. $\forall \alpha \in \mathbf{On}. V_{\alpha+} = \mathcal{P}V_\alpha$

PROOF:

- ⟨2⟩1. LET: $\alpha \in \mathbf{On}$
 ⟨2⟩2. For all $\beta < \alpha$ we have $\mathcal{P}V_\beta \subseteq \mathcal{P}V_\alpha$
 PROOF: Propositions 1.5.9 and 10.0.3.
 ⟨2⟩3. $V_{\alpha^+} = \mathcal{P}V_\alpha$

$$\begin{aligned}
 V_{\alpha^+} &= \bigcup_{\beta < \alpha^+} \mathcal{P}V_\beta \\
 &= \bigcup_{\beta < \alpha} \mathcal{P}V_\beta \cup \mathcal{P}V_\alpha \\
 &\quad \mathcal{P}V_\alpha
 \end{aligned}$$

□

- ⟨1⟩3. For any limit ordinal λ , $V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha$

PROOF:

- ⟨2⟩1. $V_\lambda \subseteq \bigcup_{\alpha < \lambda} V_\alpha$

PROOF:

$$\begin{aligned}
 V_\lambda &= \bigcup_{\alpha < \lambda} \mathcal{P}V_\alpha \\
 &= \bigcup_{\alpha < \lambda} V_{\alpha^+} & (\langle 1 \rangle 2) \\
 &\subseteq \bigcup_{\alpha < \lambda} V_\alpha
 \end{aligned}$$

- ⟨2⟩2. $\bigcup_{\alpha < \lambda} V_\alpha \subseteq V_\lambda$

PROOF: Proposition 10.0.3.

□

Proposition 10.0.5 (ZF). *For every set A , there exists an ordinal α such that $A \in V_\alpha$.*

PROOF:

- ⟨1⟩1. Let us say a set A is *grounded* iff there exists an ordinal α such that $A \in V_\alpha$.
 ⟨1⟩2. For any set A , if every element of A is grounded, then A is grounded.
 ⟨2⟩1. LET: A be a set.
 ⟨2⟩2. $S = \{\alpha \mid \exists a \in A. \alpha \text{ is the least ordinal such that } a \in V_\alpha\}$
 PROOF: S is a set by an Axiom of Replacement.
 ⟨2⟩3. LET: $\beta = \sup S$
 ⟨2⟩4. $A \subseteq V_\beta$
 ⟨3⟩1. LET: $a \in A$
 ⟨3⟩2. LET: α be the least ordinal such that $a \in V_\alpha$
 ⟨3⟩3. $\alpha \in S$
 ⟨3⟩4. $\alpha \leq \beta$
 ⟨3⟩5. $a \in V_\beta$
 ⟨2⟩5. $A \in V_{\beta^+}$
 ⟨1⟩3. ASSUME: for a contradiction there exists an ungrounded set.
 ⟨1⟩4. PICK a transitive set B that has an ungrounded member.
 PROOF: Pick a transitive set c , and take B to be the transitive closure of $\{c\}$.

- ⟨1⟩5. LET: $A = \{x \in B \mid x \text{ is ungrounded}\}$
 ⟨1⟩6. PICK $m \in A$ such that $m \cap A = \emptyset$
 PROOF: Axiom of Regularity.
 ⟨1⟩7. Every member of m is grounded.
 ⟨2⟩1. ASSUME: for a contradiction $x \in m$ is ungrounded.
 ⟨2⟩2. $x \in B$
 PROOF: Since B is transitive (⟨1⟩4).
 ⟨2⟩3. $x \in A$
 PROOF: ⟨1⟩5
 ⟨2⟩4. Q.E.D.
 PROOF: This contradicts ⟨1⟩6.
 ⟨1⟩8. m is grounded.
 PROOF: ⟨1⟩2
 ⟨1⟩9. Q.E.D.
 PROOF: This contradicts ⟨1⟩6.
 □

Definition 10.0.6 (Rank (ZF)). The *rank* of a set A is the least ordinal α such that $A \in V_{\alpha^+}$.

Proposition 10.0.7 (ZF). For any set A we have

$$\text{rank } A = \bigcup_{a \in A} (\text{rank } a)^+$$

PROOF:

- ⟨1⟩1. LET: $\alpha = \bigcup_{a \in A} (\text{rank } a)^+$
 ⟨1⟩2. $A \subseteq V_\alpha$
 ⟨2⟩1. LET: $a \in A$
 ⟨2⟩2. $a \in V_{(\text{rank } a)^+}$
 ⟨2⟩3. $a \in V_\alpha$
 ⟨1⟩3. $A \in V_{\alpha^+}$
 ⟨1⟩4. If $A \subseteq V_\beta$ then $\alpha \leq \beta$
 ⟨2⟩1. ASSUME: $A \subseteq V_\beta$
 ⟨2⟩2. For all $a \in A$ we have $(\text{rank } a)^+ \leq \beta$
 PROOF: Since $a \in V_\beta$.
 ⟨2⟩3. $\alpha \leq \beta$
 □

Corollary 10.0.7.1 (ZF). For any sets a and b , if $a \in b$ then $\text{rank } a < \text{rank } b$.

Proposition 10.0.8 (ZF). For any ordinal number α we have $\text{rank } \alpha = \alpha$.

PROOF:

- ⟨1⟩1. LET: α be an ordinal.
 ⟨1⟩2. ASSUME: as transfinite induction hypothesis $\forall \beta < \alpha. \text{rank } \beta = \beta$
 ⟨1⟩3. $\text{rank } \alpha = \bigcup_{\beta < \alpha} \beta^+$

PROOF:

$$\begin{aligned}\text{rank } \alpha &= \bigcup_{\beta < \alpha} (\text{rank } \beta)^+ \\ &= \bigcup_{\beta < \alpha} \beta^+\end{aligned}$$

$$\langle 1 \rangle 4. \bigcup_{\beta < \alpha} \beta^+ \leq \alpha$$

PROOF: Since for all $\beta < \alpha$ we have $\beta^+ \leq \alpha$.

$$\langle 1 \rangle 5. \alpha \leq \bigcup_{\beta < \alpha} \beta^+$$

$$\langle 2 \rangle 1. \text{ LET: } \gamma = \bigcup_{\beta < \alpha} \beta^+$$

$$\langle 2 \rangle 2. \text{ ASSUME: for a contradiction } \gamma < \alpha$$

$$\langle 2 \rangle 3. \gamma^+ \leq \bigcup_{\beta < \alpha} \beta^+ = \gamma$$

$$\langle 2 \rangle 4. \text{ Q.E.D.}$$

PROOF: This is a contradiction.

□

Definition 10.0.9 (Hereditarily Finite (ZF)). A set is *hereditarily finite* iff it is in V_ω .

Proposition 10.0.10 (ZF). V_ω is the smallest set X such that $\emptyset \in X$ and every finite subset of X is an element of X .

Chapter 11

Models of Set Theory

Definition 11.0.1 (Relativization). Let σ be a sentence in the language of set theory and \mathbf{M} a class. The *relativization* of σ to \mathbf{M} is the sentence $\sigma^{\mathbf{M}}$ formed by replacing every quantifier $\forall x$ with $\forall x \in \mathbf{M}$, and $\exists x$ with $\exists x \in \mathbf{M}$.

We write ' \mathbf{M} is a model of σ ' for the sentence $\sigma^{\mathbf{M}}$.

Theorem Schema 11.0.2. *For any class \mathbf{M} , the following is a theorem:*

If \mathbf{M} is a transitive class, then \mathbf{M} is a model of the Axiom of Extensionality.

PROOF:

$\langle 1 \rangle 1$. ASSUME: \mathbf{M} is a transitive class.

PROVE: $\forall x, y \in \mathbf{M} (\forall z \in \mathbf{M} (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$

$\langle 1 \rangle 2$. LET: $x, y \in \mathbf{M}$

$\langle 1 \rangle 3$. ASSUME: $\forall z \in \mathbf{M} (z \in x \Leftrightarrow z \in y)$

$\langle 1 \rangle 4$. $\forall z (z \in x \Leftrightarrow z \in y)$

PROOF: Since $z \in x \Rightarrow z \in \mathbf{M}$ and $z \in y \Rightarrow z \in \mathbf{M}$ by $\langle 1 \rangle 1$.

$\langle 1 \rangle 5$. $x = y$

□

Theorem 11.0.3. *If α is a non-zero ordinal then V_α is a model of the statement: The empty class is a set.*

PROOF:

$\langle 1 \rangle 1$. LET: $\alpha \neq 0$

PROVE: $\exists x \in V_\alpha. \forall y \in V_\alpha. y \notin x$

$\langle 1 \rangle 2$. $\emptyset \in V_\alpha$

$\langle 1 \rangle 3$. $\forall y \in V_\alpha. y \notin \emptyset$

□

Theorem 11.0.4. *For any limit ordinal λ , we have V_λ is a model of the statement: for any sets a and b , the class $\{a, b\}$ is a set.*

PROOF:

$\langle 1 \rangle 1$. LET: λ be a limit ordinal.

PROVE: $\forall a, b \in V_\lambda. \exists c \in V_\lambda. \forall x \in V_\lambda (x \in c \Leftrightarrow x = a \vee x = b)$
 (1)2. LET: $a, b \in V_\lambda$
 (1)3. PICK $\alpha, \beta < \lambda$ such that $a \in V_\alpha$ and $b \in V_\beta$
 (1)4. ASSUME: w.l.o.g. $\alpha \leq \beta$
 (1)5. $a, b \in V_\beta$
 (1)6. $\{a, b\} \in V_{\beta+1}$
 (1)7. $\{a, b\} \in V_\lambda$
 (1)8. $\forall x \in V_\lambda (x \in \{a, b\} \Leftrightarrow x = a \vee x = b)$
 \square

Theorem 11.0.5. *For any ordinal α , we have V_α is a model of the Union Axiom.*

PROOF:

(1)1. LET: α be an ordinal.
 PROVE: $\forall a \in V_\alpha. \exists b \in V_\alpha. \forall x \in V_\alpha (x \in b \Leftrightarrow \exists y \in V_\alpha (x \in y \wedge y \in a))$
 (1)2. LET: $a \in V_\alpha$
 (1)3. PICK $\beta < \alpha$ such that $a \subseteq V_\beta$
 (1)4. $\bigcup a \subseteq V_\beta$
 PROOF: V_β is a transitive set.
 (1)5. $\bigcup a \in V_\alpha$
 (1)6. $\forall x \in V_\alpha (x \in \bigcup a \Leftrightarrow \exists y \in V_\alpha (x \in y \wedge y \in a))$
 PROOF: V_α is a transitive set.
 \square

Theorem 11.0.6. *For any limit ordinal λ , we have V_λ is a model of the Power Set Axiom.*

PROOF:

(1)1. LET: λ be a limit ordinal.
 PROVE: $\forall a \in V_\lambda. \exists b \in V_\lambda. \forall x \in V_\lambda (x \in b \Leftrightarrow \forall y \in V_\lambda (y \in x \Rightarrow y \in a))$
 (1)2. LET: $a \in V_\lambda$
 (1)3. PICK $\alpha < \lambda$ such that $a \in V_\alpha$
 (1)4. $\mathcal{P}a \in V_{\alpha+1}$
 (1)5. $\mathcal{P}a \in V_\lambda$
 (1)6. $\forall x \in V_\lambda (x \in \mathcal{P}a \Leftrightarrow \forall y \in V_\lambda (y \in x \Rightarrow y \in a))$
 \square

Theorem Schema 11.0.7. *For any property $P[x, y_1, \dots, y_n]$, the following is a theorem:*

For any ordinal α , the set V_α is a model of the statement: for any sets a_1, \dots, a_n, B , the class $\{x \in B \mid P[x, a_1, \dots, a_n]\}$ is a set.

PROOF:

(1)1. LET: α be an ordinal.
 (1)2. LET: $a_1, \dots, a_n, B \in V_\alpha$
 (1)3. LET: $C = \{x \in B \mid P[x, a_1, \dots, a_n]^{V_\alpha}\}$
 (1)4. $C \in V_\alpha$

$\langle 1 \rangle 5. \forall x \in V_\alpha (x \in C \Leftrightarrow x \in B \wedge P[x, a_1, \dots, a_n]^{V_\alpha})$

□

Theorem 11.0.8. *For any ordinal $\alpha > \omega$, we have: V_α is a model of the Axiom of Infinity.*

PROOF:

$\langle 1 \rangle 1.$ LET: $\alpha > \omega$

$\langle 1 \rangle 2.$ $\mathbb{N} \in V_\alpha$

$\langle 1 \rangle 3.$ $\exists e \in V_\alpha (e \in \mathbb{N} \wedge \forall x \in V_\alpha. x \notin e)$

$\langle 1 \rangle 4.$ $\forall x \in V_\alpha (x \in \mathbb{N} \Rightarrow \exists y \in V_\alpha \forall z \in V_\alpha (z \in y \Leftrightarrow z \in x \vee z = x))$

□

Theorem 11.0.9. *For any ordinal α , we have V_α is a model of the Axiom of Choice.*

PROOF:

$\langle 1 \rangle 1.$ LET: α be an ordinal.

$\langle 1 \rangle 2.$ LET: $A \in V_\alpha$

$\langle 1 \rangle 3.$ ASSUME: $\forall x \in V_\alpha (x \in A \Rightarrow \exists y \in V_\alpha. y \in A)$

$\langle 1 \rangle 4.$ ASSUME: $\forall x, y, z \in V_\alpha (x \in A \wedge y \in A \wedge z \in x \wedge z \in y \Rightarrow x = y)$

$\langle 1 \rangle 5.$ A is a set of pairwise disjoint nonempty sets.

$\langle 1 \rangle 6.$ PICK c such that, for all $x \in A$, $x \cap c = \emptyset$

$\langle 1 \rangle 7.$ $c \cap \bigcup A \in V_\alpha$

$\langle 1 \rangle 8.$ $\forall x \in V_\alpha (x \in A \Rightarrow \exists y \in V_\alpha \forall z \in V_\alpha (z \in x \wedge z \in c \cap \bigcup A \Leftrightarrow z = y))$

□

Theorem 11.0.10. *For any ordinal α , we have V_α is a model of the Axiom of Regularity.*

PROOF:

$\langle 1 \rangle 1.$ LET: α be an ordinal.

$\langle 1 \rangle 2.$ LET: $A \in V_\alpha$

$\langle 1 \rangle 3.$ ASSUME: $\exists x \in V_\alpha. x \in A$

$\langle 1 \rangle 4.$ PICK $m \in A$ of least rank.

$\langle 1 \rangle 5.$ $m \in V_\alpha$

$\langle 1 \rangle 6.$ $\neg \exists x \in V_\alpha (x \in m \wedge x \in A)$

□

Theorem Schema 11.0.11. *For any axiom α of Zermelo set theory, the following is a theorem:*

For any limit ordinal $\lambda > \omega$, we have V_λ is a model of α .

PROOF: Theorems 11.0.2, 11.0.3, 11.0.4, 11.0.5, 11.0.6, 11.0.7, 11.0.8, 11.0.9, 11.0.10. □

Corollary Schema 11.0.11.1. *for any axiom α of Zermelo set theory, the following is a theorem:*

V_{ω_2} is a model of α .

Lemma 11.0.12. *There exists a well-ordered structure in V_{ω^2} whose ordinal is not in V_{ω^2} .*

PROOF: Take the well-ordered set $\mathbb{N} \times \{0, 1\}$ whose ordinal is ω^2 . \square

Corollary Schema 11.0.12.1. *There exists an instance α of the Axiom Schema of Replacement such that the following is a theorem:
 V_{ω^2} is not a model of α .*

Chapter 12

Infinite Cardinals

12.1 Arithmetic of Infinite Cardinals

Proposition 12.1.1. *For any infinite cardinal κ we have $\kappa\kappa = \kappa$.*

PROOF:

- $\langle 1 \rangle 1$. PICK a set B with $|B| = \kappa$
- $\langle 1 \rangle 2$. LET: $\mathcal{H} = \{f \mid f = \emptyset \vee \exists A \subseteq B. (A \text{ is infinite} \wedge f : A \times A \approx A)\}$
- $\langle 1 \rangle 3$. For any chain $\mathcal{C} \subseteq \mathcal{H}$ we have $\bigcup \mathcal{C} \in \mathcal{H}$
 - $\langle 2 \rangle 1$. LET: $\mathcal{C} \subseteq \mathcal{H}$ be a chain.
 - $\langle 2 \rangle 2$. ASSUME: w.l.o.g. \mathcal{C} has a nonempty element.
 - $\langle 2 \rangle 3$. $\bigcup \mathcal{C}$ is a function.
 - $\langle 3 \rangle 1$. ASSUME: $(x, y), (x, z) \in \bigcup \mathcal{C}$
 - $\langle 3 \rangle 2$. PICK $f, g \in \mathcal{C}$ such that $f(x) = y$ and $g(x) = z$
 - $\langle 3 \rangle 3$. ASSUME: w.l.o.g. $f \subseteq g$
 - $\langle 3 \rangle 4$. $y = z$
 - $\langle 2 \rangle 4$. $\bigcup \mathcal{C}$ is injective.
- PROOF: Similar.
- $\langle 2 \rangle 5$. LET: $A = \text{ran } \bigcup \mathcal{C}$
- $\langle 2 \rangle 6$. A is infinite.
 - $\langle 3 \rangle 1$. PICK a nonzero $f \in \mathcal{C}$
 - $\langle 3 \rangle 2$. LET: A' be the infinite subset of B such that $f : A'^2 \approx A'$
 - $\langle 3 \rangle 3$. $A' \subseteq A$
- $\langle 2 \rangle 7$. $\text{dom } \bigcup \mathcal{C} = A^2$
 - $\langle 3 \rangle 1$. LET: $x, y \in A$
 - $\langle 3 \rangle 2$. PICK $f, g \in \mathcal{C}$ such that $x \in \text{ran } f$ and $y \in \text{ran } g$
 - $\langle 3 \rangle 3$. ASSUME: w.l.o.g. $f \subseteq g$
 - $\langle 3 \rangle 4$. LET: A' be the infinite subset of B such that $g : A'^2 \approx A'$
 - $\langle 3 \rangle 5$. $x, y \in A'$
 - $\langle 3 \rangle 6$. $(x, y) \in \text{dom } g$
 - $\langle 3 \rangle 7$. $(x, y) \in \text{dom } \bigcup \mathcal{C}$
- $\langle 2 \rangle 8$. $\bigcup \mathcal{C} \in \mathcal{H}$

- ⟨1⟩4. PICK a maximal $f_0 \in \mathcal{H}$
- ⟨1⟩5. $f_0 \neq \emptyset$
 - ⟨2⟩1. PICK a countably infinite subset A of B .
PROOF: Proposition 9.2.10.
 - ⟨2⟩2. PICK a bijection $f : A^2 \approx A$
PROOF: Proposition 9.2.9.
 - ⟨2⟩3. $\emptyset \subseteq f \in \mathcal{H}$
 - ⟨2⟩4. \emptyset is not maximal in \mathcal{H}
- ⟨1⟩6. LET: A_0 be the infinite subset of B such that $f_0 : A_0^2 \approx A_0$
- ⟨1⟩7. LET: $\lambda = |A_0|$
- ⟨1⟩8. λ is infinite.
- ⟨1⟩9. $\lambda^2 = \lambda$
- ⟨1⟩10. $\lambda = \kappa$
 - ⟨2⟩1. ASSUME: for a contradiction $\lambda < \kappa$
 - ⟨2⟩2. $\lambda \leq |B - A_0|$
 - ⟨2⟩3. PICK a subset $D \subseteq B - A_0$ with $|D| = \lambda$
 - ⟨2⟩4. $(A_0 \cup D)^2 = A_0^2 \cup (A_0 \times D) \cup (D \times A_0) \cup D^2$
 - ⟨2⟩5. LET: $C = (A_0 \times D) \cup (D \times A_0) \cup D^2$
 - ⟨2⟩6. $|C| = \lambda$
PROOF:

$$|(A_0 \times D) \cup (D \times A_0) \cup D^2| = \lambda^2 + \lambda^2 + \lambda^2$$

$$= \lambda + \lambda + \lambda \quad (\langle 1 \rangle 9)$$

$$= 3\lambda$$

$$\leq \lambda \cdot \lambda$$

$$= \lambda \quad (\langle 1 \rangle 9)$$
 - ⟨2⟩7. PICK a bijection $g : C \approx D$
 - ⟨2⟩8. $f_0 \cup g : (A_0 \cup D)^2 \approx A_0 \cup D$
 - ⟨2⟩9. Q.E.D.

PROOF: This contradicts the maximality of f_0 .

□

Theorem 12.1.2 (Absorption Law of Cardinal Arithmetic). *Let κ and λ be nonzero cardinal numbers such that at least one is infinite. Then*

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

PROOF:

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

PROOF:

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

(Proposition 12.1.1)

□

12.2 Alephs

Definition 12.2.1 (Aleph). Let \aleph be the unique order isomorphism between \mathbf{On} and the class of infinite cardinals.

Proposition 12.2.2. *The operation \aleph is normal.*

PROOF: Proposition 7.5.8 and Lemma 8.2.7. □

Definition 12.2.3 (Continuum Hypothesis). The *continuum hypothesis* is the statement that $\aleph_1 = 2^{\aleph_0}$.

Definition 12.2.4 (Generalised Continuum Hypothesis). The *generalised continuum hypothesis* is the statement that, for all α , $\aleph_{\alpha+} = 2^{\aleph_\alpha}$.

12.3 Beths

Definition 12.3.1 (Beth). Define the operation $\beth : \mathbf{On} \rightarrow \mathbf{Card}$ by transfinite recursion as follows:

$$\begin{aligned}
 \beth_0 &:= \aleph_0 \\
 \beth_{\alpha+} &:= 2^{\beth_\alpha} \\
 \beth_\lambda &:= \bigcup_{\alpha < \lambda} \beth_\alpha \quad (\lambda \text{ a limit ordinal})
 \end{aligned}$$

Proposition 12.3.2. *\beth is a normal operation.*

PROOF: It is continuous by definition, and $\beth_\alpha < \beth_{\alpha+}$ by Cantor's Theorem. □

Proposition 12.3.3. *The continuum hypothesis is equivalent to the statement $\beth_1 = \aleph_1$.*

The generalised continuum hypothesis is equivalent to the statement $\beth = \aleph$.

PROOF: Immediate from definitions. □

Lemma 12.3.4. *For any ordinal number α , we have $|V_{\omega+\alpha}| = \beth_\alpha$.*

PROOF:

(1)1. $|V_\omega| = \beth_0$

PROOF: Since V_ω is the union of \aleph_0 finite sets of increasing size.

(1)2. For any ordinal α , if $|V_{\omega+\alpha}| = \beth_\alpha$ then $|V_{\omega+\alpha+1}| = \beth_{\alpha+1}$

PROOF: Since $V_{\omega+\alpha+1} = \mathcal{P}V_{\omega+\alpha}$.

(1)3. For any limit ordinal λ , if $\forall \alpha < \lambda. |V_{\omega+\alpha}| = \beth_\alpha$ then $|V_{\omega+\lambda}| = \beth_\lambda$.

PROOF:

$$\begin{aligned} |V_{\omega+\lambda}| &= \left| \bigcup_{\alpha < \lambda} V_{\omega+\alpha} \right| \\ &= \sup_{\alpha < \lambda} |V_{\omega+\alpha}| \\ &= \sup_{\alpha < \lambda} \beth_\alpha \\ &= \beth_\lambda \end{aligned}$$

□

12.4 Cofinality

Definition 12.4.1 (Cofinal). Let λ be a limit ordinal and S a set of ordinals smaller than λ . Then S is *cofinal* in λ if and only if $\lambda = \sup S$.

Definition 12.4.2 (Cofinality). For any ordinal α , define the *cofinality* of α , $\text{cf } \alpha$, as follows:

- $\text{cf } 0 = 0$
- For any ordinal α , $\text{cf } \alpha^+ = 1$
- For any limit ordinal λ , $\text{cf } \lambda$ is the smallest cardinal such that there exists a set S of ordinals cofinal in λ with $|S| = \text{cf } \lambda$.

Definition 12.4.3 (Regular). A cardinal κ is *regular* iff $\text{cf } \kappa = \kappa$; otherwise it is *singular*.

Proposition 12.4.4. \aleph_0 is regular.

PROOF: \aleph_0 is not the supremum of $< \aleph_0$ smaller ordinals, because a finite union of finite ordinals is finite. □

Proposition 12.4.5. For every ordinal α , $\aleph_{\alpha+1}$ is regular.

PROOF: If S is a set of ordinals with $|S| < \aleph_{\alpha+1}$ and $\forall \beta \in S. \beta < \aleph_{\alpha+1}$, then we have $|S| \leq \aleph_\alpha$ and $\forall \beta \in S. \beta \leq \aleph_\alpha$, hence

$$\begin{aligned} \left| \bigcup S \right| &\leq \aleph_\alpha^2 && \text{(Proposition 8.2.6)} \\ &= \aleph_\alpha && \text{(Proposition 12.1.1)} \end{aligned}$$

Proposition Schema 12.4.6. For any class \mathbf{T} , the following is a theorem.

Assume $\mathbf{T} : \mathbf{On} \rightarrow \mathbf{On}$ is a normal operation. For any limit ordinal λ we have $\text{cf } \mathbf{T}(\lambda) = \text{cf } \lambda$.

