

# Mathematics

Robin Adams

July 30, 2023



# Chapter 1

## Sets and Classes

### 1.1 Classes

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

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

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

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

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

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

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

## 1.3 The Other Axioms

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

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

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

- *There exists an element of  $I$  that has no members*
- *For every  $x \in I$ , there exists a set  $y \in I$  such that the elements of  $y$  are exactly  $x$  and the members of  $x$ .*

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

**Axiom Schema 1.3.5** (Replacement). *For any predicate  $P(x, y)$ , the following is an axiom:*

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

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

## 1.4 Consequences of the Axioms

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

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

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

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

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

PROOF:

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

$\langle 1 \rangle 2$ . For all  $x \in \mathcal{P}\mathcal{P}\emptyset$ , there exists at most one  $y$  such that  $P(x, y)$ .

$\langle 2 \rangle 1$ . LET:  $x \in \mathcal{P}\mathcal{P}\emptyset$

$\langle 2 \rangle 2$ . LET:  $y$  and  $y'$  be sets.

$\langle 2 \rangle 3$ . ASSUME:  $P(x, y)$  and  $P(x, y')$

$\langle 2 \rangle 4$ .  $(x = \emptyset \wedge y = a) \vee (x = \mathcal{P}\emptyset \wedge y = b)$

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

$\langle 2 \rangle 5$ .  $(x = \emptyset \wedge y' = a) \vee (x = \mathcal{P}\emptyset \wedge y' = b)$

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

$\langle 2 \rangle 6$ .  $\emptyset \neq \mathcal{P}\emptyset$

PROOF: Since  $\emptyset \in \mathcal{P}\emptyset$  and  $\emptyset \notin \emptyset$ .

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

$\langle 1 \rangle 3$ . LET:  $A$  be the set  $\{y \mid \exists x \in \mathcal{P}\mathcal{P}\emptyset. P(x, y)\}$ .

$\langle 1 \rangle 4$ .  $A = \{a, b\}$

$\square$

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

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

**Proposition Schema 1.4.5.** *For any number  $n$ , the following is a theorem:*

*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 Schema 1.4.6** (Comprehension). *For any predicate  $P(x)$ , the following is a theorem:*

*For any set  $A$ , the class  $\{x \in A \mid P(x)\}$  is a set.*

PROOF:

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

$\langle 1 \rangle 2$ . LET:  $Q(x, y)$  be the predicate  $P(x) \wedge y = x$ .

$\langle 1 \rangle 3$ . For all  $x \in A$ , there exists at most one  $y$  such that  $Q(x, y)$ .

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

$$y \in B \Leftrightarrow \exists x \in A. Q(x, y) \quad ((1)4)$$

$$\Leftrightarrow \exists x \in A. (P(x) \wedge y = x) \quad ((1)2)$$

$$\Leftrightarrow P(y)$$

□

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

**Corollary 1.4.6.1.** *The universal class  $\mathbf{V}$  is a proper class.*

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

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

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

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

**Proposition Schema 1.4.7.** *For any classes  $\mathbf{A}$  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 1.4.8.** *For any class  $\mathbf{A}$ , the following is a theorem:*

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

PROOF:

⟨1⟩1.  $\mathbf{A} \subseteq \bigcup \mathcal{P}\mathbf{A}$

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

⟨1⟩2.  $\bigcup \mathcal{P}\mathbf{A} \subseteq \mathbf{A}$

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

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

⟨2⟩3.  $X \subseteq \mathbf{A}$

⟨2⟩4.  $x \in \mathbf{A}$

□

## 1.5 Transitive Classes

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

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

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

PROOF: Immediate from definitions.  $\square$

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

PROOF:

$\langle 1 \rangle 1$ . 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 1.5.2.

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

$\square$

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

PROOF:

$\langle 1 \rangle 1$ . 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 1.5.2.

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

PROOF: Proposition 1.4.7.

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

PROOF: Proposition 1.5.2.

$\langle 1 \rangle 2$ . 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 1.5.2.

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

PROOF: Proposition 1.4.8.

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

PROOF: Proposition 1.5.2.



□

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

PROOF:

$\langle 1 \rangle 1$ . 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 1.5.6.** *For any class  $\mathbf{A}$ , the following is a theorem:  
If every member of  $\mathbf{A}$  is a transitive set then  $\bigcap \mathbf{A}$  is a transitive class.*

PROOF:

$\langle 1 \rangle 1$ . 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.** For any sets  $a, b, c, d$ , we have  $(a, b) = (c, d)$  if and only if  $a = c$  and  $b = d$ .

PROOF:

$\langle 1 \rangle 1$ . If  $(a, b) = (c, d)$  then  $a = c$  and  $b = d$ .

$\langle 2 \rangle 1$ . ASSUME:  $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$

$\langle 2 \rangle 2$ .  $\bigcap \{\{a\}, \{a, b\}\} = \bigcap \{\{c\}, \{c, d\}\}$

$\langle 2 \rangle 3$ .  $\{a\} = \{c\}$

$\langle 2 \rangle 4$ .  $a = c$

$\langle 2 \rangle 5$ .  $\bigcup \{\{a\}, \{a, b\}\} = \bigcup \{\{c\}, \{c, d\}\}$

$\langle 2 \rangle 6$ .  $\{a, b\} = \{c, d\}$

$\langle 2 \rangle 7$ .  $b = c$  or  $b = d$

$\langle 2 \rangle 8$ .  $a = d$  or  $b = d$

$\langle 2 \rangle 9$ . If  $b = c$  and  $a = d$  then  $b = d$

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

$\langle 2 \rangle 10$ .  $b = d$

PROOF: From  $\langle 2 \rangle 7$ ,  $\langle 2 \rangle 8$ ,  $\langle 2 \rangle 9$ .

$\langle 1 \rangle 2$ . If  $a = c$  and  $b = d$  then  $(a, b) = (c, d)$ .

PROOF: First-order logic.

□

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

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

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

**Proposition Schema 2.1.5.** *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.** *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.** *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*  $\mathbf{R}$  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  $(x, y) \in \mathbf{R}$ .

### 2.2.1 Identity Functions

**Definition 2.2.2** (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 2.2.3** (Inverse). The *inverse* of a relation  $\mathbf{R}$  between  $\mathbf{A}$  and  $\mathbf{B}$  is the relation  $\mathbf{R}^{-1}$  between  $\mathbf{B}$  and  $\mathbf{A}$  defined by

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

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

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

PROOF:

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

### 2.2.3 Composition

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

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

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

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

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

PROOF:

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

### 2.2.4 Properties of Relations

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

**Definition 2.2.8** (Irreflexive). A relation  $\mathbf{R}$  is *irreflexive* iff there is no  $x$  such that  $(x, x) \in \mathbf{R}$ .

**Definition 2.2.9** (Symmetric). A relation  $\mathbf{R}$  is *symmetric* iff, whenever  $(x, y) \in \mathbf{R}$ , then  $(y, x) \in \mathbf{R}$ .

**Definition 2.2.10** (Antisymmetric). A relation  $\mathbf{R}$  is *antisymmetric* iff, whenever  $x\mathbf{R}y$  and  $y\mathbf{R}x$ , then  $x = y$ .

**Definition 2.2.11** (Transitive). A relation  $\mathbf{R}$  is *transitive* iff, whenever  $(x, y), (y, z) \in \mathbf{R}$ , then  $(x, z) \in \mathbf{R}$ .

**Proposition Schema 2.2.12.** *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:  $(x, y), (y, z) \in \mathbf{R}^{-1}$

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

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

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

□

## 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  $\mathbf{A}$ .

## 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  $\mathbf{F}$  be a function and  $\mathbf{A} \subseteq \text{dom } \mathbf{F}$ . Then  $\mathbf{A}$  is *closed* under  $\mathbf{F}$  iff  $\forall x \in \mathbf{A}. \mathbf{F}(x) \in \mathbf{A}$ .

**Proposition 3.1.3.** *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.** *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.** *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:

- ⟨1⟩1. LET:  $A$  be a set.
- ⟨1⟩2. LET:  $\mathcal{A} = \{\{B\} \times B \mid B \in \mathcal{P}A - \{\emptyset\}\}$
- ⟨1⟩3. Every member of  $\mathcal{A}$  is nonempty.
- ⟨1⟩4. Any two distinct members of  $\mathcal{A}$  are disjoint.
- ⟨1⟩5. PICK a set  $C$  such that, for all  $X \in \mathcal{A}$ , we have  $C \cap X$  is a singleton.

PROOF: Axiom of Choice.