PROOF:

- $\langle 1 \rangle 1.$ $\text{cf } \mathbf{T}(\lambda) \leq \text{cf } \lambda$
 - $\langle 2 \rangle 1.$ PICK a set S of ordinals $< \lambda$ with $|S| = \text{cf } \lambda$ and $\sup S = \lambda$
 - $\langle 2 \rangle 2.$ $\mathbf{T}(\lambda) = \sup_{\alpha \in S} \mathbf{T}(\alpha)$
PROOF: Theorem 7.5.7.
- $\langle 1 \rangle 2.$ $\text{cf } \lambda \leq \text{cf } \mathbf{T}(\lambda)$
 - $\langle 2 \rangle 1.$ PICK a set A of ordinals $< \mathbf{T}(\lambda)$ such that $|A| = \text{cf } \mathbf{T}(\lambda)$ and $\sup A = \mathbf{T}(\lambda)$
 - $\langle 2 \rangle 2.$ LET: $B = \{\gamma < \lambda \mid \exists \alpha \in A. |\alpha| = \mathbf{T}(\gamma)\}$
 - $\langle 2 \rangle 3.$ $|B| \leq |A| = \text{cf } \mathbf{T}(\lambda)$
PROVE: $\sup B = \lambda$
 - $\langle 2 \rangle 4.$ $\forall \alpha \in A. |\alpha| \leq \mathbf{T}(\sup B)$
 - $\langle 2 \rangle 5.$ $\forall \alpha \in A. \alpha < \mathbf{T}(\sup B + 1)$
 - $\langle 2 \rangle 6.$ $\aleph_\lambda = \sup A \leq \mathbf{T}(\sup B + 1)$
 - $\langle 2 \rangle 7.$ $\lambda \leq \sup B + 1$
 - $\langle 2 \rangle 8.$ $\lambda \leq \sup B$
PROOF: λ is a limit ordinal.
 - $\langle 2 \rangle 9.$ $\sup B = \lambda$

□

Corollary 12.4.6.1. \aleph_ω is singular.

PROOF: $\text{cf } \aleph_\omega = \text{cf } \aleph_0 = \aleph_0$. □

Corollary 12.4.6.2. The operation cf is not strictly monotone or continuous.

PROOF: $\text{cf } \aleph_\omega < \text{cf } \aleph_1$ □

Definition 12.4.7 (Weakly Inaccessible). A cardinal is *weakly inaccessible* iff it is \aleph_λ for some limit ordinal λ and regular.

Lemma 12.4.8. Let λ be a limit ordinal. Then there exists a strictly increasing $\text{cf } \lambda$ -sequence that converges to λ .

PROOF:

- $\langle 1 \rangle 1.$ PICK a set S of ordinals $< \lambda$ with $|S| = \text{cf } \lambda$ and $\sup S = \lambda$
- $\langle 1 \rangle 2.$ PICK a bijection $a : \text{cf } \lambda \approx S$
- $\langle 1 \rangle 3.$ PICK a strictly increasing subsequence $(b_\delta)_{\delta < \beta}$ of a that converges to λ .
PROOF: Lemma 7.7.5.
- $\langle 1 \rangle 4.$ $\beta = \text{cf } \lambda$
PROOF: By minimality of $\text{cf } \lambda$.

□

Corollary 12.4.8.1. Let λ be a limit ordinal. Then $\text{cf } \lambda$ is the least ordinal such that there exists a strictly increasing $\text{cf } \lambda$ -sequence that converges to λ .

Proposition 12.4.9. For any ordinal λ , $\text{cf } \lambda$ is a regular cardinal.

PROOF:

- (1)1. LET: λ be an ordinal.
 (1)2. ASSUME: w.l.o.g. λ is a limit ordinal.
 (1)3. PICK a strictly increasing sequence $(a_\alpha)_{\alpha < \text{cf } \lambda}$ that converges to λ .
 (1)4. LET: S be a set of ordinals $< \text{cf } \lambda$ such that $|S| = \text{cf } \text{cf } \lambda$ and $\sup S = \text{cf } \lambda$.
 (1)5. LET: $a(S) = \{a_\alpha \mid \alpha \in S\}$
 (1)6. $a(S)$ is cofinal in λ .
 (2)1. LET: $\beta < \lambda$
 (2)2. PICK $\gamma < \text{cf } \lambda$ such that $\beta < a_\gamma$
 (2)3. PICK $\delta \in S$ such that $\gamma < \delta$
 (2)4. $a_\delta \in a(S)$ and $\beta < a_\gamma < a_\delta$
 (1)7. $\text{cf } \lambda \leq \text{cf } \text{cf } \lambda$
 PROOF: Since $a(S)$ is a set of ordinals $< \lambda$ with $|a(S)| = \text{cf } \text{cf } \lambda$ and $\sup a(S) = \lambda$.
 (1)8. $\text{cf } \text{cf } \lambda = \text{cf } \lambda$
 □

Theorem 12.4.10. *Let λ be an infinite cardinal. Then $\text{cf } \lambda$ is the least cardinal such that λ can be partitioned into $\text{cf } \lambda$ sets, each of cardinality $< \lambda$.*

PROOF:

- (1)1. λ can be partitioned into $\text{cf } \lambda$ sets, each of cardinality $< \lambda$
 (2)1. PICK a strictly increasing sequence of ordinals $(a_\alpha)_{\alpha < \text{cf } \lambda}$ that converges to λ
 (2)2. $\{\{\beta \mid a_\alpha \leq \beta < a_{\alpha+1}\} \mid \alpha < \text{cf } \lambda\}$ is a partition of λ into $\text{cf } \lambda$ sets, each of cardinality $< \lambda$
 (1)2. If λ can be partitioned into κ sets, each of cardinality $< \lambda$, then $\text{cf } \lambda \leq \kappa$.
 (2)1. LET: \mathcal{A} be a partition of λ into sets of cardinality $< \lambda$
 (2)2. LET: $\kappa = |P|$
 (2)3. PICK a bijection $A : \kappa \approx P$
 (2)4. $\lambda = \bigcup_{\xi < \kappa} A(\xi)$
 (2)5. For all $\xi < \kappa$ we have $|A(\xi)| < \lambda$
 (2)6. LET: $\mu = \sup_{\xi < \kappa} |A(\xi)|$
 (2)7. $\mu \leq \lambda$
 (2)8. For all $\xi < \kappa$ we have $|A(\xi)| \leq \mu$
 (2)9. $\lambda \leq \mu\kappa$
 PROOF: Proposition 8.2.6.
 (2)10. ASSUME: w.l.o.g. $\kappa < \lambda$
 PROOF: If $\lambda \leq \kappa$ then $\text{cf } \lambda \leq \kappa$ since $\text{cf } \lambda \leq \lambda$.
 (2)11. $\lambda = \mu$
 PROOF:

$$\lambda \leq \mu\kappa \quad ((2)9)$$

$$\leq \lambda\lambda \quad ((2)7, (2)10)$$

$$= \lambda \quad (\text{Proposition 12.1.1})$$

- (2)12. $\{|A(\xi)| \mid \xi < \kappa\}$ is a set of $\leq \kappa$ ordinals all $< \lambda$ whose supremum is λ

- (2)13. $\text{cf } \lambda \leq \kappa$

□

Theorem 12.4.11 (König). *For any infinite cardinal κ we have $\kappa < \text{cf } 2^\kappa$.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: for a contradiction $\text{cf } 2^\kappa \leq \kappa$

$\langle 1 \rangle 2$. LET: $S = 2^\kappa$

$\langle 1 \rangle 3$. PICK a partition $\{A_\xi \mid \xi < \kappa\}$ of S^κ with $\forall \xi < \kappa. |A_\xi| < 2^\kappa$.

PROOF: Theorem 12.4.10.

$\langle 1 \rangle 4$. $\forall \xi < \kappa. \{g(\xi) \mid g \in A_\xi\} \subsetneq S$

PROOF: We do not have equality because $|\{g(\xi) \mid g \in A_\xi\}| \leq |A_\xi| < 2^\kappa$.

$\langle 1 \rangle 5$. For all $\xi < \kappa$, choose $s_\xi \in S - \{g(\xi) \mid g \in A_\xi\}$

$\langle 1 \rangle 6$. $s \in S^\kappa$

$\langle 1 \rangle 7$. For all $\xi < \kappa$ we have $s \notin A_\xi$

PROOF: Since for all $\xi < \kappa$ and $g \in A_\xi$ we have $s_\xi(\xi) \neq g(\xi)$.

$\langle 1 \rangle 8$. Q.E.D.

PROOF: This contradicts $\langle 1 \rangle 3$.

□

Corollary 12.4.11.1.

$$2^{\aleph_0} \neq \aleph_\omega$$

Proposition 12.4.12. *For any ordinal α , we have $\text{cf } \alpha$ is the least cardinal such that α is the strict supremum of $\text{cf } \alpha$ smaller ordinals.*

PROOF:

$\langle 1 \rangle 1$. CASE: $\alpha = 0$

PROOF: Since $0 = \text{ssup } \emptyset$.

$\langle 1 \rangle 2$. CASE: $\alpha = \beta^+$

PROOF: Since $\beta^+ = \text{ssup } \{\beta\}$.

$\langle 1 \rangle 3$. CASE: α is a limit ordinal.

$\langle 2 \rangle 1$. There exists a set S of ordinals $< \alpha$ such that $|S| = \text{cf } \alpha$ and $\alpha = \text{ssup } S$.

$\langle 3 \rangle 1$. PICK a set S of ordinals $< \alpha$ such that $|S| = \text{cf } \alpha$ and $\sup S = \alpha$

PROVE: $\alpha = \text{ssup } S$

$\langle 3 \rangle 2$. $\forall \beta \in S. \beta < \alpha$

$\langle 3 \rangle 3$. For any ordinal γ , if $\forall \beta \in S. \beta < \gamma$ then $\alpha \leq \gamma$

$\langle 2 \rangle 2$. If T is a set of ordinals $< \alpha$ such that $\alpha = \text{ssup } T$, then $\text{cf } \alpha \leq |T|$.

$\langle 3 \rangle 1$. LET: T be a set of ordinals $< \alpha$ such that $\alpha = \text{ssup } T$

$\langle 3 \rangle 2$. $\alpha = \sup T$

$\langle 4 \rangle 1$. For all $\beta \in T$ we have $\beta \leq \alpha$

$\langle 4 \rangle 2$. LET: μ be any upper bound for T

PROVE: $\alpha \leq \mu$

$\langle 4 \rangle 3$. $\alpha \leq \mu + 1$

PROOF: Since $\forall \beta \in T. \beta < \mu + 1$.

$\langle 4 \rangle 4$. $\alpha \neq \mu + 1$

PROOF: Since α is a limit ordinal.

$\langle 4 \rangle 5$. $\alpha < \mu + 1$

$\langle 4 \rangle 6$. $\alpha \leq \mu$

$\langle 3 \rangle 3$. $\text{cf } \alpha \leq |T|$

□

12.5 Inaccessible Cardinals

Definition 12.5.1 (Inaccessible Cardinal). A cardinal number κ is *inaccessible* iff:

- $\kappa > \aleph_0$
- $\forall \lambda < \kappa. 2^\lambda < \kappa$ (cardinal exponentiation)
- κ is regular.

Any inaccessible cardinal is weakly inaccessible.

PROOF:

$\langle 1 \rangle 1$. LET: $\kappa = \aleph_\lambda$ be weakly inaccessible.

PROVE: λ is a limit ordinal.

$\langle 1 \rangle 2$. $\lambda \neq 0$

$\langle 1 \rangle 3$. ASSUME: for a contradiction $\lambda = \beta + 1$

$\langle 1 \rangle 4$. $\aleph_\beta < \kappa$

$\langle 1 \rangle 5$. $2^{\aleph_\beta} < \kappa$

$\langle 1 \rangle 6$. $\aleph_{\beta+1} < \kappa$

PROOF: Since $\aleph_{\beta+1} \leq 2^{\aleph_\beta}$.

$\langle 1 \rangle 7$. Q.E.D.

PROOF: This contradicts $\langle 1 \rangle 3$.

□

Proposition 12.5.2. *If the Generalized Continuum Hypothesis is true, then every weakly inaccessible cardinal is inaccessible.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: The Generalized Continuum Hypothesis.

$\langle 1 \rangle 2$. LET: $\kappa = \aleph_\lambda$ be weakly inaccessible.

$\langle 1 \rangle 3$. $\kappa > \aleph_0$

PROOF: $\lambda > 0$ because λ is a limit ordinal.

$\langle 1 \rangle 4$. For all $\mu < \kappa$ we have $2^\mu < \kappa$

$\langle 2 \rangle 1$. LET: $\mu < \kappa$

$\langle 2 \rangle 2$. LET: $\mu = \aleph_\alpha$

$\langle 2 \rangle 3$. $\alpha < \lambda$

$\langle 2 \rangle 4$. $\alpha + 1 < \lambda$

PROOF: λ is a limit ordinal.

$\langle 2 \rangle 5$. $2^\mu < \kappa$

PROOF:

$$\begin{aligned}
 2^\mu &= 2^{\aleph_\alpha} && (\langle 2 \rangle 2) \\
 &= 2^{\beth_\alpha} && (\langle 1 \rangle 1) \\
 &= \beth_{\alpha+1} \\
 &= \aleph_{\alpha+1} && (\langle 1 \rangle 1) \\
 &< \aleph_\lambda && (\langle 2 \rangle 4) \\
 &= \kappa && (\langle 1 \rangle 2)
 \end{aligned}$$

$\langle 1 \rangle 5.$ κ is regular.

PROOF: $\langle 1 \rangle 2$

□

Lemma 12.5.3. *Let κ be an inaccessible cardinal. For every ordinal $\alpha < \kappa$ we have $\beth_\alpha < \kappa$.*

PROOF:

$\langle 1 \rangle 1.$ $\beth_0 < \kappa$

PROOF: Since $\kappa > \aleph_0$.

$\langle 1 \rangle 2.$ For any ordinal α , if $\beth_\alpha < \kappa$ then $\beth_{\alpha+1} < \kappa$.

PROOF: Since $\beth_{\alpha+1} = 2^{\beth_\alpha} < \kappa$.

$\langle 1 \rangle 3.$ For any limit ordinal λ , if $\forall \alpha < \lambda. \beth_\alpha < \kappa$ and $\lambda < \kappa$ then $\beth_\lambda < \kappa$.

PROOF: By regularity of κ , since \beth_λ is the union of $|\lambda|$ cardinals all $< \kappa$.

□

Lemma 12.5.4. *Let κ be an inaccessible cardinal. For all $A \in V_\kappa$ we have $|A| < \kappa$.*

PROOF:

$\langle 1 \rangle 1.$ LET: $A \in V_\kappa$

$\langle 1 \rangle 2.$ PICK $\alpha < \kappa$ such that $A \in V_\alpha$

$\langle 1 \rangle 3.$ $A \subseteq V_\alpha$

$\langle 1 \rangle 4.$ $|A| \leq |V_\alpha| \leq \beth_\alpha < \kappa$

□

Theorem Schema 12.5.5. *For every axiom α of ZFC, the following is a theorem:*

For any inaccessible cardinal κ , we have V_κ is a model of α .

PROOF: For every axiom except the Replacement Axioms, we have Corollary 11.0.11.1.

For an Axiom of Replacement using the property $P[x, y, z_1, \dots, z_n]$, we reason as follows:

$\langle 1 \rangle 1.$ LET: κ be an inaccessible cardinal

PROVE:

$$\begin{aligned} & \forall a_1, \dots, a_n, B \in V_\kappa (\forall x \in B. \forall y, y' \in V_\kappa \\ & (P[x, y, a_1, \dots, a_n]^{V_\kappa} \wedge P[x, y', a_1, \dots, a_n]^{V_\kappa} \Rightarrow y = y') \Rightarrow \\ & \exists C \in V_\kappa \forall y \in V_\kappa (y \in C \Leftrightarrow \exists x \in B. P[x, y, a_1, \dots, a_n]^{V_\kappa})) \end{aligned}$$

$\langle 1 \rangle 2.$ LET: $a_1, \dots, a_n, B \in V_\kappa$

$\langle 1 \rangle 3.$ ASSUME: for all $x \in B$, there exists at most one $y \in V_\kappa$ such that

$$P[x, y, a_1, \dots, a_n]^{V_\kappa}.$$

$\langle 1 \rangle 4.$ LET: $F = \{(x, y) \in B \times V_\kappa \mid P[x, y, a_1, \dots, a_n]^{V_\kappa}\}$

$\langle 1 \rangle 5.$ LET: $C = \text{ran } F$

PROVE: $C \in V_\kappa$

$\langle 1 \rangle 6.$ LET: $S = \{\text{rank } F(x) \mid x \in \text{dom } F\}$

$\langle 1 \rangle 7.$ $|S| < \kappa$

PROOF: Since $|S| \leq |\text{dom } F| \leq |B| < \kappa$.

$\langle 1 \rangle 8. \forall \alpha \in S. \alpha < \kappa$

PROOF: Since $F(x) \in V_\kappa$ for all $x \in \text{dom } F$.

$\langle 1 \rangle 9. \sup S < \kappa$

PROOF: Since κ is regular.

$\langle 1 \rangle 10. \text{rank } C \leq \sup S + 1$

$\langle 1 \rangle 11. \text{rank } C < \kappa$

$\langle 1 \rangle 12. C \in V_\kappa$

□

Chapter 13

Group Theory

13.1 Groups

Definition 13.1.1 (Group). A *group* G consists of a set G and a function $\cdot : G^2 \rightarrow G$ 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 13.1.2. *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 13.1.3. We write x^{-1} for the inverse of x .

Proposition 13.1.4. *In any group, if $ab = ac$ then $b = c$.*

PROOF:

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

□

Definition 13.1.5. Let \mathbf{Grp} be the category of groups and group homomorphisms.

Definition 13.1.6. We identify any group G with the category G with one object whose morphisms are the elements of G , with composition given by the multiplication in G .

13.2 Abelian Groups

Definition 13.2.1 (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 14

Ring Theory

14.1 Rings

Definition 14.1.1 (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 14.1.2. *In any commutative ring, $0x = 0$.*

PROOF:

$$\begin{aligned}(0 + 0)x &= 0x \\ \therefore 0x + 0x &= 0x + 0 \\ \therefore 0x &= 0 && \text{(Proposition 13.1.4)} \quad \square\end{aligned}$$

Proposition 14.1.3. *In any commutative ring, $(-a)b = -(ab)$.*

PROOF:

$$\begin{aligned}ab + (-a)b &= (a + (-a))b \\ &= 0b \\ &= 0 && \text{(Proposition 14.1.2)} \quad \square\end{aligned}$$

14.2 Ordered Rings

Definition 14.2.1 (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 14.2.2. *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. \square

Proposition 14.2.3. *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 $z = (x + y)/2$. \square

14.3 Integral Domains

Definition 14.3.1 (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 14.3.2. *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 $b = c$. \square

Definition 14.3.3 (Ordered Integral Domain). An *ordered integral domain* is an ordered commutative ring that is an integral domain.

Chapter 15

Field Theory

15.1 Fields

Definition 15.1.1 (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 15.1.2. *Every field is an integral domain.*

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

Proposition 15.1.3. *In any field F , we have $F - \{0\}$ is an Abelian group under multiplication.*

PROOF: Immediate from the definition. \square

Definition 15.1.4 (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

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(ad + bc, bd)] \\ [(a, b)][(c, d)] &= [(ac, bd)] \end{aligned}$$

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 $cb = da$.

$\langle 2 \rangle 3$. \sim is transitive.

$\langle 3 \rangle 1$. ASSUME: $(a, b) \sim (c, d) \sim (e, f)$

$\langle 3 \rangle 2$. $ad = bc$ and $cf = de$

$\langle 3 \rangle 3$. $adf = bde$

PROOF: $adf = bcf = bde$

$\langle 3 \rangle 4$. $af = be$

PROOF: Proposition 14.3.2.

□

$\langle 1 \rangle 2$. Addition is well-defined.

PROOF:

$\langle 2 \rangle 1$. If $b \neq 0$ and $d \neq 0$ then $bd \neq 0$.

PROOF: Since D is an integral domain.

$\langle 2 \rangle 2$. If $ab' = a'b$ and $cd' = c'd$ then $(ad + bc)b'd' = (a'd' + b'c')bd$.

PROOF:

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

□

$\langle 1 \rangle 3$. Multiplication is well-defined.

PROOF:

$\langle 2 \rangle 1$. If $b \neq 0$ and $d \neq 0$ then $bd \neq 0$.

PROOF: Since D is an integral domain.

$\langle 2 \rangle 2$. 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 $acb'd' = a'c'bd$.

□

$\langle 1 \rangle 4$. Addition is commutative.

PROOF: $[(a, b)] + [(c, d)] = [(ad + bc, bd)] = [(cb + da, db)] = [(c, d)] + [(a, b)]$ □

$\langle 1 \rangle 5$. Addition is associative.

PROOF:

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

$\langle 1 \rangle 6$. For any $x \in F$ we have $x + [(0, 1)] = x$

PROOF: $[(a, b)] + [(0, 1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a, b)]$ □

$\langle 1 \rangle 7$. For any $x \in F$, there exists $y \in F$ such that $x + y = [(0, 1)]$.

PROOF: $[(a, b)] + [(-a, b)] = [(ab - ab, b^2)] = [(0, b^2)] = [(0, 1)]$ □

$\langle 1 \rangle 8$. Multiplication is commutative.

PROOF: $[(a, b)][(c, d)] = [(c, d)][(a, b)] = [(ac, bd)]$. □

$\langle 1 \rangle 9$. Multiplication is associative.

PROOF: $[(a, b)]([[(c, d)][(e, f)]] = ([[(a, b)][(c, d)]][(e, f)] = [(ace, bdf)]$. □

$\langle 1 \rangle 10$. For any $x \in F$ we have $x[(1, 1)] = x$

PROOF: $[(a, b)][(1, 1)] = [(a, b)]$ □

$\langle 1 \rangle 11$. For any non-zero $x \in F$, there exists $y \in F$ such that $xy = [(1, 1)]$.

PROOF:

- $\langle 2 \rangle 1$. LET: $[(a, b)] \in \mathbb{Q}$
- $\langle 2 \rangle 2$. ASSUME: $[(a, b)] \neq [(0, 1)]$
- $\langle 2 \rangle 3$. $a \neq 0$
- $\langle 2 \rangle 4$. $[(a, b)][(b, a)] = [(1, 1)]$

□

□

Definition 15.1.5. 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 15.1.6 (Characteristic Zero). A field F has *characteristic 0* iff $0 \notin N(F)$.

Proposition 15.1.7. In a field F with characteristic 0, the function $n : \mathbb{N} \rightarrow N(F)$ defined by

$$\begin{aligned} n(0) &= 1 \\ n(x+1) &= n(x) + 1 \end{aligned}$$

is a bijection.

PROOF:

- $\langle 1 \rangle 1$. n is injective.
- $\langle 2 \rangle 1$. ASSUME: for a contradiction $n(i) = n(j)$ with $i \neq j$
- $\langle 2 \rangle 2$. ASSUME: w.l.o.g. $i < j$
- $\langle 2 \rangle 3$. $n(j - i) = 0$
- $\langle 2 \rangle 4$. Q.E.D.

PROOF: This contradicts the fact that F has characteristic 0.

- $\langle 1 \rangle 2$. n is surjective.

PROOF: Since $\text{ran } n$ is a subset of F that includes 1 and is closed under $+1$.

□

Definition 15.1.8. In any field F , let

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

Definition 15.1.9. In any field F , let

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

Proposition 15.1.10. $Q(F)$ 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 15.1.11. Let F and G be fields of characteristic 0. Then there exists a unique field isomorphism between $Q(F)$ and $Q(G)$.

PROOF:

- (1)1. LET: $\phi : N(F) \rightarrow N(G)$ be the unique function such that $\phi(1) = 1$ and $\forall x \in N(F). \phi(x+1) = \phi(x) + 1$.
- (1)2. ϕ is a bijection.
 PROOF: Similar to Proposition 15.1.7.
- (1)3. $\forall x, y \in N(F). \phi(x+y) = \phi(x) + \phi(y)$
 PROOF: Induction on y .
- (1)4. $\forall x, y \in N(F). \phi(xy) = \phi(x)\phi(y)$
 PROOF: Induction on y .
- (1)5. Extend 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 $\forall x, y \in I(F). \phi(xy) = \phi(x)\phi(y)$
- (2)1. Define $\phi(0) = 0$ and $\phi(-x) = -\phi(x)$ for $x \in N(F)$
- (3)1. $0 \notin N(F)$
- (3)2. For all $x \in N(F)$ we have $-x \notin N(F)$
 PROOF: Then we would have $x + -x = 0 \in N(F)$.
- (3)3. For all $x \in N(F)$ we have $-x \neq 0$
- (2)2. For all $x, y \in I(F)$ we have $\phi(x+y) = \phi(x) + \phi(y)$
 PROOF: Case analysis on x and y .
- (2)3. For all $x, y \in I(F)$ we have $\phi(xy) = \phi(x)\phi(y)$
 PROOF: Case analysis on x and y .
- (1)6. Extend 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 $\forall x, y \in Q(F). \phi(xy) = \phi(x)\phi(y)$
- (2)1. Define $\phi(x/y) = \phi(x)/\phi(y)$
- (1)7. ϕ is unique.
- (2)1. LET: θ satisfy the theorem.
- (2)2. For all $x \in N(F)$ we have $\theta(x) = \phi(x)$
- (2)3. For all $x \in I(F)$ we have $\theta(x) = \phi(x)$
- (2)4. For all $x \in Q(F)$ we have $\theta(x) = \phi(x)$

□

15.2 Ordered Fields

Definition 15.2.1 (Ordered Field). An *ordered field* is an ordered commutative ring that is a field.