- ⟨1⟩6. LET:  $F = C \cap \bigcup \mathcal{A}$
- ⟨1⟩7.  $F : \mathcal{P}A - \{\emptyset\} \rightarrow A$ 
  - ⟨2⟩1.  $F$  is a function.
    - ⟨3⟩1. LET:  $(B, b), (B, b') \in F$
    - ⟨3⟩2.  $(B, b), (B, b') \in \{B\} \times B$
    - PROOF: Since  $(B, b), (B, b') \in \bigcup \mathcal{A}$ .
    - ⟨3⟩3.  $(B, b), (B, b') \in C \cap (\{B\} \times B)$
    - ⟨3⟩4.  $(B, b) = (B, b')$
    - PROOF: From ⟨1⟩5.
    - ⟨3⟩5.  $b = b'$

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

PROOF:

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

- ⟨2⟩3.  $\text{ran } F \subseteq A$

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

□

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

PROOF:

- ⟨1⟩1. LET:  $R$  be a relation between  $A$  and  $B$ .
- ⟨1⟩2. PICK a choice function  $G$  for  $B$ .
- ⟨1⟩3. Define  $H : A \rightarrow B$  by  $H(x) = G(\{y \mid xRy\})$
- ⟨1⟩4.  $H \subseteq R$

□

### 3.1.1 Injective Functions

**Definition 3.1.7** (Injective). A function  $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$  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.** *For any class  $\mathbf{A}$ , the following is a theorem:*

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



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

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

*Assume  $F : A \rightarrow B$  and  $G : B \rightarrow C$ . Then  $G \circ F : A \rightarrow C$ .*

PROOF:

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

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

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

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

PROOF: Since  $G$  is injective.

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

PROOF: Since  $F$  is injective.

$\square$

**Proposition 3.1.10.** *Let  $F : A \rightarrow B$  where  $A$  is nonempty. There exists  $G : B \rightarrow A$  (a left inverse) such that  $G \circ F = \text{id}_A$  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.** *For any class  $A$ , the following is a theorem:*

*$\text{id}_A : A \rightarrow A$  is surjective.*

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

**Proposition Schema 3.1.13.** *For any classes  $A, B, C, F$  and  $G$ , the following is a theorem:*

*If  $F : A \twoheadrightarrow B$  and  $G : B \twoheadrightarrow C$ , then  $G \circ F : A \twoheadrightarrow C$ .*

PROOF:

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

□

**Proposition 3.1.14.** *Let  $F : A \rightarrow B$ . 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:

- ⟨1⟩1. If  $F$  has a right inverse then  $F$  is surjective.
  - ⟨2⟩1. ASSUME:  $F$  has a right inverse  $H : B \rightarrow A$ .
  - ⟨2⟩2. LET:  $y \in B$
  - ⟨2⟩3.  $F(H(y)) = y$
  - ⟨2⟩4. There exists  $x \in A$  such that  $F(x) = y$
- ⟨1⟩2. If  $F$  is surjective then  $F$  has a right inverse.
  - ⟨2⟩1. ASSUME:  $F$  is surjective.
  - ⟨2⟩2. PICK a function  $H : B \rightarrow A$  such that  $H \subseteq F^{-1}$

PROOF: Proposition 3.1.6.

- ⟨2⟩3.  $F \circ H = \text{id}_B$ 
  - ⟨3⟩1. LET:  $y \in B$
  - ⟨3⟩2.  $(y, H(y)) \in F^{-1}$
  - ⟨3⟩3.  $F(H(y)) = y$

□

### 3.1.3 Bijections

**Definition 3.1.15** (Bijection). Let  $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$ . 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.** *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. □

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

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

PROOF:

- ⟨1⟩1.  $\mathbf{F}^{-1} : \mathbf{B} \rightarrow \mathbf{A}$ 
  - ⟨2⟩1. LET:  $b \in \mathbf{B}$
  - ⟨2⟩2. PICK  $a \in \mathbf{A}$  such that  $\mathbf{F}(a) = b$ .
 

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

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

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

PROOF: Since  $\mathbf{F}$  is injective.

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

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

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

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

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

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

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

□

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

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

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

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

PROOF: By an Axiom of Replacement. □

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

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

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

PROOF:

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

□

**Proposition Schema 3.1.23.** *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:

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

**Proposition 3.1.24.** *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:  $\langle 2 \rangle 1$
  - $\langle 2 \rangle 6. x \in \mathbf{A} \cap \mathbf{B}$
  - $\langle 2 \rangle 7. y \in \mathbf{F}(\mathbf{A} \cap \mathbf{B})$

$\square$

**Proposition Schema 3.1.25.** *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:

- $\langle 1 \rangle 1. \mathbf{F}(\bigcap \mathbf{A}) \subseteq \bigcap \{\mathbf{F}(X) \mid X \in \mathbf{A}\}$

- ⟨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.** *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  $\langle 2 \rangle 3$ .

□

### 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.** *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:

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

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

*Assume  $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$  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:

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

### 3.1.7 Function Sets

**Proposition 3.1.30.** *For any classes  $\mathbf{B}$  and  $\mathbf{F}$ , the following is a theorem:*

*Let  $A$  be a set. If  $\mathbf{F} : A \rightarrow \mathbf{B}$  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  $\mathbf{F} \subseteq A \times R$ . □

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

PROOF:

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

PROOF: By an Axiom of Replacement.

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

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

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

□

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

PROOF:

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

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

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

PROOF: Proposition 3.1.6.

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

□

## 3.2 Equinumerosity

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

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

PROOF:

$\langle 1 \rangle 1.$  ASSUME: for a contradiction  $f : A \approx \mathcal{P}A$

$\langle 1 \rangle 2.$  LET:  $S = \{x \in A \mid x \notin f(x)\}$

$\langle 1 \rangle 3.$  PICK  $a \in A$  such that  $f(a) = S$

$\langle 1 \rangle 4.$   $a \in S$  if and only if  $a \notin S$

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

PROOF: This is a contradiction.

□

## 3.3 Domination

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

**Proposition 3.3.2.** *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:

- ⟨1⟩1. If  $A \preceq B$  and  $A \neq \emptyset$  then there exists a surjective function  $B \rightarrow A$ .
  - ⟨2⟩1. ASSUME:  $f : A \rightarrow B$  be injective.
  - ⟨2⟩2. PICK  $a \in A$
  - ⟨2⟩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.
  - ⟨2⟩4.  $g$  is surjective.
- ⟨1⟩2. If there exists a surjective function  $B \rightarrow A$  then  $A \preceq B$ .
  - ⟨2⟩1. ASSUME: there exists a surjective function  $g : B \rightarrow A$
  - ⟨2⟩2.  $\forall a \in A. \exists b \in B. g(b) = a$
  - ⟨2⟩3. Choose a function  $f : A \rightarrow B$  such that  $\forall a \in A. g(f(a)) = a$
  - ⟨2⟩4.  $f$  is injective.

□



## Chapter 4

# Equivalence Relations

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

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

PROOF: Propositions 3.1.16, 3.1.17, 3.1.18.  $\square$

**Definition 4.0.3** (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 4.0.4** (Equivalence Class). Let  $\mathbf{R}$  be an equivalence relation on  $\mathbf{A}$  and  $a \in \mathbf{A}$ . The *equivalence class* of  $a$  modulo  $\mathbf{R}$  is

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

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

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

PROOF:

$\langle 1 \rangle 1$ . 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 4.0.6** (Partition). A *partition*  $\Pi$  of a set  $A$  is a set of nonempty subsets of  $A$  that is disjoint and exhaustive, i.e.

1. no two different sets in  $\Pi$  have any common elements, and
2. each element of  $A$  is in some set in  $\Pi$ .

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

**Theorem 4.0.8.** Let  $A$  be a set and  $\mathbf{B}$  a class. Let  $R$  be an equivalence relation on  $A$  and  $F : A \rightarrow \mathbf{B}$ . 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 4.0.5.  
 $\langle 3 \rangle 3$ .  $F(a) = F(a')$   
 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 4.0.5.  
 $\langle 2 \rangle 5$ .  $F(a) = F(a')$   
 PROOF:  $\langle 2 \rangle 1$   
 $\langle 1 \rangle 3$ . If  $G, H : A/R \rightarrow \mathbf{B}$  and  $\forall a \in A. G([a]_R) = H([a]_R)$  then  $G = H$ .  
 $\square$

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

PROOF:

- $\langle 1 \rangle 1$ . Every member of  $A/R$  is nonempty.  
 PROOF: Since  $a \in [a]_R$  by reflexivity.  
 $\langle 1 \rangle 2$ . No two different sets in  $A/R$  have any common elements.  
 $\langle 2 \rangle 1$ . LET:  $[a]_R, [b]_R \in A/R$   
 $\langle 2 \rangle 2$ . LET:  $c \in [a]_R \cap [b]_R$   
 PROVE:  $[a]_R = [b]_R$   
 $\langle 2 \rangle 3$ .  $aRc$   
 PROOF:  $\langle 2 \rangle 2$   
 $\langle 2 \rangle 4$ .  $bRc$   
 PROOF:  $\langle 2 \rangle 2$   
 $\langle 2 \rangle 5$ .  $cRb$   
 PROOF: Symmetry,  $\langle 2 \rangle 4$   
 $\langle 2 \rangle 6$ .  $aRb$   
 PROOF: Transitivity,  $\langle 2 \rangle 3$ ,  $\langle 2 \rangle 5$   
 $\langle 2 \rangle 7$ .  $[a]_R = [b]_R$   
 PROOF: Proposition 4.0.5,  $\langle 2 \rangle 6$   
 $\langle 1 \rangle 3$ . Each element of  $A$  is in some set in  $A/R$ .  
 PROOF: Since  $a \in [a]_R$  by reflexivity.  
 $\square$

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

PROOF: Easy.  $\square$

**Definition 4.0.11** (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 5

# Ordering Relations

### 5.0.1 Partial Orders

**Definition 5.0.1** (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  $x \leq y \wedge x \neq y$ .

**Definition 5.0.2** (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  $(A, \leq)$ .

**Definition 5.0.3** (Strictly Monotone). Let  $(A, <_A)$  and  $(B, <_B)$  be linearly ordered sets. A function  $f : A \rightarrow B$  is *strictly monotone* iff, whenever  $x <_A y$ , then  $f(x) <_B f(y)$ .

**Proposition 5.0.4.** *A strictly monotone function is injective.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $(A, <_A)$  and  $(B, <_B)$  be linearly ordered sets.

$\langle 1 \rangle 2$ . LET:  $f : A \rightarrow B$  be strictly monotone.

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

$\langle 1 \rangle 4$ . ASSUME:  $f(x) = f(y)$

$\langle 1 \rangle 5$ .  $f(x) \not<_B f(y)$  and  $f(y) \not<_B f(x)$

PROOF: Trichotomy.

$\langle 1 \rangle 6$ .  $x \not<_A y$  and  $y \not<_A x$

$\langle 1 \rangle 7$ .  $x = y$

PROOF: Trichotomy.

□

**Proposition 5.0.5.** *If  $\mathbf{R}$  is a partial order on  $\mathbf{A}$  then so is  $\mathbf{R}^{-1}$ .*

PROOF: Easy. □

**Proposition 5.0.6.** *Let  $\mathbf{R}$  be a partial order on  $\mathbf{A}$  and  $\mathbf{B} \subseteq \mathbf{A}$ . Then  $\mathbf{R} \cap \mathbf{B}^2$  is a partial order on  $\mathbf{B}$ .*

PROOF: Easy.  $\square$

**Definition 5.0.7** (Minimal). Let  $\leq$  be a partial order on  $\mathbf{A}$ . An element  $m \in \mathbf{A}$  is *minimal* iff there is no  $x \in \mathbf{A}$  such that  $x < m$ .

**Definition 5.0.8** (Maximal). Let  $\leq$  be a partial order on  $\mathbf{A}$ . An element  $m \in \mathbf{A}$  is *maximal* iff there is no  $x \in \mathbf{A}$  such that  $m < x$ .

**Definition 5.0.9** (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 5.0.10.** *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 5.0.11** (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 5.0.12.** *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 5.0.13** (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 5.0.14** (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 5.0.15** (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 5.0.16** (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 5.0.17** (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 5.0.18** (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 5.0.19** (Complete). A partial order is *complete* iff every nonempty subset bounded above has a supremum, and every nonempty subset bounded below has an infimum.

**Theorem 5.0.20.** *Let  $A$  and  $P$  be complete posets with no least or greatest element. Let  $B$  be dense in  $A$  and  $Q$  be dense in  $P$ . Every order isomorphism  $B \cong Q$  extends uniquely to an order isomorphism  $A \cong P$ .*

PROOF:

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

- ⟨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.
    - ⟨3⟩2. PICK  $b \in B$  such that  $a < b < a_2$
    - ⟨3⟩3.  $\phi(b)$  is an upper bound for  $\phi(S(a))$ .
- ⟨1⟩3.  $\bar{\phi}$  is monotone.
  - PROOF: If  $a \leq a'$  then  $S(a) \subseteq S(a')$  and so  $\bar{\phi}(a) \leq \bar{\phi}(a')$ .
- ⟨1⟩4.  $\bar{\phi}$  extends  $\phi$ .
  - ⟨2⟩1. LET:  $b \in B$ 
    - PROVE:  $\phi(b) = \sup \phi(S(b))$
  - ⟨2⟩2.  $\phi(b)$  is an upper bound for  $\phi(S(b))$
  - ⟨2⟩3. LET:  $u$  be any upper bound for  $\phi(S(b))$ 
    - PROVE:  $\phi(b) \leq u$
  - ⟨2⟩4. ASSUME: for a contradiction  $u < \phi(b)$
  - ⟨2⟩5. PICK  $q \in Q$  such that  $u < q < \phi(b)$
  - ⟨2⟩6. PICK  $b' \in B$  such that  $\phi(b') = q$
  - ⟨2⟩7.  $b' < b$
  - ⟨2⟩8.  $b' \in S(b)$
  - ⟨2⟩9.  $q = \phi(b') \leq u$
  - ⟨2⟩10. Q.E.D.
  - PROOF: This is a contradiction.
- ⟨1⟩5. LET:  $\bar{\psi} = \phi^{-1}$
- ⟨1⟩6. LET:  $\bar{\psi} : P \rightarrow A$  be the function  $\bar{\psi}(p) = \sup\{\psi(q) \mid q \in Q, q < p\}$
- ⟨1⟩7.  $\bar{\psi}$  is monotone and extends  $\psi$ 
  - PROOF: Similar.
- ⟨1⟩8.  $\bar{\psi} \circ \bar{\phi} : A \rightarrow A$  is monotone and the identity on  $B$ .
- ⟨1⟩9.  $\bar{\psi} \circ \bar{\phi} = \text{id}_A$ 
  - PROOF: Proposition 5.0.24.
- ⟨1⟩10.  $\bar{\phi} \circ \bar{\psi} = \text{id}_B$ 
  - PROOF: Proposition 5.0.24.
- ⟨1⟩11. If  $\phi^* : A \cong P$  is any order isomorphism that extends  $\phi$  then  $\phi^* = \bar{\phi}$ .
  - ⟨2⟩1. LET:  $a \in A$ 
    - PROVE:  $\phi^*(a) = \sup \phi(S(a))$
  - ⟨2⟩2.  $\phi^*(a)$  is an upper bound for  $\phi(S(a))$
  - ⟨2⟩3. LET:  $u$  be any upper bound for  $\phi(S(a))$ 
    - PROVE:  $\phi^*(a) \leq u$
  - ⟨2⟩4. ASSUME: for a contradiction  $u < \phi^*(a)$
  - ⟨2⟩5. PICK  $q \in Q$  such that  $u < q < \phi^*(a)$
  - ⟨2⟩6. PICK  $b \in B$  such that  $q = \phi(b)$
  - ⟨2⟩7.  $b < a$

- $\langle 2 \rangle 8. b \in S(a)$
- $\langle 2 \rangle 9. q = \phi(b) \leq u$
- $\langle 2 \rangle 10. \text{Q.E.D.}$

PROOF: This is a contradiction.

□

**Theorem 5.0.21** (Knaster Fixed-Point Theorem). *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:

- $\langle 1 \rangle 1. \text{LET: } B = \{x \in A \mid x \leq \phi(x)\}$

- $\langle 1 \rangle 2. \text{LET: } a = \sup B$

PROOF:  $B$  is nonempty because the least element of  $A$  is in  $B$ , and it is bounded above by the greatest element of  $A$ .

- $\langle 1 \rangle 3. \text{For all } b \in B \text{ we have } b \leq \phi(a)$

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

- $\langle 2 \rangle 2. b \leq \phi(b)$

- $\langle 2 \rangle 3. b \leq a$

- $\langle 2 \rangle 4. \phi(b) \leq \phi(a)$

- $\langle 2 \rangle 5. b \leq \phi(a)$

- $\langle 1 \rangle 4. a \leq \phi(a)$

- $\langle 1 \rangle 5. \phi(a) \leq \phi(\phi(a))$

- $\langle 1 \rangle 6. \phi(a) \in B$

- $\langle 1 \rangle 7. \phi(a) \leq a$

- $\langle 1 \rangle 8. \phi(a) = a$

□

**Proposition 5.0.22.** *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:

- $\langle 1 \rangle 1. \text{LET: } a \in A$

PROVE:  $\theta(a) = a$

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

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

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

- $\langle 3 \rangle 1. \text{PICK } a_1 < a$

PROOF: Since  $a$  is not least.