Proposition 15.2.2. Every ordered field F has characteristic 0.

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

Proposition 15.2.3. 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 15.2.3.1. 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 15.2.4 (Archimedean). An ordered field F is *Archimedean* iff

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

Proposition 15.2.5. *Let F be an Archimedean ordered field. Let $x, y \in F$ with $x > 0$. Then there exists $n \in N(F)$ such that $nx > y$.*

PROOF: Pick $n > y/x$. \square

Proposition 15.2.6. *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:

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

$\langle 2 \rangle 1$. PICK $n \in N(F)$ such that $n(y - x) > 1$

PROOF: Proposition 15.2.5.

$\langle 2 \rangle 2$. $ny > 1 + nx$

$\langle 2 \rangle 3$. LET: m be the least element of $N(F)$ such that $m > nx$.

$\langle 2 \rangle 4$. $m - 1 \leq nx$

$\langle 2 \rangle 5$. $nx < m < ny$

$\langle 2 \rangle 6$. $x < m/n < y$

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

$\langle 2 \rangle 1$. PICK $k \in N(F)$ such that $k > -x$

$\langle 2 \rangle 2$. $0 < x + k < y + k$

$\langle 2 \rangle 3$. PICK $r \in Q(F)$ such that $x + k < r < y + k$

PROOF: $\langle 1 \rangle 1$

$\langle 2 \rangle 4$. $x < r - k < y$

Definition 15.2.7 (Complete). An ordered field F is *complete* iff every nonempty subset of F bounded above has a least upper bound.

Proposition 15.2.8. *Every complete ordered field is Archimedean.*

PROOF:

$\langle 1 \rangle 1$. LET: F be a complete ordered field.

$\langle 1 \rangle 2$. LET: $x \in F$

$\langle 1 \rangle 3$. ASSUME: for a contradiction there is no member of $N(F)$ greater than x .

$\langle 1 \rangle 4$. x is an upper bound for $N(F)$.

$\langle 1 \rangle 5$. LET: $y = \sup N(F)$

$\langle 1 \rangle 6$. PICK $n \in N(F)$ such that $y - 1 < n$

$\langle 1 \rangle 7$. $y < n + 1$

$\langle 1 \rangle 8$. Q.E.D.

PROOF: This is a contradiction.

\square

Proposition 15.2.9. *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:

$\langle 1 \rangle 1$. LET: $B = \{x \in F \mid 0 \leq x \leq 1 + a\}$

$\langle 1 \rangle 2$. LET: $\phi : B \rightarrow B$ 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 15.2.10 (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 $x, y \in F$,*

$$\begin{aligned}\phi(x + y) &= \phi(x) + \phi(y) \\ \phi(xy) &= \phi(x)\phi(y)\end{aligned}$$

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 15.2.3.1.

- ⟨1⟩2. $Q(F)$ intersects every interval in F .

PROOF: Proposition 15.2.6.

- ⟨1⟩3. $Q(G)$ intersects every interval in G .

PROOF: Proposition 15.2.6.

- ⟨1⟩4. PICK an order isomorphism $\psi : F \cong G$ that extends ϕ .

PROOF: Theorem 6.1.21.

- ⟨1⟩5. $\forall x, y \in F. \psi(x + y) = \psi(x) + \psi(y)$
 ⟨2⟩1. LET: $x, y \in F$
 ⟨2⟩2. $\psi(x) + \psi(y) \not\leq \psi(x + y)$
 ⟨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. $x < r$

- $\langle 3 \rangle 11. y < s$
- $\langle 3 \rangle 12. x + y > r + s$
- $\langle 3 \rangle 13. \text{Q.E.D.}$

PROOF: This is a contradiction.

- $\langle 2 \rangle 3. \psi(x + y) \not\leq \psi(x) + \psi(y)$

PROOF: Similar.

- $\langle 1 \rangle 6. \forall x, y \in F. \psi(xy) = \psi(x)\psi(y)$

- $\langle 2 \rangle 1. \text{LET: } x, y \in F$

- $\langle 2 \rangle 2. \text{CASE: } x \text{ and } y \text{ are positive.}$

- $\langle 3 \rangle 1. \psi(x)\psi(y) \not\leq \psi(xy)$

- $\langle 4 \rangle 1. \text{ASSUME: for a contradiction } \psi(x)\psi(y) < \psi(xy)$

- $\langle 4 \rangle 2. \text{PICK } r' \in Q(G) \text{ such that } \psi(x) < r' < \psi(xy)/\psi(y)$

- $\langle 4 \rangle 3. \text{PICK } s' \in Q(G) \text{ such that } \psi(y) < s' < \psi(xy)/r'$

- $\langle 4 \rangle 4. r's' < \psi(xy)$

- $\langle 4 \rangle 5. \text{PICK } r, s \in Q(F) \text{ such that } \phi(r) = r' \text{ and } \phi(s) = s'$

- $\langle 4 \rangle 6. \phi(rs) = r's'$

- $\langle 4 \rangle 7. x < r, y < s \text{ and } rs < xy$

- $\langle 4 \rangle 8. \text{Q.E.D.}$

PROOF: This is a contradiction.

- $\langle 3 \rangle 2. \psi(xy) \not\leq \psi(x)\psi(y)$

PROOF: Similar.

- $\langle 2 \rangle 3. \text{CASE: } x \text{ and } y \text{ are not both positive.}$

PROOF: Follows from $\langle 2 \rangle 2$ since $\psi(-x) = -\psi(x)$ by $\langle 1 \rangle 5$.

- $\langle 1 \rangle 7. \text{For any field isomorphism } \theta : F \cong G, \text{ we have } \theta = \psi.$

- $\langle 2 \rangle 1. \theta \upharpoonright Q(F) = \phi$

PROOF: Theorem 15.1.11.

- $\langle 2 \rangle 2. \theta \text{ is strictly monotone.}$

- $\langle 3 \rangle 1. \text{LET: } x, y \in F \text{ with } x < y$

- $\langle 3 \rangle 2. y - x > 0$

- $\langle 3 \rangle 3. \text{PICK } z \in F \text{ such that } z^2 = y - x$

- $\langle 3 \rangle 4. \theta(z)^2 = \theta(y) - \theta(x)$

- $\langle 3 \rangle 5. \theta(y) - \theta(x) > 0$

- $\langle 3 \rangle 6. \theta(x) < \theta(y)$

- $\langle 2 \rangle 3. \theta = \psi$

PROOF: By the uniqueness of ψ .

□

Chapter 16

Number Systems

16.1 The Integers

Definition 16.1.1. The set of *integers* \mathbb{Z} is the quotient set \mathbb{N}^2 / \sim , where $(m, n) \sim (p, q)$ iff $m + q = n + p$.

We prove \sim is an equivalence relation on \mathbb{N}^2 .

PROOF:

$\langle 1 \rangle 1.$ \sim is reflexive.

PROOF: For all $m, n \in \mathbb{N}$ we have $m + n = n + m$.

$\langle 1 \rangle 2.$ \sim is symmetric.

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

$\langle 1 \rangle 3.$ \sim is transitive.

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

$\langle 2 \rangle 2.$ $m + q = n + p$ and $p + s = q + r$

$\langle 2 \rangle 3.$ $m + q + s = n + q + r$

$\langle 2 \rangle 4.$ $m + s = n + r$

PROOF: By cancellation.

□

Definition 16.1.2 (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 16.1.3. *Addition on \mathbb{Z} is commutative.*

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

□

Proposition 16.1.4. *Addition on \mathbb{Z} is associative.*

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

Proposition 16.1.5. *Given natural numbers m and n , we have $[(m, 0)] = [(n, 0)]$ iff $m = n$.*

PROOF: Immediate from definitions. \square

Definition 16.1.6. We identify any natural number n with the integer $[(n, 0)]$.

Proposition 16.1.7. *Addition on integers agrees with addition on natural numbers.*

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

Proposition 16.1.8. *For all $a \in \mathbb{Z}$ we have $a + 0 = a$.*

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

Proposition 16.1.9. *For all $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0$.*

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

Proposition 16.1.10. *The integers form an Abelian group under addition.*

PROOF: Proposition 16.1.3, 16.1.4, 16.1.8, 16.1.9. \square

Definition 16.1.11. Define multiplication \cdot on \mathbb{Z} by: $[(m, n)][(p, q)] = [(mp + nq, mq + np)]$.

We prove this is well defined.

PROOF:

$\langle 1 \rangle 1$. ASSUME: $m + n' = n + m'$ and $p + q' = q + p'$

PROVE: $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$

$\langle 1 \rangle 2$. $mp + n'p = np + m'p$

$\langle 1 \rangle 3$. $nq + m'q = mq + n'q$

$\langle 1 \rangle 4$. $m'p + m'q' = m'q + m'p'$

$\langle 1 \rangle 5$. $n'q + n'p' = n'p + n'q'$

$\langle 1 \rangle 6$. $mp + n'p + nq + m'q + m'p + m'q' + n'q + n'p' = np + m'p + mq + n'q + m'q + m'p' + n'p + n'q'$

$\langle 1 \rangle 7$. $mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$

PROOF: By cancellation.

\square

Proposition 16.1.12. *Multiplication on integers agrees with multiplication on natural numbers.*

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

Proposition 16.1.13. *Multiplication on \mathbb{Z} is commutative.*

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

Proposition 16.1.14. *Multiplication on \mathbb{Z} is associative.*

PROOF:

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

Proposition 16.1.15. *Multiplication distributes over addition.*

PROOF:

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

Proposition 16.1.16. *For any integer a we have $a1 = a$.*

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

Proposition 16.1.17. *For any integers a and b , if $ab = 0$ then $a = 0$ or $b = 0$.*

PROOF:

$\langle 1 \rangle 1$. ASSUME: $[(m, n)][(p, q)] = [(0, 0)]$

$\langle 1 \rangle 2$. $mp + nq = mq + np$

$\langle 1 \rangle 3$. ASSUME: $[(m, n)] \neq [(0, 0)]$

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

PROVE: $p = q$

$\langle 1 \rangle 5$. CASE: $m < n$

$\langle 2 \rangle 1$. $p \not\leq q$

PROOF: If $p < q$ then $mq + np < mp + nq$ by Proposition 9.4.6.

$\langle 2 \rangle 2$. $q \not\leq p$

PROOF: If $q < p$ then $mp + nq < mq + np$ by Proposition 9.4.6.

$\langle 2 \rangle 3$. $p = q$

PROOF: By trichotomy.

$\langle 1 \rangle 6$. CASE: $n < m$

PROOF: Similar.

\square

Proposition 16.1.18. *The integers \mathbb{Z} form an integral domain.*

PROOF: Propositions 16.1.13, 16.1.14, 16.1.15, 16.1.16, 16.1.17, 16.1.10. \square

Definition 16.1.19. Define $<$ on \mathbb{Z} by $[(m, n)] < [(p, q)]$ if and only if $m + q < n + p$.

We prove this is well-defined.

PROOF:

$\langle 1 \rangle 1$. ASSUME: $m + n' = n + m'$ and $p + q' = q + p'$.

PROVE: $m + q < n + p$ if and only if $m' + q' < n' + p'$

$\langle 1 \rangle 2$. $m + q < n + p$ if and only if $m' + q' < n' + p'$

PROOF:

$$m + q < n + p \Leftrightarrow m + n' + q < n + n' + p \quad (\text{Corollary 7.6.7.1})$$

$$\Leftrightarrow m' + n + q < n + n' + p$$

$$\Leftrightarrow m' + q < n' + p \quad (\text{Corollary 7.6.7.1})$$

$$\Leftrightarrow m' + q + p' < n' + p + p' \quad (\text{Corollary 7.6.7.1})$$

$$\Leftrightarrow m' + q' + p < n' + p + p'$$

$$\Leftrightarrow m' + q' < n' + p' \quad (\text{Corollary 7.6.7.1}) \square$$

Proposition 16.1.20. *The ordering on the integers agrees with the ordering on the natural numbers.*

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

Proposition 16.1.21. *$<$ is a linear order on \mathbb{Z} .*

PROOF:

$\langle 1 \rangle 1$. $<$ is irreflexive.

PROOF: We never have $m + n < m + n$.

$\langle 1 \rangle 2$. $<$ is transitive.

$\langle 2 \rangle 1$. ASSUME: $[(m, n)] < [(p, q)] < [(r, s)]$

$\langle 2 \rangle 2$. $m + q < n + p$ and $p + s < q + r$

$\langle 2 \rangle 3$. $m + q + s < n + q + r$

PROOF: $m + q + s < n + p + s < n + q + r$

$\langle 2 \rangle 4$. $m + s < n + r$

PROOF: Corollary 7.6.7.1.

$\langle 1 \rangle 3$. $<$ is total.

PROOF: Given natural numbers m, n, p and q , either $m + q < n + p$, or $m + q = n + p$, or $n + p < m + q$.

\square

Definition 16.1.22 (Positive). An integer a is *positive* iff $a > 0$.

Theorem 16.1.23. *For any integers a, b and c , we have $a < b$ if and only if $a + c < b + c$.*

PROOF:

$\langle 1 \rangle 1$. If $a < b$ then $a + c < b + c$.

$\langle 2 \rangle 1$. LET: $a = [(m, n)]$, $b = [(p, q)]$ and $c = [(r, s)]$.

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

$\langle 2 \rangle 3$. $m + q < n + p$

$\langle 2 \rangle 4$. $m + r + q + s < n + r + p + s$

$\langle 2 \rangle 5$. $[(m + r, n + s)] < [(p + r, q + s)]$

$\langle 2 \rangle 6$. $a + c < b + c$

$\langle 1 \rangle 2$. If $a + c < b + c$ then $a < b$.

PROOF: From $\langle 1 \rangle 1$ and Proposition 6.2.6.

□

Proposition 16.1.24. *Let a , b and c be integers. If $0 < c$, then $a < b$ if and only if $ac < bc$.*

PROOF:

$\langle 1 \rangle 1$. LET: $c = [(r, s)]$

$\langle 1 \rangle 2$. ASSUME: $0 < c$

$\langle 1 \rangle 3$. $s < r$

$\langle 1 \rangle 4$. For all integers a and b , if $a < b$ then $ac < bc$

$\langle 2 \rangle 1$. LET: $a = [(m, n)]$, $b = [(p, q)]$.

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

$\langle 2 \rangle 3$. $m + q < n + p$

$\langle 2 \rangle 4$. $(m + q)r + (p + n)s < (m + q)s + (p + n)r$

PROOF: Proposition 9.4.6, $\langle 1 \rangle 3$, $\langle 2 \rangle 3$.

$\langle 2 \rangle 5$. $mr + ns + ps + qr < ms + nr + pr + qs$

$\langle 2 \rangle 6$. $[(mr + ns, ms + nr)] < [(pr + qs, ps + qr)]$

$\langle 2 \rangle 7$. $ac < bc$

$\langle 1 \rangle 5$. For all integers a and b , if $ac < bc$ then $a < b$

PROOF: From $\langle 1 \rangle 4$ and Proposition 6.2.6.

□

Proposition 16.1.25. *Let a be a positive integer. For any integer b , there exists $k \in \mathbb{N}$ such that $b < ak$.*

PROOF:

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

PROOF: Take $k = 1$.

$\langle 1 \rangle 2$. CASE: $b > 0$

PROOF: Take $k = b + 1$.

□

16.2 The Rationals

Definition 16.2.1 (Rational Numbers). The set \mathbb{Q} of *rational numbers* is the field of fractions over the integers.

Proposition 16.2.2. *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 16.2.3. *Addition on the rationals agrees with addition on the integers.*

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

Proposition 16.2.4. *Multiplication on the rationals agrees with multiplication on the integers.*

PROOF: $[(a, 1)][(b, 1)] = [(ab, 1)]$ \square

Definition 16.2.5. Define the ordering $<$ on the rationals by: if b and d are positive, then $[(a, b)] < [(c, d)]$ iff $ad < bc$.

We prove this is well-defined.

PROOF:

$\langle 1 \rangle 1$. For any rational q , there exist integers a, b with b positive such that $q = [(a, b)]$.

PROOF: Since $[(a, b)] = [(-a, -b)]$, and if $b \neq 0$ then one of b and $-b$ is positive.

$\langle 1 \rangle 2$. If b, b', d and d' are positive, $[(a, b)] = [(a', b')]$, and $[(c, d)] = [(c', d')]$, then $ad < bc$ iff $a'd' < b'c'$.

PROOF:

$\langle 2 \rangle 1$. If $ad < bc$ then $a'd' < b'c'$.

$\langle 3 \rangle 1$. ASSUME: $ad < bc$

$\langle 3 \rangle 2$. $ab'd < bb'c$

$\langle 3 \rangle 3$. $a'bd < bb'c$

$\langle 3 \rangle 4$. $a'd < b'c$

$\langle 3 \rangle 5$. $a'dd' < b'cd'$

$\langle 3 \rangle 6$. $a'dd' < b'c'd$

$\langle 3 \rangle 7$. $a'd' < b'c'$

$\langle 2 \rangle 2$. If $a'd' < b'c'$ then $ad < bc$.

PROOF: Similar.

\square

Proposition 16.2.6. *The ordering on the rationals agrees with the ordering on the integers.*

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

Proposition 16.2.7. *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 16.2.8. *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:

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

□

Corollary 16.2.8.1. *For any rational r , we have $r < 0$ if and only if $0 < -r$.*

Definition 16.2.9 (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 16.2.10. *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 16.2.10.1. *The rationals form an ordered field.*

Proposition 16.2.11. *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 16.1.25.

$\langle 1 \rangle 3$. $r < pk$

□

Proposition 16.2.12. $\mathbb{Q} \approx \mathbb{N}$

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. □

16.3 The Real Numbers

Definition 16.3.1 (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 16.3.2 (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 16.3.3. 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 16.3.4. 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 16.3.5. Define the ordering $<$ on \mathbb{R} by: $x < y$ iff $x \subsetneq y$.

Proposition 16.3.6. *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 16.3.4.

$\langle 1 \rangle 5$. 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 16.3.7. *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: $x \not\subseteq y$

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: $r \in x$

$\langle 2 \rangle 5$. $q \not\leq r$

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 16.3.8. *Any bounded nonempty subset of \mathbb{R} has a least upper bound.*

PROOF:

⟨1⟩1. LET: A be a bounded nonempty subset of \mathbb{R} .

⟨1⟩2. $\bigcup A$ is a Dedekind cut.

⟨2⟩1. $\bigcup A \neq \emptyset$

⟨3⟩1. PICK $x \in A$

⟨3⟩2. PICK $q \in x$

⟨3⟩3. $q \in \bigcup A$

⟨2⟩2. $\bigcup A \neq \mathbb{Q}$

⟨3⟩1. PICK an upper bound u for A

⟨3⟩2. PICK $q \notin u$

PROVE: $q \notin \bigcup A$

⟨3⟩3. ASSUME: for a contradiction $q \in \bigcup A$

⟨3⟩4. PICK $x \in A$ such that $q \in x$

⟨3⟩5. $x \leq u$

⟨3⟩6. $q \in u$

⟨3⟩7. Q.E.D.

PROOF: This is a contradiction.

⟨2⟩3. $\bigcup A$ is closed downwards.

⟨3⟩1. LET: $q \in \bigcup A$ and $r < q$

⟨3⟩2. PICK $x \in A$ such that $q \in x$

⟨3⟩3. $r \in x$

⟨3⟩4. $r \in \bigcup A$

⟨2⟩4. $\bigcup A$ has no greatest element.

⟨3⟩1. LET: $q \in \bigcup A$

⟨3⟩2. PICK $x \in A$ such that $q \in x$

⟨3⟩3. PICK $r \in x$ such that $q < r$

⟨3⟩4. $r \in \bigcup A$

⟨1⟩3. $\bigcup A$ is an upper bound for A .

PROOF: For all $x \in A$ we have $x \subseteq \bigcup A$.

⟨1⟩4. For any upper bound u for $\bigcup A$ we have $\bigcup A \leq u$.

PROOF: If $\forall x \in A. x \subseteq u$ we have $\bigcup A \subseteq u$.

□

Definition 16.3.9 (Addition). Define *addition* $+$ on the reals by

$$x + y := \{q + r \mid q \in x, r \in y\} .$$

We prove this is well-defined.

PROOF:

⟨1⟩1. LET: $x, y \in \mathbb{R}$

PROVE: $X + y$ is a Dedekind cut.

$\langle 1 \rangle 2. x + y \neq \emptyset$

PROOF: Pick $q \in x$ and $r \in y$; then $q + r \in x + y$.

$\langle 1 \rangle 3. x + y \neq \mathbb{Q}$

$\langle 2 \rangle 1. \text{ PICK } q \notin x \text{ and } r \notin y$

PROVE: $q + r \notin x + y$

$\langle 2 \rangle 2. \text{ ASSUME: for a contradiction } q + r \in x + y$

$\langle 2 \rangle 3. \text{ PICK } q' \in x \text{ and } r' \in y \text{ such that } q + r = q' + r'$

$\langle 2 \rangle 4. q' < q \text{ and } r' < r$

$\langle 2 \rangle 5. q' + r' < q + r$

$\langle 2 \rangle 6. \text{ Q.E.D.}$

PROOF: This is a contradiction.

$\langle 1 \rangle 4. x + y$ is closed downwards.

$\langle 2 \rangle 1. \text{ LET: } q \in x \text{ and } r \in y$

$\langle 2 \rangle 2. \text{ LET: } s < q + r$

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.

$\langle 2 \rangle 1. \text{ LET: } q \in x \text{ and } r \in y$

PROVE: There exists $s \in x + y$ such that $q + r < s$

$\langle 2 \rangle 2. \text{ PICK } q' \in x \text{ and } r' \in y \text{ such that } q < q' \text{ and } r < r'$

$\langle 2 \rangle 3. q + r < q' + r' \in x + y$

□

Proposition 16.3.10. *Addition on the reals agrees with addition on the rationals.*

PROOF:

$\langle 1 \rangle 1. \text{ LET: } q, r \in \mathbb{Q}$

$\langle 1 \rangle 2. q \downarrow + r \downarrow \subseteq (q + r) \downarrow$

PROOF: If $s_1 < q$ and $s_2 < r$ then $s_1 + s_2 < q + r$.

$\langle 1 \rangle 3. (q + r) \downarrow \subseteq q \downarrow + r \downarrow$

$\langle 2 \rangle 1. \text{ LET: } s < q + r$

$\langle 2 \rangle 2. s - r < q$

$\langle 2 \rangle 3. \text{ PICK } t \text{ such that } s - r < t < q$

$\langle 2 \rangle 4. s - t < r$

$\langle 2 \rangle 5. s = t + (s - t) \in q \downarrow + r \downarrow$

□

Proposition 16.3.11. *Addition is associative.*

PROOF:

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

□

Proposition 16.3.12. *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 16.3.13. *For any $x \in \mathbb{R}$ we have $x + 0 = x$.*

PROOF:

⟨1⟩1. $x + 0 \subseteq x$

PROOF: If $q \in x$ and $r < 0$ then $q + r < q$ so $q + r \in x$.

⟨1⟩2. $x \subseteq x + 0$

⟨2⟩1. LET: $q \in x$

⟨2⟩2. PICK $r \in x$ such that $q < r$.

PROOF: x has no greatest element.

⟨2⟩3. $q - r < 0$

⟨2⟩4. $q = r + (q - r) \in x + 0$

□

Definition 16.3.14. For $x \in \mathbb{R}$, define $-x := \{q \in \mathbb{Q} \mid \exists r > q. -r \notin x\}$.

Proposition 16.3.15. *For all $x \in \mathbb{R}$ we have $-x \in \mathbb{R}$.*

PROOF:

⟨1⟩1. LET: $x \in \mathbb{R}$

⟨1⟩2. $-x \neq \emptyset$

⟨2⟩1. PICK $s \notin x$

⟨2⟩2. $-s - 1 \in -x$

⟨1⟩3. $-x \neq \mathbb{Q}$

⟨2⟩1. PICK $s \in x$

PROVE: $-s \notin -x$

⟨2⟩2. ASSUME: for a contradiction $-s \in -x$

⟨2⟩3. PICK $r > -s$ such that $-r \notin x$

⟨2⟩4. $-r < s$

⟨2⟩5. Q.E.D.

PROOF: This contradicts the fact that x is closed downwards.

⟨1⟩4. $-x$ is closed downwards.

PROOF: Immediate from definition.

⟨1⟩5. $-x$ has no greatest element.

⟨2⟩1. LET: $q \in -x$

⟨2⟩2. PICK $r > q$ such that $-r \notin x$

⟨2⟩3. PICK s such that $q < s < r$

⟨2⟩4. $s \in -x$

□

Lemma 16.3.16. *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 16.2.11.
 - $\langle 2 \rangle 3$. $q_1 < q_0 + kp$
 - $\langle 2 \rangle 4$. $q_0 + kp \notin x$
- $\langle 1 \rangle 3$. 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 16.3.17. *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 16.3.16.
 - $\langle 2 \rangle 4$. 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 16.3.17.1. *The reals form an Abelian group under addition.*

Proposition 16.3.18. *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 $q + r \in y + z$

⟨1⟩2. $\forall x, y, z \in \mathbb{R}. x + z = y + z \Leftrightarrow x = y$

PROOF: Proposition 13.1.4.