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

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

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

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

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

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

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



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

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

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

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

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

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

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

PROOF:  $\theta(b) = b$

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

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

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

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

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

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

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

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

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

□

**Definition 5.0.23** (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  $x < z < y$ .

**Definition 5.0.24** (Initial Segment). Let  $A$  be a poset and  $t \in A$ . The *initial segment* up to  $t$  is

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

## 5.0.2 Linear Orders

**Definition 5.0.25** (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 5.0.26** (Trichotomy). Let  $\leq$  be a linear ordering on  $\mathbf{A}$ . For any  $x, y \in \mathbf{A}$ , exactly one of  $x < y$ ,  $x = y$ ,  $y < x$  holds.

PROOF: Immediate from definitions. □

**Proposition 5.0.27**. Let  $A$  and  $B$  be linearly ordered sets. Let  $f : A \rightarrow B$ . Let  $x, y \in A$ . If  $f$  is strictly monotone and  $f(x) < f(y)$  then  $x < y$ .

PROOF:

$\langle 1 \rangle 1$ .  $f(x) \neq f(y)$  and  $f(y) \not< f(x)$

PROOF: Trichotomy.

$\langle 1 \rangle 2$ .  $x \neq y$  and  $y \not< x$

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

PROOF: Trichotomy.

□

**Proposition 5.0.28.** *Let  $<$  be an irreflexive relation on  $\mathbf{A}$  that satisfies trichotomy. Define  $\leq$  on  $\mathbf{A}$  by  $x \leq y$  iff  $x < y$  or  $x = y$ . Then  $\leq$  is a linear ordering on  $\mathbf{A}$  and  $x < y$  iff  $x \leq y$  and  $x \neq y$ .*

PROOF: Easy. □

**Proposition 5.0.29.** *If  $\mathbf{R}$  is a linear ordering on  $\mathbf{A}$  then  $\mathbf{R}^{-1}$  is also a linear ordering on  $\mathbf{A}$ .*

PROOF:

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

PROOF: Proposition 2.2.12.

$\langle 1 \rangle 2$ .  $\mathbf{R}^{-1}$  satisfies trichotomy.

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

$\langle 2 \rangle 2$ . Exactly one of  $(x, y) \in \mathbf{R}$ ,  $(y, x) \in \mathbf{R}$ ,  $x = y$  holds.

$\langle 2 \rangle 3$ . Exactly one of  $(y, x) \in \mathbf{R}^{-1}$ ,  $(x, y) \in \mathbf{R}^{-1}$ ,  $x = y$  holds.

□

**Proposition 5.0.30.** *Let  $\mathbf{R}$  be a linear order on  $\mathbf{A}$  and  $\mathbf{B} \subseteq \mathbf{A}$ . Then  $\mathbf{R} \cap \mathbf{B}^2$  is a linear order on  $\mathbf{B}$ .*

PROOF: Easy. □

**Definition 5.0.31** (Lexicographic Ordering). Let  $A$  and  $B$  be linearly ordered sets. The *lexicographic ordering*  $<$  on  $A \times B$  is defined by:

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

**Proposition 5.0.32.** *Let  $A$  and  $B$  be linearly ordered sets. Then the lexicographic ordering on  $A \times B$  is a linear ordering.*

PROOF:

$\langle 1 \rangle 1$ .  $<$  is transitive.

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

PROVE:  $(a_1, b_1) < (a_3, b_3)$

$\langle 2 \rangle 2$ . CASE:  $a_1 < a_2$

$\langle 3 \rangle 1$ .  $a_2 < a_3$  or  $a_2 = a_3$

PROOF:  $\langle 2 \rangle 1$

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

PROOF: Transitivity

$\langle 3 \rangle 3$ .  $(a_1, b_1) < (a_3, b_3)$

$\langle 2 \rangle 3$ . CASE:  $a_1 = a_2$  and  $b_1 < b_2$  and  $a_2 < a_3$

PROOF: We have  $a_1 < a_3$  so  $(a_1, b_1) < (a_3, b_3)$ .

$\langle 2 \rangle 4$ . CASE:  $a_1 = a_2$  and  $b_1 < b_2$  and  $a_2 = a_3$  and  $b_2 < b_3$

PROOF: We have  $a_1 = a_3$  and  $b_1 < b_3$  so  $(a_1, b_1) < (a_3, b_3)$ .

$\langle 1 \rangle 2$ .  $<$  satisfies trichotomy.

$\langle 2 \rangle 1$ . LET:  $(a_1, b_1), (a_2, b_2) \in A \times B$

$\langle 2 \rangle 2$ . Exactly one of  $a_1 < a_2$ ,  $a_1 = a_2$ ,  $a_2 < a_1$  holds.

$\langle 2 \rangle 3$ . CASE:  $a_1 < a_2$

PROOF: We have  $(a_1, b_1) < (a_2, b_2)$ ,  $(a_1, b_1) \neq (a_2, b_2)$ , and  $(a_2, b_2) \not< (a_1, b_1)$ .

$\langle 2 \rangle 4$ . CASE:  $a_1 = a_2$

$\langle 3 \rangle 1$ . Exactly one of  $b_1 < b_2$ ,  $b_1 = b_2$ ,  $b_2 < b_1$  holds.

$\langle 3 \rangle 2$ . Exactly one of  $(a_1, b_1) < (a_2, b_2)$ ,  $(a_1, b_1) = (a_2, b_2)$ ,  $(a_2, b_2) < (a_1, b_1)$  holds.

$\langle 2 \rangle 5$ . CASE:  $a_2 < a_1$

PROOF: We have  $(a_2, b_2) < (a_1, b_1)$ ,  $(a_2, b_2) \neq (a_1, b_1)$ , and  $(a_1, b_1) \not< (a_2, b_2)$ .

### 5.0.3 Well Orderings

**Definition 5.0.33** (Well Ordering). A *well ordering* on a class  $\mathbf{A}$  is a linear ordering on  $\mathbf{A}$  such that:

- For all  $t \in \mathbf{A}$  we have  $\text{seg } t$  is a set.
- Every nonempty subset of  $\mathbf{A}$  has a least element.

**Theorem 5.0.34.** Let  $A$  and  $B$  be well ordered sets. Then one of the following holds:  $A \cong B$ ; there exists  $b \in B$  such that  $A \cong \text{seg } b$ ; there exists  $a \in A$  such that  $\text{seg } a \cong B$ .

PROOF:

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

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

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

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

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

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

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

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

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

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

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

□

**Proposition 5.0.35.** There is at most one isomorphism between two well ordered sets.

PROOF:

$\langle 1 \rangle 1$ . LET:  $A$  and  $B$  be well ordered sets.

$\langle 1 \rangle 2$ . LET:  $f, g : A \cong B$  be isomorphisms.

$\langle 1 \rangle 3$ .  $\forall x \in A. f(x) = g(x)$

PROOF: Transfinite induction on  $x$ .

□

**Proposition 5.0.36.** *Let  $B$  be a poset,  $A$  a set, and  $f : A \rightarrow B$  an injection. Define  $\leq$  on  $A$  by  $x \leq y$  iff  $f(x) \leq f(y)$ .*

1.  $\leq$  is a partial order on  $A$ .

2. If  $B$  is a linearly ordered set then  $\leq$  is a linear order on  $A$ .

3. If  $B$  is a well ordered set then  $\leq$  is a well ordering on  $A$ .

PROOF: Easy. □

## 5.1 Transfinite Recursion

**Theorem Schema 5.1.1** (Transfinite Recursion Theorem Schema). *For any property  $G(x, y)$ , the following is a theorem:*

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

$$\forall t \in A. G(F \upharpoonright \text{seg } t, F(t)) .$$

PROOF:

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

$$\forall x \in \text{dom } v. G(v \upharpoonright \text{seg } x, v(x)) .$$

$\langle 1 \rangle 2$ . For all  $t_1, t_2 \in A$  with  $t_1 \leq t_2$ , if  $v_1$  is *G-constructed up to  $t_1$*  and  $v_2$  is *G-constructed up to  $t_2$* , then  $\forall x \leq t_1. v_1(x) = v_2(x)$ .

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

$\langle 2 \rangle 2$ . ASSUME:  $\forall y < x. (y \leq t_1 \Rightarrow v_1(y) = v_2(y))$

$\langle 2 \rangle 3$ . ASSUME:  $x \leq t_1$

$\langle 2 \rangle 4$ .  $G(v_1 \upharpoonright \text{seg } x, v_1(x))$

$\langle 2 \rangle 5$ .  $G(v_2 \upharpoonright \text{seg } x, v_2(x))$

$\langle 2 \rangle 6$ .  $v_1 \upharpoonright \text{seg } x = v_2 \upharpoonright \text{seg } x$

$\langle 2 \rangle 7$ .  $v_1(x) = v_2(x)$

$\langle 2 \rangle 8$ . Q.E.D.

PROOF: By transfinite induction.

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

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

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

$\langle 1 \rangle 5$ .  $F$  is a function.

$\langle 2 \rangle 1$ . LET:  $(x, y_1), (x, y_2) \in F$

- ⟨2⟩2. PICK  $v_1, v_2 \in \mathcal{K}$  such that  $v_1(x) = y_1$  and  $v_2(x) = y_2$ .
- ⟨2⟩3. PICK  $t_1, t_2 \in A$  such that  $v_1$  is  $G$ -constructed up to  $t_1$  and  $v_2$  is  $G$ -constructed up to  $t_2$ .
- ⟨2⟩4. ASSUME: w.l.o.g.  $t_1 \leq t_2$
- ⟨2⟩5.  $v_1(x) = v_2(x)$
- PROOF: ⟨1⟩2.
- ⟨2⟩6.  $y_1 = y_2$
- ⟨1⟩6.  $\forall x \in \text{dom } F.G(F \upharpoonright \text{seg } x, F(x))$
- ⟨2⟩1. LET:  $x \in \text{dom } F$
- ⟨2⟩2. PICK  $v \in \mathcal{K}$  such that  $v(x) = F(x)$
- ⟨2⟩3. PICK  $t$  such that  $v$  is  $G$ -constructed up to  $t$ .
- ⟨2⟩4.  $G(v \upharpoonright \text{seg } x, v(x))$
- ⟨2⟩5.  $v \upharpoonright \text{seg } x = F \upharpoonright \text{seg } x$
- ⟨3⟩1. LET:  $y < x$
- PROVE:  $v(y) = F(y)$
- ⟨3⟩2.  $y \in \text{dom } F$
- PROOF: Since  $y \in \text{dom } v$  and  $v \in \mathcal{K}$ .
- ⟨3⟩3. PICK  $u \in \mathcal{K}$  such that  $u(y) = F(y)$
- ⟨3⟩4.  $u(y) = v(y)$
- PROOF: ⟨1⟩2.
- ⟨3⟩5.  $v(y) = F(y)$
- ⟨2⟩6.  $G(F \upharpoonright \text{seg } x, F(x))$
- ⟨1⟩7.  $\text{dom } F = A$
- ⟨2⟩1. ASSUME:  $\text{dom } F \neq A$
- ⟨2⟩2. LET:  $t$  be least in  $A - \text{dom } F$
- ⟨2⟩3.  $\text{seg } t = \text{dom } F$
- ⟨2⟩4. LET:  $y$  be the unique object such that  $G(F, y)$
- ⟨2⟩5. LET:  $v = F \cup \{(t, y)\}$
- ⟨2⟩6.  $v$  is  $G$ -constructed up to  $t$ .
- ⟨2⟩7.  $t \in \text{dom } F$
- ⟨2⟩8. Q.E.D.
- PROOF: This is a contradiction.
- ⟨1⟩8.  $F$  is unique.
- PROOF: If  $F'$  also satisfies the theorem, prove  $F(x) = F'(x)$  by transfinite induction on  $x$ .

□

**Proposition 5.1.2.** *Let  $\mathbf{R}$  be a well ordering on  $\mathbf{A}$  and  $\mathbf{B} \subseteq \mathbf{A}$ . Then  $\mathbf{R} \cap \mathbf{B}^2$  is a well ordering on  $\mathbf{B}$ .*

PROOF: Easy. □

**Theorem 5.1.3** (Transfinite Induction Principle). *Let  $\leq$  be a well ordering on  $\mathbf{A}$ . Let  $\mathbf{B} \subseteq \mathbf{A}$ . Assume that, for all  $t \in \mathbf{A}$ ,*

$$\text{seg } t \subseteq \mathbf{B} \Rightarrow t \in \mathbf{B} .$$

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

PROOF:

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

$\langle 1 \rangle 2$ . PICK  $a \in \mathbf{A} - \mathbf{B}$

$\langle 1 \rangle 3$ . LET:  $m$  be the least element of  $(\text{seg } a \cup \{a\}) - B$

$\langle 1 \rangle 4$ .  $\text{seg } m \subseteq \mathbf{B}$

PROOF: By leastness of  $m$ .

$\langle 1 \rangle 5$ .  $m \in \mathbf{B}$

$\langle 1 \rangle 6$ . Q.E.D.

PROOF: This is a contradiction.

□

**Theorem 5.1.4.** *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:

$\langle 1 \rangle 1$ . LET:  $C \subseteq A$  be nonempty.

$\langle 1 \rangle 2$ . LET:  $B = \{t \in A \mid \forall x \in C. t < x\}$

$\langle 1 \rangle 3$ .  $B \cap C = \emptyset$

$\langle 1 \rangle 4$ .  $B \neq A$

$\langle 1 \rangle 5$ . PICK  $t \in A$  such that  $\text{seg } t \subseteq B$  and  $t \notin B$

$\langle 1 \rangle 6$ .  $t$  is least in  $C$ .

□

## Chapter 6

# Ordinal Numbers

**Definition 6.0.1** (Ordinal Number). Let  $A$  be a well ordered set. Define the function  $E$  on  $A$  by transfinite recursion by:

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

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

**Proposition 6.0.2.**  $E$  is a bijection between  $A$  and  $\alpha$ .

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

**Proposition 6.0.3.** For all  $s, t \in A$ , we have  $s < t$  if and only if  $E(s) \in E(t)$ .

PROOF:

$\langle 1 \rangle 1$ . If  $s < t$  then  $E(s) \in E(t)$ .

PROOF: By definition of  $E(t)$ .

$\langle 1 \rangle 2$ . If  $E(s) \in E(t)$  then  $s < t$ .

$\langle 2 \rangle 1$ . ASSUME:  $E(s) \in E(t)$

$\langle 2 \rangle 2$ . PICK  $s' < t$  such that  $E(s) = E(s')$

$\langle 2 \rangle 3$ .  $s = s'$

PROOF: Proposition 6.0.2.

$\langle 2 \rangle 4$ .  $s < t$

$\square$

**Corollary 6.0.3.1.**  $(A, \leq)$  is isomorphic to  $\alpha$  ordered by  $\in$ .

**Corollary 6.0.3.2.**  $\alpha$  is well ordered by  $\in$ .

**Corollary 6.0.3.3.** Two well-ordered sets are isomorphic if and only if they have the same ordinal number.

**Proposition 6.0.4.**  $\alpha$  is a transitive set.

PROOF:

$\langle 1 \rangle 1$ . LET:  $y \in z \in \alpha$

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

□

**Theorem 6.0.5.** *A set  $\alpha$  is an ordinal number if and only if it is a transitive set well-ordered by  $\in$ .*

PROOF:

- $\langle 1 \rangle 1$ . Every ordinal number is a transitive set.

PROOF: Proposition 6.0.4.

- $\langle 1 \rangle 2$ . Every ordinal number is well-ordered by  $\in$ .

PROOF: Corollary 6.0.3.2.

- $\langle 1 \rangle 3$ . Every transitive set well-ordered by  $\in$  is an ordinal number.

- $\langle 2 \rangle 1$ . LET:  $\alpha$  be a transitive set well-ordered by  $\in$

- $\langle 2 \rangle 2$ . LET:  $E : (\alpha, \in) \cong (\beta, \in)$  be the isomorphism between  $(\alpha, \in)$  and its ordinal number.

- $\langle 2 \rangle 3$ .  $\forall x \in \alpha. E(x) = x$

PROOF: By transfinite induction on  $x$ .

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

□

**Proposition 6.0.6.** *Every element of an ordinal number is an ordinal number.*

PROOF:

- $\langle 1 \rangle 1$ . LET:  $\alpha$  be an ordinal number.

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

- $\langle 1 \rangle 3$ .  $\beta$  is a transitive set.

- $\langle 2 \rangle 1$ . LET:  $x \in y \in \beta$

- $\langle 2 \rangle 2$ .  $y \in \alpha$

PROOF: Since  $\alpha$  is a transitive set.