⟨1⟩3. $\forall x, y, z \in \mathbb{R}. x < y \Rightarrow x + z < y + z$

⟨1⟩4. Q.E.D.

PROOF: Proposition 6.2.6.

□

Definition 16.3.19 (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 16.3.20 (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:

⟨1⟩1. LET: x and y be non-negative reals.

PROVE: xy is real.

⟨1⟩2. $xy \neq \emptyset$

PROOF: Since $-1 \in xy$.

⟨1⟩3. $xy \neq \mathbb{Q}$

⟨2⟩1. PICK $r \notin x$ and $s \notin y$

PROVE: $rs \notin xy$

⟨2⟩2. $0 \leq r$ and $0 \leq s$

PROOF: Since $0 \subseteq x$ and $0 \subseteq y$.

⟨2⟩3. ASSUME: for a contradiction $rs \in xy$

⟨2⟩4. PICK r' and s' such that $0 \leq r' \in x$, $0 \leq s' \in y$ and $rs = r's'$

⟨2⟩5. $r' < r$

⟨2⟩6. $s' < s$

⟨2⟩7. $r's' < rs$

⟨2⟩8. Q.E.D.

PROOF: This is a contradiction.

⟨1⟩4. xy is closed downwards.

⟨2⟩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 16.3.21. *Multiplication is commutative.*

PROOF: Immediate from definition. □

Proposition 16.3.22. *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 16.3.23. *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:

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

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

PROOF:

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

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

(2)1. ASSUME: w.l.o.g. y is negative and z is non-negative.

(2)2. CASE: $0 \leq y + z$

PROOF:

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

(2)3. CASE: $y + z < 0$

PROOF:

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

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

PROOF:

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

□

Proposition 16.3.24. *For any real x we have $x1 = x$.*

PROOF:

(1)1. CASE: $0 \leq x$

(2)1. $x1 \subseteq x$

(3)1. LET: $q \in x1$

- ⟨3⟩2. CASE: $q < 0$
 PROOF: Then $q \in x$ because $0 \leq x$.
 ⟨3⟩3. $q = rs$ where $0 \leq r \in x$ and $0 \leq s < 1$
 PROOF: Then $q < r$ so $q \in x$.
 ⟨2⟩2. $x \subseteq x1$
 ⟨3⟩1. LET: $q \in x$
 ⟨3⟩2. ASSUME: w.l.o.g. $0 \leq q$
 ⟨3⟩3. PICK r such that $q < r \in x$
 ⟨3⟩4. $0 \leq q/r < 1$
 ⟨3⟩5. $q = r(q/r) \in x1$
 ⟨1⟩2. CASE: $x < 0$
 PROOF:

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

□

Lemma 16.3.25. *Let $x \in \mathbb{R}$ and c be a positive rational. Then there exists $a \in x$ and a non-least rational upper bound b for x such that $b - a = c$.*

PROOF:

- ⟨1⟩1. PICK $a_1 \in x$ such that if x has a rational supremum s then $a_1 > s - c$
 ⟨1⟩2. There exists a natural number n such that $a_1 + nc$ is an upper bound for x .
 ⟨2⟩1. PICK a non-least upper bound b_1 for x .
 ⟨2⟩2. PICK a natural number n such that $nc > b_1 - a_1$
 PROOF: Proposition 16.2.11.
 ⟨2⟩3. $a_1 + nc > b_1$
 ⟨2⟩4. $a_1 + nc$ is an upper bound for x .
 ⟨1⟩3. LET: k be the least natural number such that $a_1 + kc$ is an upper bound for x .
 ⟨1⟩4. $a_1 + (k - 1)c \in x$
 ⟨1⟩5. $a_1 + kc$ is not the supremum of x .
 ⟨2⟩1. ASSUME: for a contradiction $a_1 + kc$ is the supremum of x .
 ⟨2⟩2. $a_1 > a_1 + (k - 1)c$
 PROOF: ⟨1⟩1
 ⟨2⟩3. Q.E.D.
 PROOF: This is a contradiction.
 ⟨1⟩6. LET: $a = a_1 + (k - 1)c$
 ⟨1⟩7. LET: $b = a_1 + kc$
 ⟨1⟩8. $b - a = c$

□

Proposition 16.3.26. *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 16.3.25.
 - ⟨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

1

PROOF:

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

1

Proposition 16.3.28.

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

$$|\mathbb{R}| = 2^{\aleph_0}$$

PROOF:

PROOF: The function H where $H(x)(n)$ is the n th binary digit of the binary expansion of x is an injection.

PROOF: Map f to the real number in $[0, 1/9]$ whose $n + 1$ st decimal digit is $f(n)$.

1

Proposition 16.3.30. *The set of algebraic numbers is countable.*

PROOF: There are countably many integer polynomials, each with finitely many roots. \square

Corollary 16.3.30.1. *There are uncountably many transcendental numbers.*

Proposition 16.3.31. *Let A be a set of disks in the plane, no two of which intersect. Then A is countable.*

PROOF: Every circle includes a point with rational coordinates. Define $f : \{q \in \mathbb{Q}^2 \mid \exists C \in A. q \in C\} \rightarrow A$ by $f(q) = C$ iff $q \in C$. Then f is surjective. \square

Proposition 16.3.32. *There exists an uncountable set of circles in the plane that do not intersect.*

PROOF: The set of all circles with origin O is uncountable. \square

Chapter 17

Real Analysis

Theorem 17.0.1 (Weierstrass). *Let $a, b \in \mathbb{R}$ with $a < b$. Let $f : [a, b] \rightarrow \mathbb{R}$ be continuous. For every $\epsilon > 0$, there exists a polynomial p such that $\forall x \in [a, b]. |f(x) - p(x)| < \epsilon$.*

Theorem 17.0.2 (Bolzano-Weierstrass). *Every bounded sequence in \mathbb{R}^n has a convergent subsequence.*

17.1 Step Functions

Definition 17.1.1 (Step Function). A *step function* on \mathbb{R} is a function $f : \mathbb{R} \rightarrow \mathbb{R}$, where $[a_1, b_1), \dots, [a_n, b_n)$ are disjoint half-open intervals, such that f is constant on each $[a_i, b_i)$, and zero outside them.

Definition 17.1.2 (Basic Representation). Let f be a step function. The *basic representation* of f is defined as follows.

Let a_0, a_1, \dots, a_n be the points of discontinuity of f . For $k = 1, \dots, n$, let $\alpha_k = f(a_{k-1})$ and g_k be the characteristic function of $[a_{k-1}, a_k)$. Then the basic representation of f is

$$f = \alpha_1 g_1 + \dots + \alpha_n g_n .$$

Proposition 17.1.3. *If f and g are step functions then $\lambda x.f(x) + g(x)$ is a step function.*

Proposition 17.1.4. *If $c \in \mathbb{R}$ and f is a step function then $\lambda x.cf(x)$ is a step function.*

Proposition 17.1.5. *If f is a step function then $\lambda x.|f(x)|$ is a step function.*

Proposition 17.1.6. *If f and g are step functions then $\lambda x.\min(f(x), g(x))$ and $\lambda x.\max(f(x), g(x))$ are step functions.*

Proposition 17.1.7. *If f is a step function and $c \in \mathbb{R}$ then $\lambda x.f(x - c)$ is a step function.*

Definition 17.1.8 (Support). Given $f : \mathbb{R} \rightarrow \mathbb{R}$, the *support* of f is

$$\text{supp } f := \{x \in \mathbb{R} \mid f(x) \neq 0\} .$$

Definition 17.1.9 (Integral of a Step Function). Given a step function f , define $\int f = \int f(x)dx \in \mathbb{R}$ as follows.

Let $f(x) = \lambda_1 f_1(x) + \cdots + \lambda_n f_n(x)$, where f_i is the characteristic function of $[a_i, b_i)$. Then

$$\int f = \lambda_1(b_1 - a_1) + \cdots + \lambda_n(b_n - a_n) .$$

We prove this is well defined.

PROOF:

- (1)1. LET: $f = \lambda_1 f_1(x) + \cdots + \lambda_m f_m(x) = \mu_1 g_1(x) + \cdots + \mu_n g_n(x)$, where f_i is the characteristic function of $[a_i, b_i)$ and g_i is the characteristic function of $[c_i, d_i)$, with $a_1 < b_1 \leq a_2 < b_2 \leq \cdots \leq a_m < b_m$ and $c_1 < d_1 \leq c_2 < d_2 \leq \cdots \leq c_n < d_n$.
- (1)2. ASSUME: w.l.o.g. none of the λ_i or μ_i is zero.
- (1)3. ASSUME: w.l.o.g. we never have $\lambda_i = \lambda_{i+1}$ and $b_i = a_{i+1}$, and we never have $\mu_i = \mu_{i+1}$ and $d_i = c_{i+1}$.
- (1)4. We have $m = n$ and for all i , $a_i = b_i$ and $c_i = d_i$ and $\lambda_i = \mu_i$.
 - (2)1. ASSUME: w.l.o.g. $m \leq n$
 - (2)2. ASSUME: as induction hypothesis $a_i = b_i$, $c_i = d_i$, $\lambda_i = \mu_i$ for $i = 1, \dots, k$ with $k < m$.
 - (2)3. $a_{k+1} = b_{k+1}$
PROOF: It is $\inf\{x \in (a_k, +\infty) : f(x) \neq 0\}$ (or $\inf\{x \in \mathbb{R} : f(x) \neq 0\}$ if $k = 0$).
 - (2)4. $\lambda_{k+1} = \mu_{k+1}$
PROOF: It is $f(a_{k+1})$.
 - (2)5. $c_{k+1} = d_{k+1}$
PROOF: It is $\sup\{x \in (a_{k+1}, +\infty) : f(x) = \lambda_{k+1}\}$.
 - (2)6. $m = n$
PROOF: For all $x > b_m$ we have $f(x) = 0$.

□

Proposition 17.1.10. If f and g are step functions then $\int(f(x) + g(x))dx = \int f + \int g$.

Proposition 17.1.11. If f is a step function then $\int cf(x)dx = c \int f$.

Proposition 17.1.12. If f and g are step functions and $\forall x. f(x) \leq g(x)$ then $\int f \leq \int g$.

PROOF: We have $g(x) - f(x) \geq 0$ for all x and so $\int(g(x) - f(x))dx \geq 0$. □

Proposition 17.1.13. If f is a step function then $|\int f| \leq \int |f(x)|dx$.

Proposition 17.1.14. If f is a step function and $c \in \mathbb{R}$ then $\int f(x-c)dx = \int f$.

Lemma 17.1.15. *Let f be a step function with $\text{supp } f \subseteq [a_1, b_1) \cup \cdots \cup [a_n, b_n)$. Let M be a constant. If $\forall x. |f(x)| < M$ then*

$$\int |f(x)| dx \leq M \sum_{k=1}^n (b_k - a_k) .$$

Lemma 17.1.16. *Let $\{[a_i, b_i) \mid i \in \mathbb{N}\}$ be a partition of $[a, b)$. Then*

$$\sum_{i=0}^{\infty} (b_i - a_i) = b - a .$$

PROOF:

$\langle 1 \rangle 1$. For all $c \in (a, b]$ we have $\{[a_i, b_i) \cap [a, c) \mid i \in \mathbb{N}\}$ is a partition of $[a, c)$.

$\langle 1 \rangle 2$. For $c \in (a, b]$ and $n \in \mathbb{N}$,

LET: $b_{cn} := \min(b_n, c)$

$\langle 1 \rangle 3$. LET: $S = \{c \in (a, b] \mid \sum_{a_n < b_{cn}} (b_{cn} - a_n) = c - a\}$

$\langle 1 \rangle 4$. $S \neq \emptyset$

$\langle 2 \rangle 1$. PICK n such that $a_n = a$

$\langle 2 \rangle 2$. $b_n \in S$

$\langle 1 \rangle 5$. LET: $s := \sup S$

$\langle 1 \rangle 6$. $s \in S$

$\langle 2 \rangle 1$. PICK an increasing sequence (s_n) in S that converges to S .

$\langle 2 \rangle 2$. For all n we have $s_n - a \leq \sum_{a_m < b_{sm}} (b_{sm} - a_m) \leq s - a$.

PROOF:

$$\begin{aligned} s_n - a &= \sum_{a_m < b_{s_n m}} (b_{s_n m} - a_m) && (s_n \in S) \\ &\leq \sum_{a_m < b_{sm}} (b_{sm} - a_m) && (s_n \leq s) \\ &\leq s - a && (\langle 1 \rangle 1) \end{aligned}$$

$\langle 2 \rangle 3$. $\sum_{a_m < b_{sm}} (b_{sm} - a_m) = s - a$

PROOF: Sandwich Theorem

$\langle 1 \rangle 7$. $s = b$

$\langle 2 \rangle 1$. ASSUME: for a contradiction $s < b$

$\langle 2 \rangle 2$. PICK k such that $s \in [a_k, b_k)$

$\langle 2 \rangle 3$. $b_k \in S$

PROOF: Since $\sum_{a_m < b_{sm}} (b_{sm} - a_m) = \sum_{a_m < b_{b_k m}} (b_{b_k m} - a_m)$.

$\langle 2 \rangle 4$. $b_k \leq s$

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

PROOF: This is a contradiction.

$\langle 1 \rangle 8$. $b \in S$

$\langle 1 \rangle 9$. $\sum_{a_n < b_n} (b_n - a_n) = b - a$

□

Theorem 17.1.17. *Let (f_n) be a decreasing sequence of non-negative step functions such that, for all $x \in \mathbb{R}$, we have $f_n(x) \rightarrow 0$ as $n \rightarrow \infty$. Then $\int f_n \rightarrow 0$ as $n \rightarrow \infty$.*

PROOF:

⟨1⟩1. $(\int f_n)$ is decreasing and bounded below by 0.

⟨1⟩2. LET: $\epsilon := \lim_{n \rightarrow \infty} \int f_n$

⟨1⟩3. ASSUME: for a contradiction $\epsilon > 0$.

⟨1⟩4. PICK $a, b \in \mathbb{R}$ such that $\text{supp } f_0 \subseteq [a, b]$

⟨1⟩5. LET: $\alpha := \epsilon/2(b - a)$

⟨1⟩6. For $n \in \mathbb{N}$,

LET:

$$A_n := \{x \in [a, b) : f_n(x) < \alpha\} .$$

⟨1⟩7. LET: $B_0 := A_0$

⟨1⟩8. For n a positive integer,

LET: $B_n = A_n - A_{n-1}$.

⟨1⟩9. For all n we have $A_n \subseteq A_{n+1}$.

⟨1⟩10. For $m \neq n$ we have $B_m \cap B_n = \emptyset$.

⟨1⟩11. $\bigcup_{n=0}^{\infty} A_n = [a, b)$

PROOF: For all $x \in [a, b)$, there exists N such that $f_N(x) < \alpha$ because $f_n(x) \rightarrow 0$ as $n \rightarrow \infty$.

⟨1⟩12. $\bigcup_{n=0}^{\infty} B_n = [a, b)$

⟨1⟩13. For $n \in \mathbb{N}$,

LET: $B_n = [a_{n1}, b_{n1}) \cup \dots \cup [a_{nk_n}, b_{nk_n})$.

⟨1⟩14. $\sum_{n=0}^{\infty} \sum_{k=1}^{k_n} (b_{nk} - a_{nk}) = b - a$

PROOF: Lemma 17.1.16.

⟨1⟩15. LET:

$$\delta = \frac{\epsilon}{2 \max_x |f_0(x)|} .$$

⟨1⟩16. PICK n_0 such that

$$\sum_{n=n_0}^{\infty} \sum_{k=1}^{k_n} (b_{nk} - a_{nk}) < \delta .$$

⟨1⟩17. $A_{n_0} = B_0 \cup \dots \cup B_{n_0}$

⟨1⟩18. LET: $g : \mathbb{R} \rightarrow \mathbb{R}$,

$$g(x) = \begin{cases} f_{n_0}(x) & \text{if } x \in A_{n_0} \\ 0 & \text{if } x \notin A_{n_0} \end{cases}$$

⟨1⟩19. LET: $h : \mathbb{R} \rightarrow \mathbb{R}$,

$$h(x) = \begin{cases} 0 & \text{if } x \in A_{n_0} \\ f_{n_0}(x) & \text{if } x \notin A_{n_0} \end{cases}$$

⟨1⟩20. $\forall x \in B. f_{n_0}(x) < \alpha$

⟨1⟩21. $\forall x \in \mathbb{R}. g(x) < \alpha$

⟨1⟩22.

$$\int g < \frac{\epsilon}{2}$$

⟨1⟩23.

$$\int h < \frac{\epsilon}{2}$$

PROOF:

$$\begin{aligned} \int h &< \delta \max_x |f_{n_0}(x)| \\ &\leq \delta \max_x |f_0(x)| \\ &= \epsilon/2 \end{aligned}$$

⟨1⟩24.

$$\int f_{n_0} < \epsilon$$

PROOF: Since $\forall x. f_{n_0}(x) = g(x) + h(x)$.

⟨1⟩25.

$$\lim_{n \rightarrow \infty} \int f_n < \epsilon$$

⟨1⟩26. Q.E.D.

PROOF: This contradicts ⟨1⟩2.

□

Corollary 17.1.17.1. *Let (f_n) be an increasing sequence of step functions. If $\lim_{n \rightarrow \infty} f_n(x) \geq 0$ for all x , then $\lim_{n \rightarrow \infty} \int f_n \geq 0$.*

PROOF:

⟨1⟩1. For $n \in \mathbb{N}$,

LET: $g_n : \mathbb{R} \rightarrow \mathbb{R}$ be the function $g_n(x) = \max(0, -f_n(x))$.

⟨1⟩2. (g_n) is a decreasing sequence of step functions and $g_n(x) \rightarrow 0$ as $n \rightarrow \infty$ for all x .

⟨1⟩3. $\int g_n \rightarrow 0$ as $n \rightarrow \infty$

⟨1⟩4. For all $n \in \mathbb{N}$ we have $f_n(x) = \max(0, f_n(x)) - \max(0, -f_n(x))$.

⟨1⟩5.

$$\int f_n = \int \max(0, f_n(x)) dx - \int \max(0, -f_n(x)) dx$$

⟨1⟩6.

$$\lim_{n \rightarrow \infty} \int f_n = \lim_{n \rightarrow \infty} \int \max(0, f_n(x)) dx$$

⟨1⟩7. $\lim_{n \rightarrow \infty} \int f_n \geq 0$

□

17.2 Lebesgue Integration

Definition 17.2.1 (Lebesgue Integration). Let $f : \mathbb{R} \rightarrow \mathbb{R}$. Then f is *Lebesgue integrable* iff there exists a sequence (f_n) of step functions such that:

•

$$\sum_{n=0}^{\infty} \int |f_n(x)| dx < \infty$$

• For all $x \in \mathbb{R}$, if $\sum_{n=0}^{\infty} |f_n(x)| < \infty$, then $f(x) = \sum_{n=0}^{\infty} f_n(x)$.

We write $f \simeq \sum_{n=0}^{\infty} f_n$ for these two conditions.

The *integral* of f is then

$$\int f := \sum_{n=0}^{\infty} \int f_n .$$

Chapter 18

Complex Analysis

Theorem 18.0.1 (Hölder's Inequality). *Let p and q be real numbers with $p > 1$, $q > 1$ and $1/p + 1/q = 1$. If $(x_n) \in l^p$ and $(y_n) \in l^q$ then*

$$\sum_{n=0}^{\infty} |x_n y_n| \leq \left(\sum_{n=0}^{\infty} |x_n|^p \right)^{1/p} \left(\sum_{n=0}^{\infty} |y_n|^q \right)^{1/q}$$

PROOF:

- ⟨1⟩1. LET: p and q be real numbers with $p > 1$ and $q > 1$
- ⟨1⟩2. ASSUME: $1/p + 1/q = 1$
- ⟨1⟩3. LET: $(x_n) \in l^p$
- ⟨1⟩4. LET: $(y_n) \in l^q$
- ⟨1⟩5. ASSUME: w.l.o.g. $x_0 \neq 0$ and $y_0 \neq 0$
- ⟨1⟩6. For all $x \in [0, 1]$, we have

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

PROOF:

- ⟨2⟩1. LET: $f : [0, 1] \rightarrow \mathbb{R}$ be the function

$$f(x) = \frac{1}{p}x + \frac{1}{q} - x^{1/p}.$$

- ⟨2⟩2. $f'(x) = \frac{1}{p} - \frac{1}{p}x^{-1/q}$ for $x \in (0, 1]$
- ⟨2⟩3. $f'(x) < 0$ for $x \in (0, 1]$
- ⟨2⟩4. $f(1) = 1/p + 1/q - 1 = 0$
- ⟨2⟩5. $f(x) \geq 0$ for all $x \in [0, 1]$
- ⟨1⟩7. For all non-negative reals a and b , we have

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

- ⟨2⟩1. LET: a and b be non-negative reals.

- ⟨2⟩2. CASE: $a^p \leq b^q$

- ⟨3⟩1. $0 \leq a^p/b^q \leq 1$

- ⟨3⟩2.

$$ab^{-q/p} \leq \frac{1}{p} \frac{a^p}{b^q} + \frac{1}{q}$$

PROOF: Taking $x = a^p/b^q$ in $\langle 1 \rangle 6$.

$\langle 3 \rangle 3$.

$$ab^{1-q} \leq \frac{1}{p} \frac{a^p}{b^q} + \frac{1}{q}$$

PROOF: $-q/p = 1 - q$ from $\langle 1 \rangle 2$.

$\langle 3 \rangle 4$.

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

$\langle 2 \rangle 3$. CASE: $b^q \leq a^p$

PROOF: Similar.

$\langle 1 \rangle 8$. For $j = 1, \dots, n$, we have

$$\frac{|x_j|}{(\sum_{k=0}^n |x_k|^p)^{1/p}} \frac{|y_j|}{(\sum_{k=0}^n |y_k|^q)^{1/q}} \leq \frac{1}{p} \frac{|x_j|^p}{\sum_{k=0}^n |x_k|^p} + \frac{1}{q} \frac{|y_j|^q}{\sum_{k=0}^n |y_k|^q}$$

PROOF: From $\langle 1 \rangle 7$ with

$$a = \frac{|x_j|}{(\sum_{k=0}^n |x_k|^p)^{1/p}} \text{ and } b = \frac{|y_j|}{(\sum_{k=0}^n |y_k|^q)^{1/q}}.$$

$\langle 1 \rangle 9$.

$$\frac{\sum_{j=0}^n |x_j| |y_j|}{(\sum_{k=0}^n |x_k|^p)^{1/p} (\sum_{k=0}^n |y_k|^q)^{1/q}} \leq 1$$

PROOF:

$$\begin{aligned} \frac{\sum_{j=0}^n |x_j| |y_j|}{(\sum_{k=0}^n |x_k|^p)^{1/p} (\sum_{k=0}^n |y_k|^q)^{1/q}} &\leq \frac{1}{p} + \frac{1}{q} \quad (\text{Taking the sum } j = 0 \text{ to } n \text{ in } \langle 1 \rangle 8) \\ &= 1 \end{aligned} \quad (\langle 1 \rangle 2)$$

$\langle 1 \rangle 10$. Q.E.D.

PROOF: Taking the limit $n \rightarrow \infty$ in $\langle 1 \rangle 9$.

□

Theorem 18.0.2 (Minkowski's Inequality). *Let p be a real number, $p \geq 1$. Let $(x_n), (y_n) \in l^p$. Then*

$$\left(\sum_{n=1}^{\infty} |x_n + y_n|^p \right)^{1/p} \leq \left(\sum_{n=1}^{\infty} |x_n|^p \right)^{1/p} + \left(\sum_{n=1}^{\infty} |y_n|^p \right)^{1/p}$$

PROOF:

$\langle 1 \rangle 1$. LET: p be a real number with $p \geq 1$

$\langle 1 \rangle 2$. ASSUME: w.l.o.g. $p > 1$

PROOF: The case $p = 1$ is just the Triangle Inequality.

$\langle 1 \rangle 3$. LET: q be the real such that $1/p + 1/q = 1$

$\langle 1 \rangle 4$.

$$\begin{aligned} \sum_{n=0}^{\infty} |x_n + y_n|^p &\leq \left(\sum_{n=0}^{\infty} |x_n|^p \right)^{1/p} \left(\sum_{n=0}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \\ &\quad + \left(\sum_{n=0}^{\infty} |y_n|^p \right)^{1/p} \left(\sum_{n=0}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \end{aligned}$$

PROOF:

$$\begin{aligned}
\sum_{n=0}^{\infty} |x_n + y_n|^p &= \sum_{n=0}^{\infty} |x_n + y_n| |x_n + y_n|^{p-1} \\
&\leq \sum_{n=0}^{\infty} |x_n| |x_n + y_n|^{p-1} + \sum_{n=0}^{\infty} |y_n| |x_n + y_n|^{p-1} \quad (\text{Triangle Inequality}) \\
&\leq \left(\sum_{n=0}^{\infty} |x_n|^p \right)^{1/p} \left(\sum_{n=0}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \\
&\quad + \left(\sum_{n=0}^{\infty} |y_n|^p \right)^{1/p} \left(\sum_{n=0}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \quad (\text{Hölder's Inequality})
\end{aligned}$$

$\langle 1 \rangle 5.$

$$\sum_{n=0}^{\infty} |x_n + y_n|^p \leq \left\{ \left(\sum_{n=0}^{\infty} |x_n|^p \right)^{1/p} + \left(\sum_{n=0}^{\infty} |y_n|^p \right)^{1/p} \right\} \left(\sum_{n=0}^{\infty} |x_n + y_n|^p \right)^{1/q}$$

$\langle 1 \rangle 6.$ Q.E.D.