- $\langle 2 \rangle 3$ .  $x \in \alpha$

PROOF: Since  $\alpha$  is a transitive set.

- $\langle 2 \rangle 4$ .  $x \in \beta$

PROOF: Since  $\alpha$  is well-ordered by  $\in$ .

- $\langle 1 \rangle 4$ .  $\beta$  is well-ordered by  $\in$ .

PROOF: Since  $\beta \subseteq \alpha$ .

□

**Proposition 6.0.7.** *Given two ordinal numbers  $\alpha, \beta$ , exactly one of  $\alpha \in \beta$ ,  $\alpha = \beta$ ,  $\beta \in \alpha$  holds.*

PROOF:

- $\langle 1 \rangle 1$ . At most one holds.

PROOF: Since we never have  $\alpha \in \alpha$ .

- $\langle 1 \rangle 2$ . At least one holds.

- $\langle 2 \rangle 1$ . Either  $\alpha \cong \beta$  or  $\exists t \in \beta. \alpha \cong \text{seg } t$  or  $\exists t \in \alpha. \text{seg } t \cong \beta$ .

- $\langle 2 \rangle 2$ . CASE:  $\alpha \cong \beta$



PROOF: Then  $\alpha = \beta$  as isomorphic well-ordered sets have the same ordinal number.

$\langle 2 \rangle 3$ . CASE: There exists  $t \in \beta$  such that  $\alpha \cong \text{seg } t$

PROOF:  $t$  is an ordinal number and  $\alpha = t$ , so  $\alpha \in \beta$ .

$\langle 2 \rangle 4$ . CASE: There exists  $t \in \alpha$  such that  $\text{seg } t \cong \beta$

PROOF:  $t$  is an ordinal number and  $t = \beta$ , so  $\beta \in \alpha$ .

□

**Proposition 6.0.8.** *Any nonempty set  $S$  of ordinal numbers has a least element.*

PROOF:

$\langle 1 \rangle 1$ . PICK  $\beta \in S$

$\langle 1 \rangle 2$ . CASE:  $\beta \cap S = \emptyset$

PROOF: Then  $\beta$  is least in  $S$ .

$\langle 1 \rangle 3$ . CASE:  $\beta \cap S \neq \emptyset$

PROOF: The least element of  $\beta \cap S$  is least in  $S$ .

□

**Proposition 6.0.9.** *Any transitive set of ordinal numbers is an ordinal number.*

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

**Proposition 6.0.10.**  $\emptyset$  is an ordinal number.

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

**Definition 6.0.11.** We define  $0 = \emptyset$ .

**Definition 6.0.12** (Successor). The *successor* of a set  $a$  is the set  $a^+ := a \cup \{a\}$ .

**Proposition 6.0.13.** *A set  $a$  is a transitive set if and only if*

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

PROOF:

$\langle 1 \rangle 1$ . If  $a$  is a transitive set then  $\bigcup(a^+) = a$ .

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

$\langle 2 \rangle 2$ .  $\bigcup(a^+) \subseteq a$

$\langle 3 \rangle 1$ . LET:  $x \in \bigcup(a^+)$

PROVE:  $x \in a$

$\langle 3 \rangle 2$ . PICK  $y \in a^+$  such that  $x \in y$ .

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

$\langle 3 \rangle 4$ . CASE:  $y \in a$

PROOF: Then  $x \in a$  because  $a$  is a transitive set.

$\langle 3 \rangle 5$ . CASE:  $y = a$

PROOF: Then  $x \in a$  immediately.

$\langle 2 \rangle 3$ .  $a \subseteq \bigcup(a^+)$

PROOF: Since  $a \in a^+$ .

$\langle 1 \rangle 2$ . If  $\bigcup(a^+) = a$  then  $a$  is a transitive set.

$\langle 2 \rangle 1$ . ASSUME:  $\bigcup(a^+) = a$

$\langle 2 \rangle 2$ .  $\bigcup a \subseteq a$

PROOF:

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

$\langle 2 \rangle 3$ .  $a$  is a transitive set.

PROOF: Proposition 1.5.2.

□

**Proposition 6.0.14.** *For any set  $a$ , we have  $a$  is a transitive set if and only if  $a^+$  is a transitive set.*

PROOF:

$\langle 1 \rangle 1$ . If  $a$  is a transitive set then  $a^+$  is a transitive set.

PROOF: If  $a$  is a transitive set then  $\bigcup(a^+) = a \subseteq a^+$  by Proposition 6.0.13 and so  $a^+$  is a transitive set.

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

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

$\langle 2 \rangle 2$ . LET:  $x \in y \in a$

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

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

PROOF:  $\langle 2 \rangle 1$

$\langle 2 \rangle 5$ .  $x \neq a$

PROOF: From  $\langle 2 \rangle 2$  and the Axiom of Regularity.

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

□

**Definition 6.0.15.** We write 0 for  $\emptyset$ , 1 for  $\emptyset^+$ , 2 for  $\emptyset^{++}$ , etc.

**Proposition 6.0.16.** *Let  $2 = \{\emptyset, \{\emptyset\}\}$ . For any set  $A$  we have  $\mathcal{P}A \approx 2^A$ .*

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

**Proposition 6.0.17.** *For any ordinal number  $\alpha$  we have  $\alpha^+$  is an ordinal number.*

PROOF:

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

PROOF: Proposition 6.0.14.

$\langle 1 \rangle 2$ .  $\alpha^+$  is well-ordered by  $\in$ .

$\langle 2 \rangle 1$ . For all  $x, y, z \in \alpha^+$ , if  $x \in y \in z$  then  $x \in z$

$\langle 3 \rangle 1$ . CASE:  $z = \alpha$

PROOF: Then  $x \in \alpha$  since  $\alpha$  is a transitive set.

$\langle 3 \rangle 2$ . CASE:  $z \in \alpha$

PROOF: Then  $x \in z$  since  $\alpha$  is well-ordered by  $\in$ .

$\langle 2 \rangle 2$ . For all  $x, y \in \alpha^+$  we have  $x \in y$  or  $x = y$  or  $y \in x$

- ⟨3⟩1. CASE:  $x, y \in \alpha$   
PROOF: The result follows because  $\alpha$  is well-ordered by  $\in$ .
- ⟨3⟩2. CASE:  $x \in \alpha, y = \alpha$   
PROOF: Then  $x \in y$ .
- ⟨3⟩3. CASE:  $x = \alpha, y \in \alpha$   
PROOF: Then  $y \in x$ .
- ⟨3⟩4. CASE:  $x = \alpha, y = \alpha$   
PROOF: Then  $x = y$ .
- ⟨2⟩3. Every nonempty subset of  $\alpha^+$  has an  $\in$ -least element.
  - ⟨3⟩1. LET:  $S \subseteq \alpha^+$  be nonempty
  - ⟨3⟩2. CASE:  $S = \{\alpha\}$   
PROOF:  $\alpha$  is least in  $S$ .
  - ⟨3⟩3. CASE:  $S \neq \{\alpha\}$ 
    - ⟨4⟩1.  $S - \{\alpha\}$  is a nonempty subset of  $\alpha$
    - ⟨4⟩2. LET:  $\beta$  be least in  $S - \{\alpha\}$
    - ⟨4⟩3.  $\beta$  is least in  $S$ .

□

**Proposition 6.0.18.** *If  $A$  is a set of ordinal numbers then  $\bigcup A$  is an ordinal number.*

PROOF:

⟨1⟩1.  $\bigcup A$  is a transitive set.

PROOF: Proposition 1.5.3.

⟨1⟩2.  $\bigcup A$  is a set of ordinals.

□

**Theorem 6.0.19** (Burali-Forti). *The class of ordinal numbers is a proper class.*

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

**Theorem 6.0.20** (Hartogs). *For any set  $A$ , there exists an ordinal not dominated by  $A$ .*

PROOF:

⟨1⟩1. LET:  $\alpha$  be the class of all ordinals  $\beta$  such that  $\beta \prec A$

PROVE:  $\alpha$  is a set.

⟨1⟩2. LET:  $W = \{(B, R) \mid B \subseteq A, R \text{ is a well ordering on } B\}$

⟨1⟩3.  $\alpha$  is the class of the ordinals of the elements of  $W$ .

⟨2⟩1. For all  $(B, R) \in W$ , the ordinal of  $(B, R)$  is in  $\alpha$ .

⟨3⟩1. LET:  $(B, R) \in W$

⟨3⟩2. LET:  $\beta$  be the ordinal of  $(B, R)$

⟨3⟩3. LET:  $E : B \cong \beta$  be the canonical isomorphism.