□

Chapter 19

Topology

19.1 Topological Spaces

Definition 19.1.1 (Topology). Let X be a set. A *topology* on X is a set $\mathcal{T} \subseteq \mathcal{P}X$, whose elements are called *open sets*, such that:

- $X \in \mathcal{T}$
- $\forall \mathcal{U} \subseteq \mathcal{T}. \bigcup \mathcal{U} \in \mathcal{T}$
- $\forall U, V \in \mathcal{T}. U \cap V \in \mathcal{T}$

A *topological space* is a pair (X, \mathcal{T}) such that X is a set and \mathcal{T} is a topology on X . We refer to the elements of X as *points*.

An *open neighbourhood* of a point x is an open set U such that $x \in U$. We write \mathcal{T}_x for the set of all open neighbourhoods of x .

Definition 19.1.2 (Closed Set). In a topological space X , a set C is *closed* iff $X - C$ is open.

Definition 19.1.3 (Discrete Topology). The *discrete topology* on a set X is $\mathcal{P}X$.

Definition 19.1.4 (Indiscrete Topology). The *indiscrete topology* or *trivial topology* on a set X is $\{\emptyset, X\}$.

Definition 19.1.5 (Finer, Coarser). Let \mathcal{T} and \mathcal{T}' be topologies on the same set X . Then \mathcal{T} is *finer*, *larger* or *stronger* than \mathcal{T}' , and \mathcal{T}' is *coarser*, *smaller* or *weaker* than \mathcal{T} , iff $\mathcal{T}' \subseteq \mathcal{T}$.

Definition 19.1.6 (Basis). Let X be a set. A *basis* for a topology on X is a set $\mathcal{B} \subseteq \mathcal{P}X$, whose elements we call *basic open neighbourhoods*, such that:

- $\bigcup \mathcal{B} = X$
- $\forall A, B \in \mathcal{B}. \forall x \in A \cap B. \exists C \in \mathcal{B}. x \in C \subseteq A \cap B.$

The topology *generated* by \mathcal{B} is the coarsest topology that includes \mathcal{B} .

Proposition 19.1.7. *The topology generated by \mathcal{B} is $\{U \in \mathcal{P}X \mid \forall x \in U. \exists B \in \mathcal{B}. x \in B \subseteq U\}$*

19.2 Continuous Functions

Definition 19.2.1 (Continuous). Let X and Y be topological spaces. Let $f : X \rightarrow Y$. Then f is *continuous* iff, for every open set U in Y , the set $f^{-1}(U)$ is open in X .

Proposition 19.2.2. *For any topological space X , the identity function $\text{id}_X : X \rightarrow X$ is continuous.*

Proposition 19.2.3. *If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are continuous then $g \circ f : X \rightarrow Z$ is continuous.*

Definition 19.2.4. Let Top be the category of topological spaces and continuous functions.

Proposition 19.2.5. *Let X and Y be topological spaces and $f : X \rightarrow Y$. Then f is continuous if and only if, for every closed set C in Y , we have $f^{-1}(C)$ is closed in X .*

Definition 19.2.6 (Continuous at a Point). Let X and Y be topological spaces. Let $f : X \rightarrow Y$. Let $x \in X$. Then f is *continuous at x* iff, for every open neighbourhood V of $f(x)$, we have $f^{-1}(V)$ is open.

Definition 19.2.7. The category of *pointed* topological spaces, Top_* , is the category with:

- objects all pairs (A, a) where A is a topological space and $a \in A$;
- morphisms $f : (A, a) \rightarrow (B, b)$ all continuous functions $f : A \rightarrow B$ such that $f(a) = b$.

Definition 19.2.8 (Homeomorphism). A *homeomorphism* is an isomorphism in Top . Two isomorphic topological spaces are called *homeomorphic*.

Definition 19.2.9 (Topological Property). A property of topological spaces is a *topological* property iff it is preserved by homeomorphism.

Proposition 19.2.10. *Cardinality of a topological space is a topological property.*

19.3 Convergence

Definition 19.3.1 (Convergence). Let X be a topological space. Let (x_n) be a sequence in X and $l \in X$. Then (x_n) *converges* to l , $x_n \rightarrow l$ as $n \rightarrow \infty$, if and only if, for every open neighbourhood U of l , there exists N such that $\forall n \geq N. x_n \in U$.

Theorem 19.3.2. *Let X and Y be topological spaces. Let Z be a closed subspace of X and $f : Z \rightarrow Y$ a continuous function. Then the graph of f , $G = \{(x, f(x)) \mid x \in Z\}$, is closed in $X \times Y$.*

PROOF:

$\langle 1 \rangle 1$. LET: $((x_n, f(x_n)))$ be a sequence in G .

$\langle 1 \rangle 2$. LET: $(x_n, f(x_n)) \rightarrow (x, y)$ as $n \rightarrow \infty$

$\langle 1 \rangle 3$. $x \in W$

PROOF: Since $x_n \rightarrow x$ and W is closed.

$\langle 1 \rangle 4$. $y = f(x)$

PROOF:

$$\begin{aligned} y &= \lim_{n \rightarrow \infty} f(x_n) \\ &= f\left(\lim_{n \rightarrow \infty} x_n\right) \\ &= f(x) \end{aligned}$$

□

19.4 Homotopy

Definition 19.4.1. Let \mathbf{hTop} be the category whose objects are topological spaces, and whose morphisms are homotopy classes of continuous functions.

Definition 19.4.2. A *homotopy equivalence* is an isomorphism in \mathbf{hTop} . Isomorphic topological spaces are called *homotopic*.

19.5 Metric Spaces

Definition 19.5.1 (Metric). Let X be a set. A *metric* on a set X is a function $d : X^2 \rightarrow \mathbb{R}$ such that:

- $\forall x, y \in X. d(x, y) \geq 0$
- $\forall x, y \in X. d(x, y) = d(y, x)$
- *Triangle Inequality* $\forall x, y, z \in X. d(x, y) + d(y, z) \geq d(x, z)$
- $\forall x, y \in X. d(x, y) = 0$ iff $x = y$.

A *metric space* is a pair (X, d) such that d is a metric on X .

Definition 19.5.2 (Open Ball). In a metric space X , let $c \in X$ and $r > 0$. The *open ball* with *centre* c and *radius* r is

$$B(c, r) := \{x \in X \mid d(x, c) < r\} .$$

Proposition 19.5.3. *In a metric space, the set of open balls forms a basis for a topology.*

Definition 19.5.4 (Metric Topology). Given a metric space X , the *metric topology* on X is the topology generated by the basis of open balls.

A topological space (X, \mathcal{T}) is *metrizable* iff there exists a metric d on X such that \mathcal{T} is the metric topology induced by d .

We identify a metric space with this topological space.

Proposition 19.5.5. *If d is a metric on X and $Y \subseteq X$ then $d \upharpoonright Y^2$ is a metric on Y .*

We write just Y for the metric space $(Y, d \upharpoonright Y^2)$.

Proposition 19.5.6. *Let X and Y be metric spaces. Let $f : X \rightarrow Y$. Then f is continuous if and only if, for every sequence (x_n) in X and $l \in X$, if $x_n \rightarrow l$ as $n \rightarrow \infty$ then $f(x_n) \rightarrow f(l)$ as $n \rightarrow \infty$.*

PROOF:

- $\langle 1 \rangle 1$. If f is continuous then, for every sequence (x_n) in X and $l \in X$, if $x_n \rightarrow l$ as $n \rightarrow \infty$, then $f(x_n) \rightarrow f(l)$ as $n \rightarrow \infty$.
- $\langle 2 \rangle 1$. ASSUME: f is continuous.
- $\langle 2 \rangle 2$. LET: (x_n) be a sequence in X .
- $\langle 2 \rangle 3$. LET: $l \in X$
- $\langle 2 \rangle 4$. ASSUME: $x_n \rightarrow l$ as $n \rightarrow \infty$.
- $\langle 2 \rangle 5$. LET: V be an open neighbourhood of $f(l)$
- $\langle 2 \rangle 6$. $f^{-1}(V)$ is an open neighbourhood of l .
- $\langle 2 \rangle 7$. PICK N such that $\forall n \geq N. x_n \in f^{-1}(V)$
- $\langle 2 \rangle 8$. $\forall n \geq N. f(x_n) \in V$
- $\langle 1 \rangle 2$. If, for every sequence (x_n) in X and $l \in X$, if $x_n \rightarrow l$ as $n \rightarrow \infty$, then $f(x_n) \rightarrow f(l)$ as $n \rightarrow \infty$, then f is continuous.
- $\langle 2 \rangle 1$. ASSUME: f is not continuous.
- $\langle 2 \rangle 2$. PICK an open set V in Y such that $f^{-1}(V)$ is not open in X
- $\langle 2 \rangle 3$. PICK $l \in f^{-1}(V)$ such that, for all $\epsilon > 0$, $B(l, \epsilon) \not\subseteq f^{-1}(V)$.
- $\langle 2 \rangle 4$. For $n \in \mathbb{N}$, PICK $x_n \in B(l, 1/(n+1))$ such that $x_n \notin f^{-1}(V)$.
- $\langle 2 \rangle 5$. $x_n \rightarrow l$ as $n \rightarrow \infty$.
- $\langle 2 \rangle 6$. $f(x_n) \not\rightarrow f(l)$ as $n \rightarrow \infty$

□

Proposition 19.5.7. *Completeness is not a topological property.*

PROOF: We have $(-1, 1) \cong \mathbb{R}$, but \mathbb{R} is complete and $(-1, 1)$ is not. □

Chapter 20

Ring Theory

Definition 20.0.1. Given a ring R , let $R\text{-Mod}$ be the category of modules over R and R -linear maps.

Chapter 21

Linear Algebra

21.1 Vector Spaces

Definition 21.1.1 (Vector Space). Let K be a field. A *vector space* over K consists of:

- a set V , whose elements are called *vectors*;
- an operation $+$: $V^2 \rightarrow V$, *addition*;
- an operation \cdot : $K \times V \rightarrow V$, *scalar multiplication*

such that:

- V is an Abelian group under $+$
- $\forall \alpha, \beta \in K. \forall x \in V. \alpha(\beta x) = (\alpha\beta)x$
- $\forall \alpha, \beta \in K. \forall x \in V. (\alpha + \beta)x = \alpha x + \beta x$
- $\forall \alpha \in K. \forall x, y \in V. \alpha(x + y) = \alpha x + \alpha y$
- $\forall x \in V. 1x = x$

We call the elements of K *scalars*. A *real vector space* is a vector space over \mathbb{R} , and a *complex vector space* is a vector space over \mathbb{C} .

Proposition 21.1.2. *Let K be a field. Let V be a vector space over K . For any $\lambda \in K$ we have $\lambda 0 = 0$.*

PROOF:

$$\begin{aligned}\lambda 0 &= \lambda(0 + 0) \\ &= \lambda 0 + \lambda 0 \\ \therefore 0 &= \lambda 0\end{aligned}$$

□

Proposition 21.1.3. *Let K be a field. Let V be a vector space over K . Let $\lambda \in K$ and $x \in V$. If $\lambda x = 0$ then either $\lambda = 0$ or $x = 0$.*

PROOF: If $\lambda \neq 0$ then $x = 1x = \lambda^{-1}\lambda x = \lambda^{-1}0 = 0$. \square

Proposition 21.1.4. *Let K be a field. Let V be a vector space over K . For any $x \in V$ we have $0x = 0$.*

PROOF:

$$\begin{aligned} 0x &= (0 + 0)x \\ &= 0x + 0x \\ \therefore 0 &= 0x \end{aligned} \quad \square$$

Proposition 21.1.5. *Let K be a field. Let V be a vector space over K . For any $x \in V$, we have $(-1)x = -x$.*

PROOF:

$$\begin{aligned} x + (-1)x &= 1x + (-1)x \\ &= (1 + (-1))x \\ &= 0x \\ &= 0 \\ \therefore (-1)x &= -x \end{aligned} \quad \square$$

Proposition 21.1.6. *Let K be a field. Then K is a vector space over K under addition and multiplication in K .*

PROOF: Easy. \square

Proposition 21.1.7. \mathbb{C} is a vector space over \mathbb{R} .

PROOF: Easy. \square

Proposition 21.1.8. *Let K be a field. 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 under*

$$\begin{aligned} (f + g)(i) &= f(i) + g(i) & (f, g \in \prod_{i \in I} V_i, x \in X) \\ (\lambda f)(x) &= \lambda f(x) & (\lambda \in K, f \in \prod_{i \in I} V_i, x \in X) \end{aligned}$$

PROOF: Easy. \square

21.2 Subspaces

Definition 21.2.1 (Vector Subspace). Let K be a field. Let V be a vector space over K . A *vector subspace* of V is a subset $U \subseteq V$ such that, for all $\alpha, \beta \in K$ and $x, y \in U$, we have $\alpha x + \beta y \in U$.

It is a *proper* subspace iff $U \neq V$.

Proposition 21.2.2. *If U is a subspace of V then U is a vector space under the restrictions of $+$ and \cdot to U .*

PROOF: Easy. \square

Proposition 21.2.3. *V is a subspace of V .*

PROOF: Easy. \square

Proposition 21.2.4. *If U is a subspace of V and V is a subspace of W then U is a subspace of W .*

PROOF: Easy. \square

Definition 21.2.5. Let Ω be a topological space. Then $\mathcal{C}(\Omega)$ is the complex vector space of all continuous functions from Ω to \mathbb{C} . This is a subspace of \mathbb{C}^Ω .

Definition 21.2.6. Let $n, k \in \mathbb{N}$. Let Ω be an open subset of \mathbb{R}^n . Then $\mathcal{C}^k(\Omega)$ is the complex vector space of all functions $\Omega \rightarrow \mathbb{C}$ that have all continuous partial derivatives of order k . This is a subspace of $\mathcal{C}(\Omega)$. If $l > k$ then $\mathcal{C}^l(\Omega)$ is a subspace of $\mathcal{C}^k(\Omega)$.

Definition 21.2.7. Let $n \in \mathbb{N}$. Let Ω be an open subset of \mathbb{R}^n . Then $\mathcal{C}^\infty(\Omega)$ is the complex vector space of all infinitely differentiable functions $\Omega \rightarrow \mathbb{C}$. This is a subspace of $\mathcal{C}^k(\Omega)$ for all k .

Definition 21.2.8. Let $n \in \mathbb{N}$. Let Ω be an open subset of \mathbb{R}^n . Then $\mathcal{P}(\Omega)$ is the complex vector space of all complex polynomials of n variables, considered as functions $\Omega \rightarrow \mathbb{C}$. This is a subspace of $\mathcal{C}^\infty(\Omega)$.

Proposition 21.2.9. *The space of all convergent sequences in \mathbb{C} is a subspace of the space of all bounded sequences in \mathbb{C} , which is a subspace of $\mathbb{C}^\mathbb{N}$.*

PROOF: Easy. \square

Definition 21.2.10. Let p be a real number, $p \geq 1$. Let l^p be the set of all complex sequences (z_n) such that $\sum_{n=1}^\infty |z_n|^p < \infty$.

Proposition 21.2.11. *For p a real number ≥ 1 , we have that l^p is a subspace of $\mathbb{C}^\mathbb{N}$.*

PROOF:

(1)1. For all $(x_n), (y_n) \in l^p$, we have $(x_n + y_n) \in l^p$.

PROOF: From Minkowski's Inequality.

(1)2. For all $\lambda \in \mathbb{C}$ and $(x_n) \in l^p$ we have $(\lambda x_n) \in l^p$

PROOF:

$$\sum_{n=1}^\infty |\lambda x_n|^p = |\lambda|^p \sum_{n=1}^\infty |x_n|^p < \infty$$

\square

Definition 21.2.12 (Linear Combination). Let K be a field. Let V be a vector space over K . Let $x, x_1, \dots, x_n \in V$. Then x is a *linear combination* of x_1, \dots, x_n iff there exist $\alpha_1, \dots, \alpha_n \in K$ such that

$$x = \alpha_1 x_1 + \dots + \alpha_n x_n .$$

Definition 21.2.13 (Linearly Independent). A finite set of vectors $\{x_1, \dots, x_n\}$ is *linearly independent* iff, whenever $\alpha_1 x_1 + \dots + \alpha_n x_n = 0$, then $\alpha_1 = \dots = \alpha_n = 0$.

A set of vectors is *linearly independent* iff every finite subset is linearly independent; otherwise, it is *linearly dependent*.

Definition 21.2.14 (Span). Let \mathcal{A} be a set of vectors. The *span* of \mathcal{A} , $\text{span } \mathcal{A}$, is the set of all linear combinations of elements of \mathcal{A} .

Proposition 21.2.15. $\text{span } \mathcal{A}$ is the smallest subspace of V that includes \mathcal{A} .

PROOF: Easy. \square

Definition 21.2.16 (Basis). A *basis* for V is a linearly independent set of vectors \mathcal{B} such that $\text{span } \mathcal{B} = V$.

Definition 21.2.17 (Finite Dimensional). A vector space is *finite dimensional* iff it has a finite basis; otherwise it is *infinite dimensional*.

Proposition 21.2.18. In a finite dimensional vector space, any two bases have the same number of elements.

Definition 21.2.19 (Dimension). The *dimension* of a finite dimensional vector space V , $\dim V$, is the number of elements in any basis.

Proposition 21.2.20.

$$\dim K^n = n$$

PROOF: The standard basis is the set of vectors with one coordinate 1 and all others 0. \square

Proposition 21.2.21. The dimension of \mathbb{C}^n as a real vector space is $2n$.

Proposition 21.2.22. The set of all step functions is a subspace of $\mathbb{R}^{\mathbb{R}}$.

21.3 Linear Transformations

Definition 21.3.1 (Linear Transformation). Let K be a field. Let U and V be vector spaces over K . Let $T : U \rightarrow V$. Then T is a *linear transformation* iff

$$\forall \alpha, \beta \in K. \forall x, y \in U. T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) .$$

Let Vect_K be the category of vector spaces over K and linear transformations.

Proposition 21.3.2. *If $T : U \rightarrow V$ is a linear transformation then $T(U)$ is a subspace of V .*

Proposition 21.3.3. *If $T : U \rightarrow V$ is a linear transformation then the graph of T , $\{(x, T(x)) \mid x \in U\}$, is a subspace of $U \times V$.*

Definition 21.3.4 (Null Space). Let U and V be vector spaces over K and $T : U \rightarrow V$. The *null space* of T is

$$\mathcal{N}(T) := \{x \in U \mid T(x) = 0\} .$$

Proposition 21.3.5. *If $T : U \rightarrow V$ is a linear transformation then $\mathcal{N}(T)$ is a subspace of U .*

Proposition 21.3.6. *Let U and V be vector spaces over K . The set of all linear transformations $U \rightarrow V$ is a vector space over K under*

$$\begin{aligned} (S + T)(u) &= S(u) + T(u) \\ (\lambda S)(u) &= \lambda S(u) \end{aligned}$$

21.4 Normed Spaces

Definition 21.4.1 (Norm). Let K be either \mathbb{R} or \mathbb{C} . A *norm* on a vector space V over K is a function $\| \cdot \| : V \rightarrow \mathbb{R}$ such that:

1. $\forall x \in V. \|x\| = 0 \Rightarrow x = 0$
2. $\forall \lambda \in K. \forall x \in V. \|\lambda x\| = |\lambda| \|x\|$
3. *Triangle Inequality* $\forall x, y \in V. \|x + y\| \leq \|x\| + \|y\|$

Proposition 21.4.2. *Let K be either \mathbb{R} or \mathbb{C} . Let V be a normed space over K . Define $d : V^2 \rightarrow \mathbb{R}$ by $d(x, y) = \|x - y\|$. Then d is a metric on V .*

PROOF: Easy. \square

We identify any normed space V with this metric space.

Proposition 21.4.3. *Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector space over K . Let $\| \cdot \|$ be a norm on V . Then*

$$\|0\| = 0 .$$

PROOF:

$$\begin{aligned} \|0\| &= \|0 \cdot 0\| && \text{(Proposition 21.1.4)} \\ &= |0| \|0\| && \text{(Axiom 2 for a norm)} \\ &= 0 && \square \end{aligned}$$

Proposition 21.4.4. *Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector space over K . Let $\| \cdot \|$ be a norm on V . Let $x \in V$. Then*

$$\|x\| \geq 0 .$$

PROOF:

$$\begin{aligned}
 0 &= \|0\| && \text{(Proposition 21.4.3)} \\
 &= \|x - x\| \\
 &\leq \|x\| + \|-x\| && \text{(Triangle Inequality)} \\
 &= \|x\| + \|x\| && \text{(Axiom 2 for a norm)} \\
 &= 2\|x\| && \square
 \end{aligned}$$

Proposition 21.4.5. *Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector space over K . Let $\|\cdot\|$ be a norm on V . Let $x, y \in V$. Then*

$$|\|x\| - \|y\|| \leq \|x - y\|.$$

PROOF:

$$\langle 1 \rangle 1. \quad \|x\| - \|y\| \leq \|x - y\|$$

PROOF: $\|x\| \leq \|x - y\| + \|y\|$ by the Triangle Inequality.

$$\langle 1 \rangle 2. \quad \|y\| - \|x\| \leq \|x - y\|$$

PROOF:

$$\begin{aligned}
 \|x\| + \|x - y\| &= \|x\| + \|y - x\| && \text{(Axiom 2 for a norm)} \\
 &\leq \|y\| && \text{(Triangle Inequality)}
 \end{aligned}$$

\square

Corollary 21.4.5.1. *Let V be a normed space. Then $\|\cdot\| : V \rightarrow \mathbb{R}$ is continuous.*

Definition 21.4.6 (Euclidean Norm). The *Euclidean norm* on \mathbb{C}^n is defined by

$$\|(z_1, \dots, z_n)\| = \sqrt{|z_1|^2 + \dots + |z_n|^2}$$

Proposition 21.4.7. *Define $\|\cdot\| : \mathbb{C}^n \rightarrow \mathbb{R}$ by*

$$\|(z_1, \dots, z_n)\| = |z_1| + \dots + |z_n|$$

Then this defines a norm on \mathbb{C}^n .

PROOF: Easy. \square

Proposition 21.4.8. *Define $\|\cdot\| : \mathbb{C}^n \rightarrow \mathbb{R}$ by*

$$\|(z_1, \dots, z_n)\| = \max(|z_1|, \dots, |z_n|)$$

Then this defines a norm on \mathbb{C}^n .

PROOF: Easy. \square

Proposition 21.4.9. *Let Ω be a closed bounded subset of \mathbb{R}^n . Define $\|\cdot\| : \mathcal{C}(\Omega) \rightarrow \mathbb{R}$ by $\|f\| = \max_{x \in \Omega} |f(x)|$. Then $\|\cdot\|$ defines a norm on $\mathcal{C}(\Omega)$.*

PROOF: Easy. \square

Proposition 21.4.10. Let p be a real number, $p \geq 1$. Define $\| \cdot \| : l^p \rightarrow \mathbb{R}$ by

$$\|(z_n)\| = \left(\sum_{n=0}^{\infty} |z_n|^p \right)^{1/p}.$$

Then this defines a norm on l^p .

PROOF: Easy. The triangle inequality is Minkowski's Inequality. \square

Definition 21.4.11 (Normed Space). Let K be either \mathbb{R} or \mathbb{C} . A *normed space* over K consists of a vector space V over K and a norm on V .

We shall write simply:

- K^n for the normed space K^n under the Euclidean norm
- l^p for the normed space l^p under the norm $\|(z_n)\| = (\sum_{n=0}^{\infty} |z_n|^p)^{1/p}$.

Proposition 21.4.12. Let K be either \mathbb{R} or \mathbb{C} . Let V be a normed space over K . If $x_n \rightarrow l$ as $n \rightarrow \infty$ in V and $\lambda_n \rightarrow \lambda$ as $n \rightarrow \infty$ in K , then $\lambda_n x_n \rightarrow \lambda l$ as $n \rightarrow \infty$.