⟨3⟩4. LET:  $i : B \hookrightarrow A$  be the inclusion

⟨3⟩5.  $i \circ E^{-1}$  is an injection  $\beta \rightarrow A$

⟨3⟩6.  $\beta \in \alpha$

⟨2⟩2. For all  $\beta \in \alpha$ , there exists  $(B, R) \in W$  such that  $\beta$  is the ordinal number of  $(B, R)$ .

- ⟨3⟩1. LET:  $\beta \in \alpha$
- ⟨3⟩2. PICK an injection  $f : \beta \rightarrow A$
- ⟨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.  $\beta$  is the ordinal number of  $(\text{ran } f, \leq)$
- ⟨1⟩4.  $\alpha$  is a set.
- PROOF: By an Axiom of Replacement.
- ⟨1⟩5.  $\alpha$  is an ordinal.
- PROOF: It is a transitive set of ordinals.
- ⟨1⟩6.  $\alpha \not\subseteq A$
- PROOF: Since  $\alpha \notin \alpha$ .

□

**Theorem 6.0.21** (Numeration Theorem). *Every set is equinumerous with some ordinal.*

PROOF:

- ⟨1⟩1. LET:  $A$  be any set.
- ⟨1⟩2. PICK an ordinal  $\alpha$  not dominated by  $A$ .
- ⟨1⟩3. PICK a choice function  $G$  for  $A$ .
- ⟨1⟩4. PICK  $e \notin A$
- ⟨1⟩5. LET:  $F : \alpha \rightarrow A \cup \{e\}$  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:  $\delta$  be least such that  $F(\delta) = e$
- ⟨1⟩8.  $F \upharpoonright \delta : \delta \approx A$

**Theorem 6.0.22** (Well-Ordering Theorem). *Any set can be well ordered.*

PROOF:

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

□

**Theorem 6.0.23** (Zorn's Lemma). *Let  $\mathcal{A}$  be a set such that, for every chain  $\mathcal{B} \subseteq \mathcal{A}$ , we have  $\bigcup \mathcal{B} \in \mathcal{A}$ . Then  $\mathcal{A}$  has a maximal element.*

PROOF:

$\langle 1 \rangle 1$ . PICK a well ordering  $<$  on  $\mathcal{A}$ .

$\langle 1 \rangle 2$ . LET:  $F : \mathcal{A} \rightarrow 2$  be the function defined by transfinite recursion by:

$$F(A) = \begin{cases} 1 & \text{if } A \text{ includes every set } B < A \text{ for which } F(B) = 1 \\ 0 & \text{otherwise} \end{cases}$$

$\langle 1 \rangle 3$ . LET:  $\mathcal{C} = \{A \in \mathcal{A} \mid F(A) = 1\}$

PROVE:  $\bigcup \mathcal{C}$  is a maximal element of  $\mathcal{A}$

$\langle 1 \rangle 4$ . For all  $A \in \mathcal{A}$ , we have  $A \in \mathcal{C}$  iff  $\forall B < A. B \in \mathcal{C} \Rightarrow B \subseteq A$

$\langle 1 \rangle 5$ .  $\mathcal{C}$  is a chain.

$\langle 2 \rangle 1$ . LET:  $A, A' \in \mathcal{C}$

$\langle 2 \rangle 2$ . ASSUME: w.l.o.g.  $A \leq A'$

$\langle 2 \rangle 3$ .  $A \subseteq A'$

PROOF: By  $\langle 1 \rangle 4$

$\langle 1 \rangle 6$ .  $\bigcup \mathcal{C} \in \mathcal{A}$

$\langle 1 \rangle 7$ .  $\bigcup \mathcal{C}$  is maximal in  $\mathcal{A}$ .

$\langle 2 \rangle 1$ . LET:  $A \in \mathcal{A}$  and  $\bigcup \mathcal{C} \subseteq A$

$\langle 2 \rangle 2$ .  $A \in \mathcal{C}$

PROOF: By  $\langle 1 \rangle 4$  since  $\forall B \in \mathcal{C}. B \subseteq A$ .

$\langle 2 \rangle 3$ .  $A \subseteq \bigcup \mathcal{C}$

$\langle 2 \rangle 4$ .  $A = \bigcup \mathcal{C}$

□

**Proposition 6.0.24** (Teichmüller-Tukey Lemma). *Let  $\mathcal{A}$  be a nonempty set such that, for every  $B$ , we have  $B \in \mathcal{A}$  if and only if every finite subset of  $B$  is a member of  $\mathcal{A}$ . Then  $\mathcal{A}$  has a maximal element.*

PROOF:

$\langle 1 \rangle 1$ . For every chain  $\mathcal{B} \subseteq \mathcal{A}$ , we have  $\bigcup \mathcal{B} \in \mathcal{A}$

$\langle 2 \rangle 1$ . LET:  $\mathcal{B} \subseteq \mathcal{A}$  be a chain.

$\langle 2 \rangle 2$ . Every finite subset of  $\bigcup \mathcal{B}$  is a member of  $\mathcal{A}$ .

$\langle 3 \rangle 1$ . LET:  $C$  be a finite subset of  $\bigcup \mathcal{B}$ .

$\langle 3 \rangle 2$ . PICK  $B \in \mathcal{B}$  such that  $C \subseteq B$ .

$\langle 3 \rangle 3$ .  $B \in \mathcal{A}$

$\langle 3 \rangle 4$ . Every finite subset of  $B$  is in  $\mathcal{A}$ .

$\langle 3 \rangle 5$ .  $C \in \mathcal{A}$

$\langle 2 \rangle 3$ .  $\bigcup \mathcal{B} \in \mathcal{A}$ .

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

PROOF: Zorn's lemma.

□



## Chapter 7

# Cardinal Numbers

### 7.1 Cardinal Numbers

**Definition 7.1.1** (Cardinality). For any set  $A$ , the *cardinality*  $|A|$  of  $A$  is the least ordinal equinumerous with  $A$ .

**Proposition 7.1.2.** For any sets  $A$  and  $B$ , we have  $A \approx B$  iff  $|A| = |B|$ .

PROOF: Easy.  $\square$

**Definition 7.1.3** (Addition). Given cardinal numbers  $\kappa$  and  $\lambda$ , we define  $\kappa + \lambda$  to be  $|A \cup B|$  where  $A$  and  $B$  are disjoint sets of cardinality  $\kappa$  and  $\lambda$  respectively.

We prove this is well-defined.

PROOF:

$\langle 1 \rangle 1$ . 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 7.1.4.** For any cardinal number  $\kappa$ , we have  $\kappa + 0 = \kappa$ .

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

**Theorem 7.1.5** (Associative Law for Addition). For any cardinal numbers  $\kappa$ ,  $\lambda$ ,  $\mu$  we have  $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$ .

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

**Proposition 7.1.6.** For any cardinal numbers  $\kappa$  and  $\lambda$  we have  $\kappa + \lambda = \lambda + \kappa$ .

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

**Definition 7.1.7** (Multiplication). For  $\kappa$  and  $\lambda$  cardinal numbers, we define  $\kappa\lambda$  to be the cardinal number of  $A \times B$ , where  $|A| = \kappa$  and  $|B| = \lambda$ .

We prove this is well-defined.

PROOF: If  $f : A \approx A'$  and  $g : B \approx B'$  then the function that maps  $(a, b)$  to  $(f(a), g(b))$  is a bijection  $A \times B \approx A' \times B'$ .  $\square$

**Proposition 7.1.8.** For any cardinal number  $\kappa$  we have  $\kappa \cdot 0 = 0$ .

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

**Proposition 7.1.9.** For any cardinal number  $\kappa$  we have  $\kappa \cdot 1 = \kappa$ .

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

**Theorem 7.1.10** (Distributive Law). For any cardinal numbers  $\kappa$ ,  $\lambda$  and  $\mu$ , we have  $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$ .

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

**Theorem 7.1.11** (Associative Law for Multiplication). For any cardinal numbers  $\kappa$ ,  $\lambda$  and  $\mu$ , we have  $\kappa(\lambda\mu) = (\kappa\lambda)\mu$ .

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

**Theorem 7.1.12** (Commutative Law for Multiplication). For any cardinal numbers  $\kappa$  and  $\lambda$ , we have  $\kappa\lambda = \lambda\kappa$ .

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

**Theorem 7.1.13.** For any cardinal numbers  $\kappa$  and  $\lambda$ , if  $\kappa\lambda = 0$  then  $\kappa = 0$  or  $\lambda = 0$ .

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

**Definition 7.1.14** (Exponentiation). Given cardinal numbers  $\kappa$  and  $\lambda$ , we define  $\kappa^\lambda$  to be  $|A^B|$ , where  $|A| = \kappa$  and  $|B| = \lambda$ .