PROOF:

$\langle 1 \rangle 1$. LET: $\epsilon > 0$

$\langle 1 \rangle 2$. LET: $K = |\lambda| + \epsilon/2 \|l\|$

$\langle 1 \rangle 3$. PICK N such that, for all $n \geq N$, we have $|\lambda_n - \lambda| < \epsilon/2 \|l\|$ and $\|x_n - l\| < \epsilon/(2K)$

$\langle 1 \rangle 4$. For all $n \geq N$ we have $|\lambda_n| < K$

$\langle 1 \rangle 5$. $\|\lambda_n x_n - \lambda l\| < \epsilon$

PROOF:

$$\begin{aligned} \|\lambda_n x_n - \lambda l\| &\leq \|\lambda_n x_n - \lambda_n l\| + \|\lambda_n l - \lambda l\| \\ &= |\lambda_n| \|x_n - l\| + |\lambda_n - \lambda| \|l\| \\ &< K \frac{\epsilon}{2K} + \frac{\epsilon}{2\|l\|} \|l\| \\ &= \epsilon \end{aligned}$$

\square

Proposition 21.4.13. In a normed space, if $x_n \rightarrow l$ and $y_n \rightarrow m$ then $x_n + y_n \rightarrow l + m$

PROOF:

$$\begin{aligned} \|(x_n + y_n) - (l + m)\| &\leq \|x_n - l\| + \|y_n - m\| \\ &\rightarrow 0 \end{aligned}$$

\square

Definition 21.4.14 (Uniform Convergence). Let Ω be a closed bounded set in \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 if and only if, for every $\epsilon > 0$, there exists N such that $\forall x \in \Omega, \forall n \geq N, |f_n(x) - f(x)| < \epsilon$.

Proposition 21.4.15. (f_n) converges uniformly to f iff (f_n) converges to f under the uniform convergence norm.

PROOF: Easy. \square

Proposition 21.4.16. There is no norm on $\mathcal{C}([0, 1])$ that induces pointwise convergence.

PROOF:

$\langle 1 \rangle 1$. LET: $\| \cdot \|$ be any norm on $\mathcal{C}([0, 1])$

$\langle 1 \rangle 2$. For $n \in \mathbb{N}$, define $g_n \in \mathcal{C}([0, 1])$ by

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

$\langle 1 \rangle 3$. For all $n \in \mathbb{N}$ we have $\|g_n\| \neq 0$

$\langle 1 \rangle 4$. For $n \in \mathbb{N}$,

LET: $f_n = g_n / \|g_n\|$

$\langle 1 \rangle 5$. For all $n \in \mathbb{N}$, $\|f_n\| = 1$

$\langle 1 \rangle 6$. f_n does not converge to 0

$\langle 1 \rangle 7$. $f_n \rightarrow 0$ as $n \rightarrow \infty$ pointwise.

\square

Definition 21.4.17 (Equivalent Norms). Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector spaces over K . Then two norms $\| \cdot \|_1$ and $\| \cdot \|_2$ are *equivalent* if and only if, for any sequence (x_n) in V and $l \in V$, we have $x_n \rightarrow l$ under $\| \cdot \|_1$ if and only if $x_n \rightarrow l$ under $\| \cdot \|_2$.

Proposition 21.4.18. Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector spaces over K . Let $\| \cdot \|_1$ and $\| \cdot \|_2$ be norms on V . Then $\| \cdot \|_1$ and $\| \cdot \|_2$ are equivalent if and only if there exist positive reals α and β such that, for all $x \in V$,

$$\alpha \|x\|_1 \leq \|x\|_2 \leq \beta \|x\|_1 \quad (21.1)$$

PROOF:

$\langle 1 \rangle 1$. If $\| \cdot \|_1$ and $\| \cdot \|_2$ are equivalent then (21.1) holds.

$\langle 2 \rangle 1$. ASSUME: $\| \cdot \|_1$ and $\| \cdot \|_2$ are equivalent.

$\langle 2 \rangle 2$. There exists $\alpha > 0$ such that, for all $x \in V$, we have $\alpha \|x\|_1 \leq \|x\|_2$

$\langle 3 \rangle 1$. ASSUME: for a contradiction $\forall \alpha > 0. \exists x \in V. \alpha \|x\|_1 > \|x\|_2$

$\langle 3 \rangle 2$. For $n \in \mathbb{Z}^+$, choose $x_n \in V$ such that $1/n \|x_n\|_1 > \|x_n\|_2$

$\langle 3 \rangle 3$. For $n \in \mathbb{Z}^+$,

LET:

$$y_n = \frac{1}{\sqrt{n}} \frac{x_n}{\|x_n\|_2}$$

$\langle 3 \rangle 4$. $\|y_n\|_2 \rightarrow 0$ as $n \rightarrow \infty$

$\langle 3 \rangle 5$. For all $n \in \mathbb{Z}^+$, $\|y_n\|_1 > \sqrt{n}$

$\langle 3 \rangle 6$. $\|y_n\| \not\rightarrow 0$ as $n \rightarrow \infty$

$\langle 2 \rangle 3$. There exists $\beta > 0$ such that, for all $x \in V$, we have $\|x\|_2 \leq \beta \|x\|_1$

PROOF: Similar.

(1)2. If (21.1) holds then $\| \cdot \|_1$ and $\| \cdot \|_2$ are equivalent.

(2)1. ASSUME: (21.1) holds.

(2)2. LET: (x_n) be a sequence in V and $l \in V$

(2)3. If $x_n \rightarrow l$ under $\| \cdot \|_1$ then $x_n \rightarrow l$ under $\| \cdot \|_2$.

(3)1. ASSUME: $x_n \rightarrow l$ und $\| \cdot \|_1$.

(3)2. LET: $\epsilon > 0$

(3)3. PICK N such that $\forall n \geq N. \|x_n - l\| < \epsilon/\beta$

(3)4. LET: $n \geq N$

(3)5. $\|x_n - l\|_2 < \epsilon$

PROOF:

$$\begin{aligned} \|x_n - l\|_2 &\leq \beta \|x_n - l\|_1 \\ &< \epsilon \end{aligned}$$

(2)4. If $x_n \rightarrow l$ under $\| \cdot \|_2$ then $x_n \rightarrow l$ under $\| \cdot \|_1$.

PROOF: Similar.

□

Proposition 21.4.19. *Let K be either \mathbb{R} or \mathbb{C} . Let V be a normed space over K . If $x_1, \dots, x_n \in V$ are linearly independent, then there exists $c > 0$ such that, for all $\alpha_1, \dots, \alpha_n \in K$,*

$$\|\alpha_1 x_1 + \dots + \alpha_n x_n\| \geq c(|\alpha_1| + \dots + |\alpha_n|) .$$

PROOF:

(1)1. LET: $B = \{(\beta_1, \dots, \beta_n) \in K^n \mid |\beta_1| + \dots + |\beta_n| = 1\}$

(1)2. LET: $f : B \rightarrow \mathbb{R}$ be the function

$$f(\beta_1, \dots, \beta_n) = \|\beta_1 x_1 + \dots + \beta_n x_n\| .$$

(1)3. LET: c be the minimum value in $f(B)$

PROOF: f is continuous and B is compact.

(1)4. $c > 0$

PROOF: We never have $f(\beta_1, \dots, \beta_n) = 0$ by linear independence.

(1)5. LET: $\alpha_1, \dots, \alpha_n \in K$

(1)6. ASSUME: w.l.o.g. $\alpha_1, \dots, \alpha_n$ are not all zero.

(1)7. For $i = 1, \dots, n$,

$$\text{LET: } \beta_i = \alpha_i / (|\alpha_1| + \dots + |\alpha_n|)$$

(1)8. $(\beta_1, \dots, \beta_n) \in B$

(1)9. $f(\beta_1, \dots, \beta_n) \geq c$

(1)10. $\|\alpha_1 x_1 + \dots + \alpha_n x_n\| \geq c(|\alpha_1| + \dots + |\alpha_n|)$

□

Theorem 21.4.20. *Let K be either \mathbb{R} or \mathbb{C} . Let V be a finite dimensional vector space over K . Then any two norms on V are equivalent.*

PROOF:

(1)1. PICK a basis $\{e_1, \dots, e_n\}$ for V

(1)2. LET: $\| \cdot \|_0 : V \rightarrow \mathbb{R}$ be the function

$$\|\alpha_1 e_1 + \dots + \alpha_n e_n\|_0 = |\alpha_1| + \dots + |\alpha_n| .$$

(1)3. $\| \cdot \|_0$ is a norm.

⟨2⟩1. $\forall x \in V. \|x\|_0 = 0 \Rightarrow x = 0$

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

⟨2⟩2. $\forall \lambda \in K. \forall x \in V. \|\lambda x\| = |\lambda| \|x\|$

PROOF:

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

⟨2⟩3. The triangle inequality holds.

PROOF:

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

⟨1⟩4. LET: $\| \cdot \|$ be any norm on V .

PROVE: $\| \cdot \|$ is equivalent to $\| \cdot \|_0$.

⟨1⟩5. For all $\alpha_1, \dots, \alpha_n \in K$,

$$\|\alpha_1 e_1 + \cdots + \alpha_n e_n\| \leq \max(\|e_1\|, \dots, \|e_n\|)(|\alpha_1| + \cdots + |\alpha_n|)$$

⟨2⟩1. LET: $\alpha_1, \dots, \alpha_n \in K$

⟨2⟩2. $\|\alpha_1 e_1 + \cdots + \alpha_n e_n\| \leq \max(\|e_1\|, \dots, \|e_n\|)(|\alpha_1| + \cdots + |\alpha_n|)$

PROOF:

$$\begin{aligned} \|\alpha_1 e_1 + \cdots + \alpha_n e_n\| &\leq |\alpha_1| \|e_1\| + \cdots + |\alpha_n| \|e_n\| \\ &\leq (|\alpha_1| + \cdots + |\alpha_n|) \max(\|e_1\|, \dots, \|e_n\|) \quad \square \end{aligned}$$

⟨1⟩6. LET: $\beta = \max(\|e_1\|, \dots, \|e_n\|)$

⟨1⟩7. For all $x \in V$,

$$\|x\| \leq \beta \|x\|_0 .$$

⟨1⟩8. There exists $\alpha > 0$ such that, for all $x \in V$,

$$\alpha \|x\|_0 \leq \|x\| .$$

PROOF: Proposition 21.4.19.

□

Definition 21.4.21 (Closed Ball). Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector space over K . Let $x \in V$ and let r be a positive real number. The *closed ball* with *centre* x and *radius* r is

$$\overline{B(x, r)} := \{y \in V \mid \|x - y\| \leq r\} .$$

Definition 21.4.22 (Sphere). Let K be either \mathbb{R} or \mathbb{C} . Let V be a vector space over K . Let $x \in V$ and let r be a positive real number. The *sphere* with *centre* x and *radius* r is

$$S(x, r) := \{y \in V \mid \|x - y\| = r\} .$$

Proposition 21.4.23. *Every closed ball is closed.*

Proposition 21.4.24. *Every sphere is closed.*

Proposition 21.4.25. *The union of two closed sets is closed.*

Proposition 21.4.26. *The intersection of a nonempty set of closed sets is closed.*

Proposition 21.4.27. *In a normed space V , both \emptyset and V are closed.*

Proposition 21.4.28. *Let V be a normed space and $C \subseteq V$. Then C is closed iff, for every sequence (x_n) in C and $l \in V$, if $x_n \rightarrow l$ then $l \in C$.*

PROOF:

$\langle 1 \rangle 1$. If C is closed then, for every sequence (x_n) in C and $l \in V$, if $x_n \rightarrow l$ then $l \in C$.

$\langle 2 \rangle 1$. ASSUME: C is closed.

$\langle 2 \rangle 2$. LET: (x_n) be a sequence in C .

$\langle 2 \rangle 3$. LET: $l \in V$

$\langle 2 \rangle 4$. ASSUME: $x_n \rightarrow l$ as $n \rightarrow \infty$

$\langle 2 \rangle 5$. ASSUME: for a contradiction $l \notin C$

$\langle 2 \rangle 6$. PICK $\epsilon > 0$ such that $B(l, \epsilon) \subseteq V - C$

$\langle 2 \rangle 7$. PICK N such that $\forall n \geq N, \|x_n - l\| < \epsilon$

$\langle 2 \rangle 8$. $x_N \in C$

$\langle 2 \rangle 9$. $\|x_N - l\| < \epsilon$

$\langle 2 \rangle 10$. Q.E.D.

PROOF: This is a contradiction.

$\langle 1 \rangle 2$. If, for every sequence (x_n) in C and $l \in V$, if $x_n \rightarrow l$ then $l \in C$, then C is closed.

$\langle 2 \rangle 1$. ASSUME: for every sequence (x_n) in C and $l \in V$, if $x_n \rightarrow l$ then $l \in C$.

$\langle 2 \rangle 2$. LET: $x \in V - C$

$\langle 2 \rangle 3$. ASSUME: for a contradiction there is no $\epsilon > 0$ such that $B(x, \epsilon) \subseteq V - C$

$\langle 2 \rangle 4$. For $n \in \mathbb{Z}^+$, PICK $x_n \in B(x, \epsilon) \cap C$

$\langle 2 \rangle 5$. $x_n \rightarrow x$ as $n \rightarrow \infty$

$\langle 2 \rangle 6$. Q.E.D.

PROOF: This is a contradiction.

□

Definition 21.4.29 (Closure). Let V be a normed space and $A \subseteq V$. The *closure* of A , $\text{cl } A$, is the intersection of all the closed sets that include A .

Theorem 21.4.30. *Let V be a normed space and $S \subseteq V$. Then the closure of S is the set of all limits of convergent sequences in S .*

PROOF:

$\langle 1 \rangle 1$. For all $l \in \text{cl } S$, there exists a sequence (x_n) that converges to l .

$\langle 2 \rangle 1$. LET: $l \in \text{cl } S$

$\langle 2 \rangle 2$. For $n \in \mathbb{N}$, PICK $x_n \in B(l, 1/(n+1)) \cap S$

$\langle 3 \rangle 1$. ASSUME: for a contradiction $B(l, 1/(n+1))$ does not intersect S .

$\langle 3 \rangle 2$. $V - B(l, 1/(n+1))$ is a closed set that includes S .

$\langle 3 \rangle 3$. $\text{cl } S \subseteq V - B(l, 1/(n+1))$

$\langle 3 \rangle 4.$ $l \notin B(l, 1/(n+1))$

$\langle 3 \rangle 5.$ Q.E.D.

PROOF: This is a contradiction.

$\langle 2 \rangle 3.$ $x_n \rightarrow l$

$\langle 1 \rangle 2.$ For every sequence (x_n) in S , if $x_n \rightarrow l$ then $l \in \text{cl } S$.

PROOF: Proposition 21.4.28.

□

Definition 21.4.31 (Dense). Let V be a normed space and $S \subseteq V$. Then S is *dense* iff $\text{cl } S = V$.

Proposition 21.4.32. In $\mathcal{C}([a, b])$, the set of polynomials is dense.

PROOF: By the Weierstrass Theorem. □

Proposition 21.4.33. For any real $p \geq 1$, the set of all sequences with only finitely many non-zero terms is dense in l^p .

PROOF:

$\langle 1 \rangle 1.$ LET: $p \geq 1$

$\langle 1 \rangle 2.$ LET: $(z_n) \in l^p$

$\langle 1 \rangle 3.$ LET: $\epsilon > 0$

$\langle 1 \rangle 4.$ PICK N such that $\forall n \geq N, |z_n| < \epsilon/2$

$\langle 1 \rangle 5.$ LET: (y_n) be the sequence with $y_n = z_n$ for $n < N$, and $y_n = 0$ for $n \geq N$

$\langle 1 \rangle 6.$ $\|(z_n) - (y_n)\| \leq \epsilon/2$

$\langle 1 \rangle 7.$ $\|(z_n) - (y_n)\| < \epsilon$

□

Theorem 21.4.34. Let V be a normed space. Let $S \subseteq V$. Then the following are equivalent:

1. S is dense.
2. For all $x \in V$, there exists a sequence (x_n) in S such that $x_n \rightarrow x$.
3. Every nonempty open subset of V intersects S .

PROOF:

$\langle 1 \rangle 1.$ $1 \Leftrightarrow 2$

PROOF: Theorem 21.4.30.

$\langle 1 \rangle 2.$ $1 \Leftrightarrow 3$

PROOF:

S is dense \Leftrightarrow the only closed set that includes S is V

\Leftrightarrow the only open set that does not intersect S is empty

□

Definition 21.4.35 (Compact). Let V be a normed space and $S \subseteq V$. Then S is *compact* if and only if every sequence in S has a subsequence that converges to a limit in S .

Proposition 21.4.36. *Every compact set is closed.*

PROOF:

- ⟨1⟩1. LET: V be a normed space.
- ⟨1⟩2. LET: $C \subseteq V$ be compact.
- ⟨1⟩3. LET: (x_n) be a sequence in C that converges to $l \in V$.
- ⟨1⟩4. PICK a subsequence (y_n) of (x_n) that converges to $m \in C$.
- ⟨1⟩5. $l = m$
- ⟨1⟩6. $l \in C$
- ⟨1⟩7. Q.E.D.

PROOF: Proposition 21.4.28.

□

Definition 21.4.37 (Bounded). Let V be a normed space and $S \subseteq V$. Then S is *bounded* iff there exists $r > 0$ such that $S \subseteq B(0, r)$.

Proposition 21.4.38. *In \mathbb{R}^n and \mathbb{C}^n , the compact sets are the closed bounded sets.*

PROOF:

- ⟨1⟩1. LET: $C \subseteq K^n$
- ⟨1⟩2. If C is compact then C is closed.
- PROOF: Proposition 21.4.36.
- ⟨1⟩3. If C is compact then C is bounded.
- ⟨2⟩1. ASSUME: C is compact.
- ⟨2⟩2. ASSUME: for a contradiction C is not bounded.
- ⟨2⟩3. For $n \in \mathbb{N}$, PICK $x_n \in C$ with $\|x_n\| > n + 1$.
- ⟨2⟩4. PICK a convergent subsequence (x_{n_r}) that converges to $l \in C$
- ⟨2⟩5. $\|x_{n_r}\| \rightarrow \|l\|$
- ⟨2⟩6. $\|x_{n_r}\| \rightarrow +\infty$
- ⟨2⟩7. Q.E.D.

PROOF: This is a contradiction.

- ⟨1⟩4. If C is closed and bounded then C is compact.

PROOF: By the Bolzano-Weierstrass Theorem.

□

Proposition 21.4.39. *Let V be a normed space and $S \subseteq V$. Then S is bounded if and only if, for every sequence (x_n) in S and every sequence (λ_n) in K , if $\lambda_n \rightarrow 0$ then $\|\lambda_n x_n\| \rightarrow 0$.*

PROOF:

- ⟨1⟩1. If S is bounded then, for every sequence (x_n) in S and every sequence (λ_n) in K , if $\lambda_n \rightarrow 0$ then $\|\lambda_n x_n\| \rightarrow 0$.
- ⟨2⟩1. ASSUME: S is bounded.
- ⟨2⟩2. PICK $r > 0$ such that $S \subseteq B(0, r)$.
- ⟨2⟩3. LET: (x_n) be a sequence in S .
- ⟨2⟩4. LET: (λ_n) be a sequence in K .
- ⟨2⟩5. ASSUME: $\lambda_n \rightarrow 0$

- ⟨2⟩6. LET: $\epsilon > 0$
- ⟨2⟩7. PICK N such that $\forall n \geq N, |\lambda_n| < \epsilon/r$
- ⟨2⟩8. $\forall n \geq N, \|\lambda_n x_n\| < \epsilon$
- ⟨1⟩2. If S is unbounded then there exists a sequence (x_n) in S and (λ_n) in K such that $\lambda_n \rightarrow 0$ and $\|\lambda_n x_n\| \not\rightarrow 0$.
- ⟨2⟩1. S is unbounded.
- ⟨2⟩2. For $n \in \mathbb{N}$, PICK $x_n \in S$ such that $\|x_n\| > n$.
- ⟨2⟩3. For $n \in \mathbb{N}$,
LET: $\lambda_n = 1/n$ if $n > 0$, 1 if $n = 0$
- ⟨2⟩4. $\lambda_n \rightarrow 0$
- ⟨2⟩5. $\|\lambda_n x_n\| > 1$ for all $n > 1$

□

Proposition 21.4.40. *In $\mathcal{C}([0, 1])$, the unit ball $\overline{B(0, 1)}$ is closed and bounded but not compact.*

PROOF:

- ⟨1⟩1. $\overline{B(0, 1)}$ is closed.
PROOF: Proposition 21.4.23.
- ⟨1⟩2. $\overline{B(0, 1)}$ is bounded.
PROOF: $\overline{B(0, 1)} \subseteq B(0, 2)$.
- ⟨1⟩3. $\overline{B(0, 1)}$ is not compact.
- ⟨2⟩1. For $n \in \mathbb{N}$,
LET: $x_n : [0, 1] \rightarrow \mathbb{R}$ be the function $x_n(t) = t^n$.
- ⟨2⟩2. For $n \in \mathbb{N}$, we have $x_n \in \overline{B(0, 1)}$.
- ⟨2⟩3. No subsequence of (x_n) converges.

□

Theorem 21.4.41 (Riesz's Lemma). *Let X be a closed proper subspace of a normed space V . For every $\epsilon \in (0, 1)$, there exists $x_\epsilon \in V$ such that $\|x_\epsilon\| = 1$ and $\forall x \in X, \|x_\epsilon - x\| \geq \epsilon$.*

PROOF:

- ⟨1⟩1. PICK $z \in E - X$
- ⟨1⟩2. LET: $d = \inf_{x \in X} \|z - x\|$
- ⟨1⟩3. $d > 0$
 - ⟨2⟩1. PICK- $\epsilon > 0$ such that $B(z, \epsilon) \subseteq E - X$
 - ⟨2⟩2. $d \geq \epsilon$
- ⟨1⟩4. For all $\epsilon \in (0, 1)$, choose $y_\epsilon \in X$ such that

$$d \leq \|z - y_\epsilon\| < d/\epsilon .$$
- ⟨1⟩5. For $\epsilon \in (0, 1)$,
LET:

$$x_\epsilon = \frac{z - y_\epsilon}{\|z - y_\epsilon\|} .$$

- ⟨1⟩6. For all $x \in X$ we have $\|x_\epsilon - x\| > \epsilon$

PROOF:

$$\begin{aligned}
 \|x_\epsilon - x\| &= \left\| \frac{z - y_\epsilon}{\|z - y_\epsilon\|} - x \right\| \\
 &= \frac{1}{\|z - y_\epsilon\|} \|z - y_\epsilon - \|z - y_\epsilon\|x\| \quad (y_\epsilon + \|z - y_\epsilon\|x \in X) \\
 &\geq \frac{1}{\|z - y_\epsilon\|} d \\
 &> \epsilon
 \end{aligned}$$

□

Theorem 21.4.42. *Let V be a normed space. 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 $\{e_1, \dots, e_n\}$.

⟨2⟩3. ASSUME: w.l.o.g. $\forall \alpha_1, \dots, \alpha_n \in K, \|\alpha_1 e_1 + \dots + \alpha_n e_n\| = |\alpha_1| + \dots + |\alpha_n|$

⟨2⟩4. LET: (x_m) be a sequence in $\overline{B(0,1)}$

⟨2⟩5. For $m \in \mathbb{N}$,

$$\text{LET: } x_m = \alpha_{m1}e_1 + \dots + \alpha_{mn}e_n$$

⟨2⟩6. For $m \in \mathbb{N}$ and $i = 1, \dots, n$, we have $|\alpha_{mi}| \leq 1$

⟨2⟩7. For $i = 1, \dots, n$, PICK a convergent subsequence $(\alpha_{m_r i})$ of (α_{mi}) in \mathbb{C} that converges to l_i

PROOF: Since $\overline{B(0,1)}$ is compact in K .

⟨2⟩8. x_m converges to $l_1 e_1 + \dots + l_n e_n$

PROOF:

$$\begin{aligned}
 \|x_m - l_1 e_1 - \dots - l_n e_n\| &= \|(\alpha_{m1} - l_1)e_1 + \dots + (\alpha_{mn} - l_n)e_n\| \\
 &= |\alpha_{m1} - l_1| + \dots + |\alpha_{mn} - l_n| \\
 &\rightarrow 0 \quad \text{as } m \rightarrow \infty
 \end{aligned}$$

⟨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) such that $\|x_n\| = 1$ and $\|x_m - x_n\| \geq 1/2$ for all $m \neq n$.

⟨3⟩1. ASSUME: as induction hypothesis there exists a sequence (x_0, x_1, \dots, x_n) such that $\|x_i\| = 1$ and $\|x_i - x_j\| \geq 1/2$ for $i \neq j$

⟨3⟩2. PICK x_{n+1} such that $\|x_{n+1}\| = 1$ and $\|x_{n+1} - x\| \geq 1/2$ for $x \in \{x_1, \dots, x_n\}$.

⟨2⟩3. ASSUME: for a contradiction (x_{n_r}) is a subsequence that converges to l

⟨2⟩4. For all r we have $1/2 \leq \|x_{n_r} - l\| + \|x_{n_{r+1}} - l\|$

PROOF:

$$\begin{aligned}
 1/2 &\leq \|x_{n_r} - x_{n_{r+1}}\| && (\langle 2 \rangle 2) \\
 &\leq \|x_{n_r} - l\| + \|x_{n_{r+1}} - l\| && (\text{Triangle Inequality})
 \end{aligned}$$

⟨2⟩5. Q.E.D.

PROOF: This is a contradiction.

□

Proposition 21.4.43. *Let U and V be normed spaces. Let $f : U \rightarrow V$. If f is continuous at one point, then it is continuous.*

PROOF:

- ⟨1⟩1. ASSUME: f is continuous at $x_0 \in U$.
- ⟨1⟩2. LET: (x_n) be a sequence in U that converges to $l \in U$.
- ⟨1⟩3. $x_n - l + x_0 \rightarrow x_0$ as $n \rightarrow \infty$
- ⟨1⟩4. $f(x_n - l + x_0) \rightarrow f(x_0)$ as $n \rightarrow \infty$
- ⟨1⟩5. $f(x_n) - f(l) + f(x_0) \rightarrow f(x_0)$ as $n \rightarrow \infty$
- ⟨1⟩6. $f(x_n) \rightarrow f(l)$ as $n \rightarrow \infty$.

□

Definition 21.4.44 (Bounded). Let U and V be normed spaces and $L : U \rightarrow V$ be a linear transformation. Then L is *bounded* iff there exists $\alpha > 0$ such that $\forall x \in U, \|L(x)\| \leq \alpha\|x\|$.

Theorem 21.4.45. *Let U and V be normed spaces. Let $L : U \rightarrow V$ be a linear transformation. Then L is continuous if and only if it is bounded.*

PROOF:

- ⟨1⟩1. If L is continuous then L is bounded.
 - ⟨2⟩1. ASSUME: L is not bounded.
 - ⟨2⟩2. For $n \in \mathbb{N}$, choose $x_n \in U$ such that $\|L(x_n)\| > (n+1)\|x_n\|$
 - ⟨2⟩3. For $n \in \mathbb{N}$,
LET: $y_n = x_n/(n+1)\|x_n\|$
 - ⟨2⟩4. $y_n \rightarrow 0$ as $n \rightarrow \infty$
 - ⟨2⟩5. For $n \in \mathbb{N}$, we have $\|L(y_n)\| > 1$
 - ⟨2⟩6. $L(y_n) \not\rightarrow 0 = L(0)$ as $n \rightarrow \infty$
 - ⟨2⟩7. L is not continuous.
- ⟨1⟩2. If L is bounded then L is continuous.
 - ⟨2⟩1. LET: $\alpha > 0$ be such that $\forall x \in U, \|L(x)\| \leq \alpha\|x\|$
PROVE: L is continuous at 0.
 - ⟨2⟩2. LET: (x_n) be a sequence in U that converges to 0.
 - ⟨2⟩3. $L(x_n) \rightarrow 0$ as $n \rightarrow \infty$
 - ⟨2⟩4. Q.E.D.

PROOF: Proposition 21.4.43.

□

□

Corollary 21.4.45.1. *If U and V are finite dimensional normed spaces, then every linear transformation $U \rightarrow V$ is continuous.*

Definition 21.4.46. For U and V normed spaces, let $\mathcal{B}(U, V)$ be the space of all bounded linear transformations $U \rightarrow V$. This is a subspace of the space of all linear transformations $U \rightarrow V$.

Define the *uniform convergence norm* on $\mathcal{B}(U, V)$ by

$$\|L\| = \sup\{\|L(x)\| \mid x \in U, \|x\| = 1\} .$$

We prove this is a norm.

PROOF:

$\langle 1 \rangle 1.$ $\forall L \in \mathcal{B}(U, V). \|L\| = 0 \Rightarrow L = 0$

$\langle 2 \rangle 1.$ LET: $L \in \mathcal{B}(U, V)$

$\langle 2 \rangle 2.$ ASSUME: $\|L\| = 0$

$\langle 2 \rangle 3.$ For all $x \in U$, if $\|x\| = 1$ then $\|L(x)\| = 0$

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

PROVE: $L(x) = 0$

$\langle 2 \rangle 5.$ ASSUME: w.l.o.g. $x \neq 0$

$\langle 2 \rangle 6.$ $\|L(x/\|x\|)\| = 0$

PROOF: $\langle 2 \rangle 3$

$\langle 2 \rangle 7.$ $L(x/\|x\|) = 0$

$\langle 2 \rangle 8.$ $L(x)/\|x\| = 0$

$\langle 2 \rangle 9.$ $L(x) = 0$

$\langle 1 \rangle 2.$ $\forall \lambda \in K. \forall L \in \mathcal{B}(U, V). \|\lambda L\| = |\lambda| \|L\|$

$\langle 2 \rangle 1.$ LET: $\lambda \in K$

$\langle 2 \rangle 2.$ LET: $L \in \mathcal{B}(U, V)$

$\langle 2 \rangle 3.$ $\|\lambda L\| = |\lambda| \|L\|$

PROOF:

$$\begin{aligned} \|\lambda L\| &= \sup_{\|x\|=1} \|\lambda L(x)\| \\ &= \sup_{\|x\|=1} (|\lambda| \|L(x)\|) \\ &= |\lambda| \sup_{\|x\|=1} \|L(x)\| \\ &= |\lambda| \|L\| \end{aligned}$$

$\langle 1 \rangle 3.$ The triangle inequality holds.

$\langle 2 \rangle 1.$ LET: $L, M \in \mathcal{B}(U, V)$

$\langle 2 \rangle 2.$ For all $x \in U$, if $\|x\| = 1$ then

$$\|L(x) + M(x)\| \leq \|L(x)\| + \|M(x)\| .$$

$\langle 2 \rangle 3.$ For all $x \in U$, if $\|x\| = 1$ then

$$\|L(x) + M(x)\| \leq \|L\| + \|M\| .$$

$\langle 2 \rangle 4.$ $\|L + M\| \leq \|L\| + \|M\|$

□

Proposition 21.4.47. Let U and V be normed spaces and $L \in \mathcal{B}(U, V)$. Then $\|L\|$ is the least number such that $\forall x \in U. \|L(x)\| \leq \|L\| \|x\|$.

Theorem 21.4.48. Let U and V be normed spaces. Let $T : U \rightarrow V$ be a continuous linear transformation. Then the null space $\mathcal{N}(T)$ is closed in U .

PROOF: If (x_n) is a sequence in $\mathcal{N}(T)$ and $x_n \rightarrow l$ then $T(l) = \lim_{n \rightarrow \infty} T(x_n) = 0$ so $l \in \mathcal{N}(T)$. □

Theorem 21.4.49 (Diagonal Theorem). Let V be a normed space. Let $(x_{ij})_{i,j \in \mathbb{N}}$ be an infinite matrix in V . If:

1. $\forall j \in \mathbb{N}. x_{ij} \rightarrow 0$ as $i \rightarrow \infty$;
2. Every strictly increasing sequence of natural numbers (p_i) has a subsequence (q_i) such that

$$\sum_{j=0}^{\infty} x_{q_i q_j} \rightarrow 0 \text{ as } i \rightarrow \infty$$

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

PROOF:

- $\langle 1 \rangle 1$. LET: V be a normed space.
- $\langle 1 \rangle 2$. LET: $(x_{ij})_{i,j \in \mathbb{N}}$ be an infinite matrix in V .
- $\langle 1 \rangle 3$. ASSUME: $\forall j \in \mathbb{N}. x_{ij} \rightarrow 0$ as $i \rightarrow \infty$
- $\langle 1 \rangle 4$. ASSUME: Every strictly increasing sequence of natural numbers (p_i) has a subsequence (q_i) such that

$$\sum_{j=0}^{\infty} x_{q_i q_j} \rightarrow 0 \text{ as } i \rightarrow \infty$$
- $\langle 1 \rangle 5$. ASSUME: for a contradiction $x_{ii} \not\rightarrow 0$ as $i \rightarrow \infty$
- $\langle 1 \rangle 6$. PICK a strictly increasing sequence (p_i) and $\epsilon > 0$ such that $\forall i \in \mathbb{N}. \|x_{p_i p_i}\| \geq \epsilon$
 - $\langle 2 \rangle 1$. PICK $\epsilon > 0$ such that, for all N , there exists $n \geq N$ such that $\|x_{ii}\| \geq \epsilon$
 - $\langle 2 \rangle 2$. Choose a sequence (p_i) such that, for all i , we have $p_{i+1} \geq p_i + 1$ and $\|x_{p_i p_i}\| \geq \epsilon$
- $\langle 1 \rangle 7$. PICK a subsequence (q_i) of (p_i) such that $\sum_{j=0}^{\infty} x_{q_i q_j} \rightarrow 0$ as $i \rightarrow \infty$.

PROOF: $\langle 1 \rangle 4$
- $\langle 1 \rangle 8$. For all i we have $x_{q_i q_j} \rightarrow 0$ as $j \rightarrow \infty$.

PROOF: Since $\sum_{j=0}^{\infty} x_{q_i q_j} < \infty$.
- $\langle 1 \rangle 9$. For all j we have $x_{q_i q_j} \rightarrow 0$ as $i \rightarrow \infty$.

PROOF: $\langle 1 \rangle 3$
- $\langle 1 \rangle 10$. PICK a subsequence (r_i) of (q_i) such that, for all i, j with $i \neq j$, we have $\|x_{r_i r_j}\| < \epsilon/2^{j+2}$.
 - $\langle 2 \rangle 1$. LET: $r_1 = q_1$
 - $\langle 2 \rangle 2$. ASSUME: as induction hypothesis we have defined (r_1, \dots, r_n) such that:
 - $r_1 < r_2 < \dots < r_n$
 - Whenever $q_i > r_j$ then $\|x_{q_i r_j}\| < \epsilon/2^{j+2}$
 - Whenever $i < j$ then $\|x_{r_i r_j}\| < \epsilon/2^{j+2}$
 - $\langle 2 \rangle 3$. LET: r_{n+1} be the first element of (q_i) such that $r_{n+1} > r_n$, $\|x_{q_i r_{n+1}}\| < \epsilon/2^{n+2}$ whenever $q_i \geq r_{n+1}$, and $\|x_{r_j r_{n+1}}\| < \epsilon/2^{n+3}$ for $j = 1, \dots, n$.

PROOF: One exists by $\langle 1 \rangle 8$.
- $\langle 2 \rangle 4$. $r_1 < \dots < r_n < r_{n+1}$
- $\langle 2 \rangle 5$. Whenever $q_i > r_j$ then $\|x_{q_i r_j}\| < \epsilon/2^{j+2}$
- $\langle 2 \rangle 6$. Whenever $i < j$ then $\|x_{r_i r_j}\| < \epsilon/2^{j+2}$
- $\langle 1 \rangle 11$. PICK a subsequence (s_i) of (r_i) such that $\sum_{j=0}^{\infty} x_{s_i s_j} \rightarrow 0$ as $i \rightarrow \infty$

PROOF: $\langle 1 \rangle 4$

$$\langle 1 \rangle 12. \forall i \in \mathbb{N}. \left\| \sum_{j=0}^{\infty} x_{s_i s_j} \right\| > \epsilon/2$$

PROOF:

$$\begin{aligned} \left\| \sum_{j=0}^{\infty} x_{s_i s_j} \right\| &= \left\| x_{s_i s_i} + \sum_{j \neq i} x_{s_i s_j} \right\| \\ &\geq \left\| x_{s_i s_i} \right\| - \left\| \sum_{j \neq i} x_{s_i s_j} \right\| && \text{(Proposition 21.4.5)} \\ &= \left\| x_{s_i s_i} \right\| - \left\| \sum_{j \neq i} x_{s_i s_j} \right\| && \left(\left\| x_{s_i s_i} \right\| > \epsilon, \left\| \sum_j x_{s_i s_j} \right\| \leq \epsilon/2 \right) \\ &\geq \left\| x_{s_i s_i} \right\| - \sum_{j \neq i} \|x_{s_i s_j}\| && \text{(Triangle Inequality,)} \\ &> \epsilon - \sum_{j \neq i} \epsilon/2^{j+2} && (\langle 1 \rangle 6, \langle 1 \rangle 10) \\ &> \epsilon/2 \end{aligned}$$

$\langle 1 \rangle 13$. Q.E.D.

PROOF: This contradicts $\langle 1 \rangle 11$.

□

21.4.1 Functionals

Definition 21.4.50 (Functional). Let K be either \mathbb{R} or \mathbb{C} . Let V be a normed space over K . A *functional* over V is a bounded linear transformation $V \rightarrow K$. The *dual space* of V is

$$V' := \mathcal{B}(V, K) .$$

21.4.2 Contraction Mappings

Definition 21.4.51 (Contraction). Let V be a normed space and $A \subseteq V$. Let $f : A \rightarrow V$. Then f is a *contraction* iff there exists a real number α with $0 < \alpha < 1$ such that, for all $x, y \in A$, we have

$$\|f(x) - f(y)\| \leq \alpha \|x - y\| .$$

Proposition 21.4.52. *Every contraction mapping is continuous.*

21.5 Banach Spaces

Definition 21.5.1 (Cauchy Sequence). A sequence (x_n) in a normed space is a *Cauchy sequence* iff, for every $\epsilon > 0$, there exists N such that $\forall m, n \geq N. \|x_m - x_n\| < \epsilon$.

Theorem 21.5.2. *Let V be a normed space. Let (x_n) be a sequence in V . Then the following are equivalent.*

1. (x_n) is Cauchy.
2. For every pair of strictly increasing sequences of natural numbers (p_n) and (q_n) , we have $\|x_{p_n} - x_{q_n}\| \rightarrow 0$ as $n \rightarrow \infty$.
3. For every strictly increasing sequence of natural numbers (p_n) , we have $\|x_{p_{n+1}} - x_{p_n}\| \rightarrow 0$ as $n \rightarrow \infty$.

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) be a pair of increasing sequences of natural numbers.
- $\langle 2 \rangle 3.$ LET: $\epsilon > 0$
- $\langle 2 \rangle 4.$ PICK N such that $\forall m, n \geq N. \|x_m - x_n\| < \epsilon$
- $\langle 2 \rangle 5.$ $\forall n \geq N. p_n, q_n \geq N$
- $\langle 2 \rangle 6.$ $\forall n \geq N. \|x_{p_n} - x_{q_n}\| < \epsilon$

$\langle 1 \rangle 2. 2 \Rightarrow 3$

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 all N , there exist $m, n \geq N$ such that $\|x_m - x_n\| \geq \epsilon$
- $\langle 2 \rangle 3.$ PICK strictly increasing sequences of natural numbers (p_n) and (q_n) such that, for all n , $\|x_{p_n} - x_{q_n}\| \geq \epsilon$
- $\langle 3 \rangle 1.$ ASSUME: as induction hypothesis we have chosen (p_1, \dots, p_n) and (q_1, \dots, q_n) strictly increasing such that $\forall i. \|x_{p_i} - x_{q_i}\| \geq \epsilon$
- $\langle 3 \rangle 2.$ PICK $p_{n+1}, q_{n+1} \geq \max(p_n, q_n)$ such that $\|x_{p_{n+1}} - x_{q_{n+1}}\| \geq \epsilon$
- $\langle 2 \rangle 4.$ 2 is false.

$\langle 1 \rangle 4. 3 \Rightarrow 2$

- $\langle 2 \rangle 1.$ ASSUME: (p_n) and (q_n) are strictly increasing sequences such that $\|x_{p_n} - x_{q_n}\| \not\rightarrow 0$ as $n \rightarrow \infty$.
- $\langle 2 \rangle 2.$ PICK $\epsilon > 0$ such that, for all N , there exists $n \geq N$ such that $\|x_{p_n} - x_{q_n}\| \geq \epsilon$
- $\langle 2 \rangle 3.$ Choose a strictly increasing sequence (r_n) such that, for all n , we have $\|x_{r_{2n}} - x_{r_{2n+1}}\| \geq \epsilon$
- $\langle 3 \rangle 1.$ ASSUME: as induction hypothesis we have chosen $(r_0, r_1, \dots, r_{2n+1})$ such that, for $i = 0, 1, \dots, n$, we have $\|x_{r_{2i}} - x_{r_{2i+1}}\| \geq \epsilon$
- $\langle 3 \rangle 2.$ PICK $i, j \geq r_{2n+1}$ such that $\|x_i - x_j\| \geq \epsilon$
- $\langle 3 \rangle 3.$ Set $r_{2n+2} = \min(i, j)$ and $r_{2n+3} = \max(i, j)$
- $\langle 2 \rangle 4.$ 3 is false.

□

Proposition 21.5.3. *Every convergent sequence is a Cauchy sequence.*

PROOF:

- ⟨1⟩1. LET: (x_n) be a convergent sequence in a normed space V with limit l .
 ⟨1⟩2. LET: $\epsilon > 0$
 ⟨1⟩3. PICK N such that $\forall n \geq N. \|x_n - l\| < \epsilon/2$
 ⟨1⟩4. $\forall m, n \geq N. \|x_m - x_n\| < \epsilon$
 \square

Proposition 21.5.4. *Let $\mathcal{P}([0, 1])$ be the space of polynomials on $[0, 1]$ under the norm of uniform convergence. For $n \in \mathbb{N}$, let $P_n = 1 + x + x^2/2! + \cdots + x^n/n!$. Then (P_n) is Cauchy but does not converge, since e^x is not a polynomial.*

PROOF: Easy. \square

Proposition 21.5.5. *If (x_n) is a Cauchy sequence in a normed space 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 21.4.5.

- ⟨1⟩2. Q.E.D.

PROOF: Since \mathbb{R} is complete.

\square

Corollary 21.5.5.1. *Every Cauchy sequence is bounded.*

Definition 21.5.6 (Banach space). A normed space is *complete* or a *Banach space* iff every Cauchy sequence converges.

Proposition 21.5.7. *For all $p \geq 1$, the space l^p is complete.*

PROOF:

- ⟨1⟩1. LET: (a_n) be a Cauchy sequence in l^p .
 ⟨1⟩2. For $n \in \mathbb{N}$,
 LET: $a_n = (\alpha_{n0}, \alpha_{n1}, \dots)$
 ⟨1⟩3. For all $\epsilon > 0$, there exists N such that $\forall m, n \geq N$

$$\sum_{k=0}^{\infty} |\alpha_{mk} - \alpha_{nk}|^p < \epsilon .$$

PROOF: ⟨1⟩1

- ⟨1⟩4. For all $k \in \mathbb{N}$ and $\epsilon > 0$, there exists N such that $\forall m, n \geq N$
 $|\alpha_{mk} - \alpha_{nk}| < \epsilon .$

PROOF: ⟨1⟩3

- ⟨1⟩5. For all $k \in \mathbb{N}$, the sequence $(\alpha_{nk})_n$ converges in \mathbb{C} .

PROOF: \mathbb{C} is complete.

- ⟨1⟩6. For $k \in \mathbb{N}$,

LET:

$$\alpha_k = \lim_{n \rightarrow \infty} \alpha_{nk} .$$

⟨1⟩7. LET: $a = (\alpha_k)_k$

⟨1⟩8. For all $\epsilon > 0$, there exists N such that $\forall n \geq N$

$$\sum_{k=0}^{\infty} |\alpha_k - \alpha_{nk}|^p < \epsilon .$$

PROOF: Take the limit $m \rightarrow \infty$ in ⟨1⟩4.

⟨1⟩9. $a \in l^p$

⟨2⟩1. PICK N such that $\forall n \geq N, \sum_{k=0}^{\infty} |\alpha_k - \alpha_{nk}|^p < 1$

⟨2⟩2. $a - a_N \in l^p$

⟨2⟩3. Q.E.D.

PROOF: Since l^p is closed under $+$.

⟨1⟩10. $a_n \rightarrow a$ as $n \rightarrow \infty$.

PROOF: Immediate from ⟨1⟩8.

□

Proposition 21.5.8. *For any real number a, b with $a < b$, the space $\mathcal{C}([a, b])$ is complete.*

PROOF:

⟨1⟩1. LET: (f_n) be a Cauchy sequence in $\mathcal{C}([a, b])$

⟨1⟩2. For all $\epsilon > 0$, there exists N such that, for all $m, n \geq N$ and $x \in [a, b]$,

$$|f_m(x) - f_n(x)| < \epsilon .$$

⟨1⟩3. For all $x \in [a, b]$, $(f_n(x))_n$ is Cauchy.

⟨1⟩4. LET: $f : [a, b] \rightarrow \mathbb{C}$ be the function

$$f(x) = \lim_{n \rightarrow \infty} f_n(x) .$$

⟨1⟩5. For all $\epsilon > 0$, there exists N such that, for all $n \geq N$ and $x \in [a, b]$,

$$|f_n(x) - f(x)| < \epsilon .$$

PROOF: Take the limit $m \rightarrow \infty$ in ⟨1⟩2.

⟨1⟩6. f is continuous.

⟨2⟩1. LET: $x_0 \in [a, b]$

⟨2⟩2. LET: $\epsilon > 0$

⟨2⟩3. PICK N such that, for all $n \geq N$ and $y \in [a, b]$, we have

$$|f_n(y) - f(y)| < \epsilon/3 .$$

PROOF: ⟨1⟩5

⟨2⟩4. PICK $\delta > 0$ such that, for all $y \in [a, b]$ with $|x_0 - y| < \delta$, we have

$$|f_N(x_0) - f_N(y)| < \epsilon/3$$

⟨2⟩5. For all $y \in [a, b]$, if $|x_0 - y| < \delta$ then $|f(x_0) - f(y)| < \epsilon$

PROOF:

$$|f(x_0) - f(y)|$$

$$\leq |f(x_0) - f_N(x_0)| + |f_N(x_0) - f_N(y)| + |f_N(y) - f(y)| \quad (\text{Triangle Inequality})$$

$$< \epsilon/3 + \epsilon/3 + \epsilon/3 \quad (\langle 2 \rangle 3, \langle 2 \rangle 4)$$

$$= \epsilon$$

⟨1⟩7. $f_n \rightarrow f$ as $n \rightarrow \infty$.

PROOF: Immediate from ⟨1⟩5.

□

Definition 21.5.9 (Convergent Series). Let (x_n) be a sequence in a normed space V . We say the series $\sum_{n=0}^{\infty} x_n$ is *convergent* iff the sequence $(\sum_{n=0}^N x_n)_N$ is convergent, and then we write $\sum_{n=0}^{\infty} x_n = l$ for $\lim_{N \rightarrow \infty} \sum_{n=0}^N x_n = l$.

Definition 21.5.10 (Absolutely Convergent Series). Let (x_n) be a sequence in a normed space V . We say the series $\sum_{n=0}^{\infty} x_n$ is *absolutely convergent* iff the series $\sum_{n=0}^{\infty} \|x_n\|$ converges in \mathbb{R} .

Theorem 21.5.11. *A normed space is complete if and only if every absolutely convergent series is convergent.*

PROOF:

$\langle 1 \rangle 1$. LET: V be a normed space.

$\langle 1 \rangle 2$. If V is complete then every absolutely convergent series is convergent.

$\langle 2 \rangle 1$. ASSUME: V is complete.

$\langle 2 \rangle 2$. LET: (x_n) be a sequence in V .

$\langle 2 \rangle 3$. ASSUME: $\sum_{n=0}^{\infty} \|x_n\|$ converges.

PROVE: $(\sum_{n=0}^N x_n)_N$ is Cauchy.

$\langle 2 \rangle 4$. LET: $\epsilon > 0$

$\langle 2 \rangle 5$. PICK N such that $\sum_{n=N}^{\infty} \|x_n\| < \epsilon$

$\langle 2 \rangle 6$. LET: $m > n \geq N$

$\langle 2 \rangle 7$. $\|\sum_{k=0}^m x_k - \sum_{k=0}^n x_k\| < \epsilon$

PROOF:

$$\begin{aligned} \left\| \sum_{k=0}^m x_k - \sum_{k=0}^n x_k \right\| &= \left\| \sum_{k=n+1}^m x_k \right\| \\ &\leq \sum_{k=n+1}^m \|x_k\| \\ &\leq \sum_{k=n+1}^{\infty} \|x_k\| \\ &< \epsilon \end{aligned}$$

$\langle 1 \rangle 3$. If every absolutely convergent series is convergent then V is complete.

$\langle 2 \rangle 1$. ASSUME: Every absolutely convergent series is convergent.

$\langle 2 \rangle 2$. LET: (x_n) be a Cauchy sequence in V .

$\langle 2 \rangle 3$. Choose an increasing sequence of natural numbers (p_k) such that, for all $m, n \geq p_k$, we have

$$\|x_m - x_n\| < 2^{-k}.$$

$\langle 2 \rangle 4$. $\sum_{k=0}^{\infty} \|x_{p_{k+1}} - x_{p_k}\|$ is absolutely convergent.

$\langle 2 \rangle 5$. $\sum_{k=0}^{\infty} \|x_{p_{k+1}} - x_{p_k}\|$ is convergent.

$\langle 2 \rangle 6$. (x_{p_k}) converges.

$\langle 2 \rangle 7$. LET: $l = \lim_{k \rightarrow \infty} x_{p_k}$

$\langle 2 \rangle 8$. $x_n \rightarrow l$ as $n \rightarrow \infty$.

PROOF:

$$\begin{aligned} \|x_n - l\| &\leq \|x_n - x_{p_n}\| + \|x_{p_n} - l\| \\ &\rightarrow 0 \quad \text{as } n \rightarrow \infty \text{ (Theorem 21.5.2)} \end{aligned}$$

□

Proposition 21.5.12. *A closed subspace of a Banach space is a Banach space.*

PROOF:

- ⟨1⟩1. LET: V be a Banach space.
- ⟨1⟩2. LET: U be a closed subspace of V .
- ⟨1⟩3. LET: (x_n) be a Cauchy sequence in U .
- ⟨1⟩4. (x_n) is a Cauchy sequence in V .
- ⟨1⟩5. LET: l be the limit of (x_n) in V .
- ⟨1⟩6. $l \in U$

PROOF: Proposition 21.4.28.

□

Definition 21.5.13 (Completion). Let V be a normed space. A *completion* of V consists of a Banach space W and a function $\phi : V \rightarrow W$ such that:

- ϕ is injective.
- ϕ is a linear transformation.
- ϕ preserves the norm.
- $\phi(V)$ is dense in W .

Definition 21.5.14 (Equivalent Cauchy Sequences). Let V be a normed space. Let (x_n) and (y_n) be Cauchy sequences in V . Then (x_n) and (y_n) are *equivalent*, $(x_n) \sim (y_n)$, iff $\|x_n - y_n\| \rightarrow 0$ as $n \rightarrow \infty$.

Proposition 21.5.15. *Equivalence is an equivalence relation on the set of Cauchy sequences.*

Proposition 21.5.16. *If $(x_n) \sim (y_n)$ then $\lim_{n \rightarrow \infty} \|x_n\| = \lim_{n \rightarrow \infty} \|y_n\|$.*

Theorem 21.5.17. *Let V be a normed space. Let W be the quotient set of all Cauchy sequences modulo \sim . Define $+$, \cdot and $\| \cdot \|$ on W by*

$$\begin{aligned} [(x_n)] + [(y_n)] &= [(x_n + y_n)] \\ \lambda[(x_n)] &= [(\lambda x_n)] \\ \|[(x_n)]\| &= \lim_{n \rightarrow \infty} \|x_n\| \end{aligned}$$

Define $\phi : V \rightarrow W$ by $\phi(x)$ is the constant sequence (x) . Then $\phi : V \rightarrow W$ is the completion of V .

PROOF:

- ⟨1⟩1. $+$, \cdot and $\| \cdot \|$ are well defined.
- ⟨1⟩2. W is a normed space.
- ⟨1⟩3. $\phi(V)$ is dense in W .

PROOF: For any $[(x_n)] \in W$ we have $[(x_n)] = \lim_{n \rightarrow \infty} \phi(x_n)$.

- ⟨1⟩4. W is complete.

- (2)1. LET: (X_n) be a Cauchy sequence in W .
 (2)2. For all $n \in \mathbb{N}$, PICK $x_n \in V$ such that $\|\phi(x_n) - X_n\| < 1/n$
 PROOF: (1)3
 (2)3. For all m, n we have $\|x_n - x_m\| \leq \|X_n - X_m\| + 1/n + 1/m$
 PROOF:

$$\begin{aligned} \|x_n - x_m\| &= \|\phi(x_n) - \phi(x_m)\| \\ &\leq \|\phi(x_n) - X_n\| + \|X_n - X_m\| + \|\phi(x_m) - X_m\| \\ &\leq \|X_n - X_m\| + 1/n + 1/m \end{aligned}$$

 (2)4. (x_n) is a Cauchy sequence in V .
 (2)5. LET: $X = [(x_n)]$
 PROVE: $X_n \rightarrow X$ as $n \rightarrow \infty$
 (2)6. $\|X_n - X\| \rightarrow 0$ as $n \rightarrow \infty$
 PROOF:

$$\begin{aligned} \|X_n - X\| &\leq \|X_n - \phi(x_n)\| + \|\phi(x_n) - X\| \\ &< \| \phi(x_n) - X \| + 1/n \\ &\rightarrow 0 \end{aligned}$$

- (1)5. ϕ is injective.
 (1)6. ϕ is a linear transformation.
 (1)7. ϕ preserves the norm.
 \square

Theorem 21.5.18. *Let U be a normed space and V a Banach space. Then $\mathcal{B}(U, V)$ is a Banach space.*

PROOF:

- (1)1. LET: (L_n) be a Cauchy sequence in $\mathcal{B}(U, V)$
 (1)2. For all $x \in U$, we have $(L_n(x))$ is a Cauchy sequence in V .
 (2)1. LET: $x \in U$
 (2)2. ASSUME: w.l.o.g. $x \neq 0$
 (2)3. LET: $\epsilon > 0$
 (2)4. PICK N such that $\forall m, n \geq N. \|L_m - L_n\| < \epsilon/\|x\|$
 (2)5. $\forall m, n \geq N. \|L_m(x) - L_n(x)\| < \epsilon$
 PROOF: $\|L_m(x) - L_n(x)\| \leq \|L_m - L_n\| \|x\| < \epsilon$
 (1)3. Define $L : U \rightarrow V$ by $L(x) = \lim_{n \rightarrow \infty} L_n(x)$
 (1)4. $L \in \mathcal{B}(U, V)$
 (2)1. L is linear.
 (3)1. LET: $\lambda, \mu \in K$ and $x, y \in U$
 (3)2. $L(\lambda x + \mu y) = \lambda L(x) + \mu L(y)$
 PROOF:

$$\begin{aligned} L(\lambda x + \mu y) &= \lim_{n \rightarrow \infty} L_n(\lambda x + \mu y) \\ &= \lim_{n \rightarrow \infty} (\lambda L_n(x) + \mu L_n(y)) \\ &= \lambda L(x) + \mu L(y) \end{aligned}$$

 (2)2. L is bounded.
 (3)1. PICK N such that $\forall m, n \geq N. \|L_m - L_n\| < 1$

PROVE: $\forall x \in U. \|L(x)\| \leq (\|L_N\| + 1)\|x\|$
 (3)2. $\forall n \geq N. \|L_n\| \leq \|L_N\| + 1$
 PROOF: Since $|\|L_n\| - \|L_N\|| \leq \|L_n - L_N\| < 1$.
 (3)3. LET: $x \in U$
 (3)4. $\|L(x)\| \leq (\|L_N\| + 1)\|x\|$
 PROOF:

$$\begin{aligned} \|L(x)\| &= \left\| \lim_{n \rightarrow \infty} L_n(x) \right\| \\ &= \lim_{n \rightarrow \infty} \|L_n(x)\| \\ &\leq \lim_{n \rightarrow \infty} \|L_n\| \|x\| \\ &\leq (\|L_N\| + 1)\|x\| \end{aligned}$$

(1)5. $L_n \rightarrow L$ as $n \rightarrow \infty$
 (2)1. LET: $\epsilon > 0$
 (2)2. PICK N such that $\forall m, n \geq N. \|L_m - L_n\| < \epsilon/4$
 (2)3. LET: $n \geq N$
 (2)4. For all $x \in U$ we have $\|L_n(x) - L(x)\| < (\epsilon/2)\|x\|$
 (3)1. LET: $x \in U$
 (3)2. For all $m \geq N$ we have $\|L_n(x) - L_m(x)\| < (\epsilon/4)\|x\|$
 (3)3. $\|L_n(x) - L(x)\| \leq (\epsilon/4)\|x\|$
 PROOF: Taking the limit as $m \rightarrow \infty$.
 (2)5. $\|L_n - L\| \leq \epsilon/2$
 (2)6. $\|L_n - L\| < \epsilon$

□

Corollary 21.5.18.1. *The dual space of a normed space is a Banach space.*

Theorem 21.5.19. *Let U be a normed space and V a Banach space. Let W be a subspace of U . Let $L : W \rightarrow V$ be a bounded linear transformation. Then L has a unique extension to a bounded linear transformation $\overline{W} \rightarrow V$.*

PROOF:

(1)1. Define $L' : \overline{W} \rightarrow V$ as follows. Given $x \in \overline{W}$, pick a sequence (x_n) in W that converges to x . Then $L'(x) = \lim_{n \rightarrow \infty} L(x_n)$
 (2)1. For all $x \in \overline{W}$, there exists a sequence (x_n) in W that converges to x .
 PROOF: Theorem 21.4.30.
 (2)2. For any sequence (x_n) in W that converges in \overline{W} , we have $(L(x_n))$ converges in V .
 (3)1. LET: (x_n) be a sequence in W that converges in \overline{W}
 (3)2. (x_n) is Cauchy.
 (3)3. $(L(x_n))$ is Cauchy.
 PROOF: For any strictly increasing sequence of natural numbers (p_n) , we have $\|L(x_{p_{n+1}}) - L(x_{p_n})\| \leq \|L\| \|x_{p_{n+1}} - x_{p_n}\| \rightarrow 0$ as $n \rightarrow \infty$.
 (3)4. Q.E.D.
 PROOF: W is a Banach space.
 (2)3. If (x_n) and (y_n) are sequences in W that converge to the same point in \overline{W} , then $\lim_{n \rightarrow \infty} L(x_n) = \lim_{n \rightarrow \infty} L(y_n)$

PROOF: Since $\|L(x_n) - L(y_n)\| \leq \|L\|\|x_n - y_n\| \rightarrow 0$.

(1)2. L' extends L

PROOF: For $x \in W$ we have the constant sequence (x) converges to x , and the constant sequence $(L(x))$ converges to $L(x)$, so $L'(x) = L(x)$.

(1)3. L' is a linear transformation.

(2)1. LET: $\lambda, \mu \in K$ and $x, y \in \overline{W}$

(2)2. PICK sequences $(x_n), (y_n)$ in W that converge to x and y respectively.

(2)3. $\lambda x_n + \mu y_n \rightarrow \lambda x + \mu y$

(2)4. Q.E.D.

PROOF:

$$\begin{aligned} L'(\lambda x + \mu y) &= \lim_{n \rightarrow \infty} L(\lambda x_n + \mu y_n) \\ &= \lim_{n \rightarrow \infty} (\lambda L(x_n) + \mu L(y_n)) \\ &= \lambda L'(x) + \mu L'(y) \end{aligned}$$

(1)4. L' is bounded.

(2)1. LET: $x \in \overline{W}$

(2)2. PICK a sequence (x_n) in W that converges to x .

(2)3. $\|L'(x)\| \leq \|L\|\|x\|$

PROOF:

$$\begin{aligned} \|L'(x)\| &= \left\| \lim_{n \rightarrow \infty} L(x_n) \right\| \\ &= \lim_{n \rightarrow \infty} \|L(x_n)\| \\ &\leq \|L\| \lim_{n \rightarrow \infty} \|x_n\| \\ &= \|L\|\|x\| \end{aligned}$$

(1)5. If $L'' : \overline{W} \rightarrow V$ is a bounded linear transformation that extends L , then $L'' = L'$.

(2)1. LET: $x \in \overline{W}$

(2)2. PICK a sequence (x_n) in W that converges to x .

(2)3. $L''(x) = L'(x)$

PROOF:

$$\begin{aligned} L''(x) &= \lim_{n \rightarrow \infty} L''(x_n) \\ &= \lim_{n \rightarrow \infty} L(x_n) \\ &= L'(x_n) \end{aligned}$$

□

Theorem 21.5.20 (Banach-Steinhaus). *Let X be a Banach space and Y a normed space. Let \mathcal{T} be a set of bounded linear transformations from X into Y . Assume that, for all $x \in X$, there exists $M_x > 0$ such that, for all $T \in \mathcal{T}$, we have $\|T(x)\| \leq M_x$. Then there exists $M > 0$ such that, for all $T \in \mathcal{T}$, we have $\|T\| \leq M$.*

PROOF:

(1)1. LET: X be a Banach space.

(1)2. LET: Y be a normed space.

- ⟨1⟩3. LET: \mathcal{T} be a set of bounded linear transformations.
 ⟨1⟩4. ASSUME: For all $x \in X$, there exists $M_x > 0$ such that, for all $T \in \mathcal{T}$, we have $\|T(x)\| \leq M_x$.
 ⟨1⟩5. ASSUME: for a contradiction there is no $M > 0$ such that, for all $T \in \mathcal{T}$, we have $\|T\| \leq M$
 ⟨1⟩6. For every positive integer n , choose $T_n \in \mathcal{T}$ such that $\|T_n\| > n2^n$.
 ⟨1⟩7. For every positive integer n , choose $x_n \in U$ such that $\|x_n\| = 1$ and $\|T_n(x_n)\| > n2^n$.
 ⟨1⟩8. For every positive integer n we have

$$\left\| \frac{1}{n} T_n \left(\frac{x_n}{2^n} \right) \right\| > 1 .$$

- ⟨1⟩9. For positive integers i and j ,

LET:

$$y_{ij} = \frac{1}{i} T_i \left(\frac{x_j}{2^j} \right)$$

- ⟨1⟩10. LET: $z = \sum_{j=1}^{\infty} \frac{x_j}{2^j}$

- ⟨2⟩1. $\sum_{j=1}^{\infty} \frac{x_j}{2^j}$ is absolutely convergent.

PROOF:

$$\begin{aligned} \sum_{j=1}^{\infty} \left\| \frac{x_j}{2^j} \right\| &= \sum_{j=1}^{\infty} \frac{1}{2^j} & (\langle 1 \rangle 7) \\ &= 1 \end{aligned}$$

- ⟨2⟩2. Q.E.D.

PROOF: Theorem 21.5.11.

- ⟨1⟩11. PICK $C > 0$ such that, for all i , we have $\left\| \sum_{j=1}^{\infty} y_{ij} \right\| \leq C/i$.

- ⟨2⟩1. PICK $C > 0$ such that, for all $T \in \mathcal{T}$, we have $\|T(z)\| \leq C$.

PROOF: ⟨1⟩4.

- ⟨2⟩2. For all i we have $\left\| \sum_{j=1}^{\infty} y_{ij} \right\| \leq C/i$

PROOF:

$$\left\| \sum_{j=1}^{\infty} y_{ij} \right\| = \left\| \sum_{j=1}^{\infty} \frac{1}{i} T_i \left(\frac{x_j}{2^j} \right) \right\| \quad (\langle 1 \rangle 9)$$

$$= \frac{1}{i} \left\| T_i \left(\sum_{j=1}^{\infty} \frac{x_j}{2^j} \right) \right\| \quad (T_i \text{ continuous by } \langle 1 \rangle 3)$$

$$= \frac{1}{i} \|T_i(z)\| \quad (\langle 1 \rangle 10)$$

$$\leq \frac{C}{i} \quad (\langle 2 \rangle 1)$$

- ⟨1⟩12. $\sum_{j=1}^{\infty} y_{ij} \rightarrow 0$ as $i \rightarrow \infty$

- ⟨1⟩13. For any increasing sequence of positive integers (q_i) , we have $\sum_{j=0}^{\infty} y_{q_i q_j} \rightarrow 0$ as $i \rightarrow \infty$

PROOF: Similar.

- ⟨1⟩14. For all j we have $y_{ij} \rightarrow 0$ as $i \rightarrow \infty$

PROOF: From ⟨1⟩9 and the fact that T_i is continuous.

$\langle 1 \rangle 15.$ $y_{ii} \rightarrow 0$ as $i \rightarrow \infty$.

PROOF: By the Diagonal Theorem.

$\langle 1 \rangle 16.$ Q.E.D.

PROOF: This contradicts $\langle 1 \rangle 8$.

□

Theorem 21.5.21 (Banach Fixed Point Theorem). *Let V be a Banach space. Let $F \subseteq V$ be closed and nonempty. Let $f : F \rightarrow F$ be a contraction. 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 $\forall x, y \in V. \|f(x) - f(y)\| \leq \alpha \|x - y\|$.

$\langle 1 \rangle 2.$ PICK $x_0 \in F$

$\langle 1 \rangle 3.$ Extend to the sequence (x_n) in F by defining $x_{n+1} := f(x_n)$.

$\langle 1 \rangle 4.$ (x_n) is Cauchy.

$\langle 2 \rangle 1.$ $\forall n \in \mathbb{N}. \|x_{n+1} - x_n\| \leq \alpha^n \|x_1 - x_0\|$

$\langle 2 \rangle 2.$ LET: $\epsilon > 0$

$\langle 2 \rangle 3.$ PICK N such that $\frac{\|x_1 - x_0\|}{1 - \alpha} \alpha^N \leq \epsilon$

$\langle 2 \rangle 4.$ $\forall m, n \geq N. \|x_n - x_m\| < \epsilon$

$\langle 3 \rangle 1.$ LET: $m, n \geq N$

$\langle 3 \rangle 2.$ ASSUME: w.l.o.g. $m < n$

$\langle 3 \rangle 3.$ $\|x_n - x_m\| < \epsilon$

PROOF:

$$\begin{aligned} \|x_n - x_m\| &\leq \|x_n - x_{n-1}\| + \|x_{n-1} - x_{n-2}\| + \cdots + \|x_{m+1} - x_m\| \\ &\leq (\alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha^m) \|x_1 - x_0\| \\ &< \frac{\|x_1 - x_0\|}{1 - \alpha} \alpha^m \\ &\leq \frac{\|x_1 - x_0\|}{1 - \alpha} \alpha^N \\ &\leq \epsilon \end{aligned}$$

$\langle 1 \rangle 5.$ LET: $z = \lim_{n \rightarrow \infty} x_n$

$\langle 1 \rangle 6.$ z is unique such that $f(z) = z$.

$\langle 2 \rangle 1.$ $f(z) = z$

PROOF:

$$\begin{aligned} f(z) &= f\left(\lim_{n \rightarrow \infty} x_n\right) \\ &= \lim_{n \rightarrow \infty} f(x_n) \\ &= \lim_{n \rightarrow \infty} x_{n+1} \\ &= z \end{aligned}$$

$\langle 2 \rangle 2.$ If $f(w) = w$ then $w = z$.

$\langle 3 \rangle 1.$ $\|w - z\| \leq \alpha \|w - z\|$

PROOF: $\|w - z\| = \|f(w) - f(z)\| \leq \alpha \|w - z\|$

$\langle 3 \rangle 2.$ $\|w - z\| = 0$

PROOF: Otherwise $\|w - z\| < \|w - z\|$.

$\langle 3 \rangle 3.$ $w = z$

□

21.6 Inner Product Spaces

Definition 21.6.1 (Inner Product Space). An *inner product* on a complex vector space V is a function $\langle \cdot, \cdot \rangle : V^2 \rightarrow \mathbb{C}$ such that:

- $\forall x, y \in V. \langle x, y \rangle = \overline{\langle y, x \rangle}$
- $\forall \lambda \in \mathbb{C}. \forall x, y \in V. \langle \lambda x, y \rangle = \lambda \langle x, y \rangle$
- $\forall x, y, z \in V. \langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$
- $\forall x \in V. \langle x, x \rangle = 0 \Rightarrow x = 0$

An *inner product space* or *pre-Hilbert space* is a complex vector space with an inner product.

Proposition 21.6.2. \mathbb{C}^n is an inner product space under

$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle = x_1 \overline{y_1} + \dots + x_n \overline{y_n} .$$

Proposition 21.6.3. l^2 is an inner product under

$$\langle (x_n), (y_n) \rangle = \sum_{n=0}^{\infty} x_n \overline{y_n} .$$

PROOF:

$\langle 1 \rangle 1$. For all $(x_n), (y_n) \in l^2$ we have $\sum_n x_n \overline{y_n} < \infty$

$\langle 2 \rangle 1$. LET: $(x_n), (y_n) \in l^2$

$\langle 2 \rangle 2$. $\sum_{n=1}^N |x_n \overline{y_n}| \leq (\sum_{n=1}^{\infty} |x_n|^2)^{1/2} (\sum_{n=1}^{\infty} |y_n|^2)^{1/2}$

PROOF:

$$\begin{aligned} \sum_{n=1}^N |x_n \overline{y_n}| &= \sum_{n=1}^N |x_n| |y_n| \\ &\leq \left(\sum_{n=1}^N |x_n|^2 \right)^{1/2} \left(\sum_{n=1}^N |y_n|^2 \right)^{1/2} \quad (\text{Cauchy-Schwarz}) \\ &\leq \left(\sum_{n=1}^{\infty} |x_n|^2 \right)^{1/2} \left(\sum_{n=1}^{\infty} |y_n|^2 \right)^{1/2} \end{aligned}$$

$\langle 2 \rangle 3$. $\sum_{n=1}^N x_n \overline{y_n}$ is absolutely convergent.

$\langle 1 \rangle 2$. $\forall (x_n), (y_n) \in l^2. \langle (x_n), (y_n) \rangle = \overline{\langle (y_n), (x_n) \rangle}$

$\langle 1 \rangle 3$. $\forall \lambda \in \mathbb{C}. \forall (x_n), (y_n) \in l^2. \langle \lambda (x_n), (y_n) \rangle = \lambda \langle (x_n), (y_n) \rangle$

$\langle 1 \rangle 4$. $\forall (x_n), (y_n), (z_n) \in l^2. \langle (x_n) + (y_n), (z_n) \rangle = \langle (x_n), (z_n) \rangle + \langle (y_n), (z_n) \rangle$

$\langle 1 \rangle 5$. $\forall (x_n) \in l^2. \langle (x_n), (x_n) \rangle = 0 \Rightarrow (x_n) = 0$

□

Proposition 21.6.4. *The space $C[0, 1]$ of all continuous functions $[0, 1] \rightarrow \mathbb{C}$ is an inner product space under*

$$\langle f, g \rangle = \int_0^1 f(t) \overline{g(t)} dt .$$

Proposition 21.6.5. *The space \mathbb{C}^{mn} of all $m \times n$ complex matrices is an inner product space under*

$$\langle A, B \rangle = \text{tr}(B^* A)$$

where B^* is the conjugate transpose of B .

Theorem 21.6.6. *Let V be an inner product space. Let $x, y, z \in V$ and $\lambda \in \mathbb{C}$. Then:*

1. $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$
2. $\langle x, \lambda y \rangle = \overline{\lambda} \langle x, y \rangle$
3. $\langle x, 0 \rangle = \langle 0, x \rangle = 0$
4. If $\forall w \in V. \langle x, w \rangle = \langle y, w \rangle$ then $x = y$
5. $\langle x, x \rangle$ is a non-negative real.

PROOF: For part 4, take $w = x - y$. \square

Theorem 21.6.7 (Cauchy-Schwarz Inequality). *Let V be an inner product space. Let $x, y \in V$. Then*

$$|\langle x, y \rangle| \leq \langle x, x \rangle^{1/2} \langle y, y \rangle^{1/2} .$$

Equality holds if and only if x and y are linearly dependent.

PROOF:

$\langle 1 \rangle 1$. If x and y are linearly dependent then $|\langle x, y \rangle| = \langle x, x \rangle^{1/2} \langle y, y \rangle^{1/2}$.

PROOF: If $y = \lambda x$ then both sides are equal to $|\lambda| \langle x, x \rangle$.

$\langle 1 \rangle 2$. If x and y are linearly independent then $|\langle x, y \rangle| < \langle x, x \rangle^{1/2} \langle y, y \rangle^{1/2}$.

$\langle 2 \rangle 1$. For any $\lambda \in \mathbb{C}$ with $x + \lambda y \neq 0$ we have

$$\langle x, x \rangle + 2\Re(\overline{\lambda} \langle x, y \rangle) + |\lambda|^2 \langle y, y \rangle > 0 .$$

PROOF:

$$\begin{aligned} 0 &< \langle x + \lambda y, x + \lambda y \rangle \\ &= \langle x, x \rangle + \overline{\lambda} \langle x, y \rangle + \lambda \langle y, x \rangle + |\lambda|^2 \langle y, y \rangle \\ &= \langle x, x \rangle + 2\Re(\overline{\lambda} \langle x, y \rangle) + |\lambda|^2 \langle y, y \rangle \end{aligned}$$

$\langle 2 \rangle 2$. LET: $u = |\langle x, y \rangle| / \langle x, y \rangle$ or $u = 1$ if $\langle x, y \rangle = 0$

$\langle 2 \rangle 3$. For any $t \in \mathbb{R}$,

$$\langle x, x \rangle + 2|\langle x, y \rangle|t + \langle y, y \rangle t^2 > 0$$

PROOF: Take $\lambda = tu$ in $\langle 2 \rangle 1$

$\langle 2 \rangle 4$.

$$4|\langle x, y \rangle|^2 - 4\langle x, x \rangle \langle y, y \rangle < 0$$

PROOF: The quadratic $\langle 2 \rangle 3$ must have negative discriminant.
 $\langle 2 \rangle 5$.

$$|\langle x, y \rangle| < \langle x, x \rangle^{1/2} \langle y, y \rangle^{1/2}$$

□

Theorem 21.6.8. *Every inner product space is a normed space under $\|x\| = \langle x, x \rangle^{1/2}$.*

PROOF:

$\langle 1 \rangle 1$. If $\|x\| = 0$ then $x = 0$

$\langle 1 \rangle 2$. $\|\lambda x\| = |\lambda| \|x\|$

$\langle 1 \rangle 3$. $\|x + y\| \leq \|x\| + \|y\|$

PROOF:

$$\begin{aligned} \|x + y\|^2 &= \langle x + y, x + y \rangle \\ &= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\ &= \|x\|^2 + 2\Re \langle x, y \rangle + \|y\|^2 \\ &\leq \|x\|^2 + 2|\langle x, y \rangle| + \|y\|^2 \\ &< \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 && \text{(Cauchy-Schwarz)} \\ &= (\|x\| + \|y\|)^2 \end{aligned}$$

□

Theorem 21.6.9 (Parallelogram Law). *Let V be an inner product space. Let $x, y \in V$. Then*

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2 .$$

PROOF:

$$\begin{aligned} \|x + y\|^2 &= \|x\|^2 + \langle x, y \rangle + \langle y, x \rangle + \|y\|^2 \\ \|x - y\|^2 &= \|x\|^2 - \langle x, y \rangle - \langle y, x \rangle + \|y\|^2 \end{aligned}$$

Theorem 21.6.10 (Polarization Identity). *Let V be an inner product space. Let $x, y \in V$. Then*

$$4\langle x, y \rangle = \|x + y\|^2 - \|x - y\|^2 + i\|x + iy\|^2 - i\|x - iy\|^2 .$$

PROOF: Straightforward calculation. □