We prove this is well-defined.

PROOF: If  $f : A \approx A'$  and  $g : B \approx B'$ , then the function that maps  $h : B \rightarrow A$  to  $f \circ h \circ g^{-1}$  is a bijection  $A^B \approx A'^{B'}$ .  $\square$

**Proposition 7.1.15.** For any cardinal numbers  $\kappa$ ,  $\lambda$  and  $\mu$ ,

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

PROOF: The function that maps  $f : A \times B \rightarrow C$  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 7.1.16.** For any cardinal numbers  $\kappa$ ,  $\lambda$  and  $\mu$ ,

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



PROOF: The function  $f : A^C \times B^C \rightarrow (A \times B)^C$  with  $f(g, h)(c) = (g(c), h(c))$  is a bijection.  $\square$

**Proposition 7.1.17.** *For any cardinal numbers  $\kappa$ ,  $\lambda$  and  $\mu$ , we have*

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

PROOF: If  $B \cap C = \emptyset$ , then  $f : A^B \times A^C \rightarrow A^{B \cup C}$  given by  $f(g, h)(b) = g(b)$  and  $f(g, h)(c) = h(c)$  is a bijection.  $\square$

**Proposition 7.1.18.** *For any cardinal number  $\kappa$ , we have  $\kappa^0 = 1$ .*

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

**Proposition 7.1.19.** *For any cardinal number  $\kappa$ , we have  $\kappa^1 = \kappa$ .*

PROOF: For any sets  $A$  and  $B$ , if  $B = \{b\}$  then the function  $f : A \rightarrow A^B$  with  $f(a)(b) = a$  is a bijection.  $\square$

**Proposition 7.1.20.** *For any non-zero cardinal number  $\kappa$  we have  $0^\kappa = 0$ .*

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

**Proposition 7.1.21.** *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  $a \in X$ .  $\square$

**Corollary 7.1.21.1.** *For any cardinal number  $\kappa$  we have  $2^\kappa \neq \kappa$ .*

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

## 7.2 Ordering on Cardinal Numbers

**Definition 7.2.1** (Domination). A set  $A$  is *dominated* by a set  $B$ ,  $A \preceq B$ , iff there exists an injection  $A \rightarrow B$ .

**Definition 7.2.2.** Given cardinal numbers  $\kappa$  and  $\lambda$ , we write  $\kappa \leq \lambda$  iff  $A \preceq B$  where  $|A| = \kappa$  and  $|B| = \lambda$ . We write  $\kappa < \lambda$  iff  $\kappa \leq \lambda$  and  $\kappa \neq \lambda$ .

We prove this is well-defined.

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

**Proposition 7.2.3.** *For any cardinal number  $\kappa$  we have  $\kappa \leq \kappa$ .*

PROOF: For any set  $A$  we have  $\text{id}_A$  is an injection  $A \rightarrow A$ .  $\square$

**Proposition 7.2.4.** *For any cardinal numbers  $\kappa$ ,  $\lambda$  and  $\mu$ , if  $\kappa \leq \lambda$  and  $\lambda \leq \mu$  then  $\kappa \leq \mu$ .*

PROOF: If  $f : A \rightarrow B$  and  $g : B \rightarrow C$  are injective then so is  $g \circ f : A \rightarrow C$ .  $\square$

**Proposition 7.2.5.** *For any cardinal number  $\kappa$  we have  $0 \leq \kappa$ .*

PROOF: For any set  $A$ , we have  $\emptyset$  is an injection  $\emptyset \rightarrow A$ .  $\square$

**Proposition 7.2.6.** *For any cardinal number  $\kappa$  we have  $\kappa < 2^\kappa$ .*

PROOF: The function that maps  $a$  to  $\{a\}$  is an injection  $A \rightarrow \mathcal{P}A$ , so  $\kappa \leq 2^\kappa$ . They are unequal by Cantor's Theorem.  $\square$

**Corollary 7.2.6.1.** *There is no largest cardinal number.*

**Proposition 7.2.7.** *For any cardinal numbers  $\kappa, \lambda, \mu$ , 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.  $\square$

**Proposition 7.2.8.** *For any cardinal numbers  $\kappa, \lambda, \mu$ , 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.  $\square$

**Proposition 7.2.9.** *For any cardinal numbers  $\kappa, \lambda, \mu$ , 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.  $\square$

**Proposition 7.2.10.** *For any cardinal numbers  $\kappa, \lambda, \mu$ , if  $\kappa \leq \lambda$  and  $\mu$  and  $\kappa$  are not both 0, then  $\mu^\kappa \leq \mu^\lambda$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $A, B$  and  $C$  be sets with  $A$  and  $C$  not both empty.

$\langle 1 \rangle 2$ . LET:  $f : A \rightarrow B$  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:  $C \neq \emptyset$

$\langle 2 \rangle 1$ . PICK  $c \in C$

$\langle 2 \rangle 2$ . LET:  $g : C^A \rightarrow C^B$  be the function  $g(h)(f(a)) = h(a)$ ,  $g(h)(b) = c$  if  $b \notin f(A)$

$\langle 2 \rangle 3$ .  $g$  is an injection.

$\square$

**Proposition 7.2.11.** *Let  $\mathcal{A}$  be a set such that  $\forall X \in \mathcal{A}. |X| \leq \kappa$ . Then*

$$|\bigcup \mathcal{A}| \leq |\mathcal{A}|^\kappa.$$

PROOF:

$\langle 1 \rangle 1$ . For  $X \in \mathcal{A}$ , choose a surjection  $f_X : \kappa \rightarrow X$ .

$\langle 1 \rangle 2$ . Define  $g : \mathcal{A} \times \kappa \rightarrow \bigcup \mathcal{A}$  by  $g(X, \alpha) = f_X(\alpha)$

$\langle 1 \rangle 3$ .  $g$  is surjective.

$\square$

## Chapter 8

# Natural Numbers

### 8.1 Inductive Sets

**Definition 8.1.1** (Inductive). A set  $I$  is *inductive* iff  $\emptyset \in I$  and  $\forall x \in I. x^+ \in I$ .

**Definition 8.1.2** (Natural Number). A *natural number* is a set that belongs to every inductive set.

**Theorem 8.1.3.** *The class  $\mathbb{N}$  of natural numbers is a set.*

PROOF:

$\langle 1 \rangle 1$ . PICK an inductive set  $I$ .

PROOF: Axiom of Infinity.

$\langle 1 \rangle 2$ .  $\mathbb{N} \subseteq I$

□

**Theorem 8.1.4.**  *$\mathbb{N}$  is inductive, and is a subset of every other inductive set.*

PROOF:

$\langle 1 \rangle 1$ .  $\mathbb{N}$  is inductive.

$\langle 2 \rangle 1$ .  $0 \in \mathbb{N}$

PROOF: Since 0 is a member of every inductive set.

$\langle 2 \rangle 2$ .  $\forall n \in \mathbb{N}. n^+ \in \mathbb{N}$

$\langle 3 \rangle 1$ . LET:  $n \in \mathbb{N}$

$\langle 3 \rangle 2$ . LET:  $I$  be any inductive set.

PROVE:  $n^+ \in I$

$\langle 3 \rangle 3$ .  $n \in I$

PROOF:  $\langle 3 \rangle 1$ ,  $\langle 3 \rangle 2$

$\langle 3 \rangle 4$ .  $n^+ \in I$

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

$\langle 1 \rangle 2$ .  $\mathbb{N}$  is a subset of every inductive set.

PROOF: Immediate from definitions.

□

**Corollary 8.1.4.1** (Induction Principle for  $\mathbb{N}$ ). *Any inductive subset of  $\mathbb{N}$  coincides with  $\mathbb{N}$ .*

**Theorem 8.1.5.** *Every natural number except 0 is the successor of some natural number.*

PROOF: Trivially by induction.  $\square$

**Proposition 8.1.6.** *Every natural number is a transitive set.*

PROOF:

$\langle 1 \rangle 1$ . 0 is a transitive set.

PROOF: Vacuously, if  $x \in y \in 0$  then  $x \in 0$ .

$\langle 1 \rangle 2$ . For every natural number  $n$ , if  $n$  is a transitive set then  $n^+$  is a transitive set.

PROOF: Proposition 6.0.14.

$\square$

**Proposition 8.1.7.** *For natural numbers  $m$  and  $n$ , if  $m^+ = n^+$  then  $m = n$ .*

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

$$m = \bigcup (m^+) \quad (\text{Proposition 6.0.13})$$

$$= \bigcup (n^+)$$

$$= n \quad (\text{Proposition 6.0.13})$$

**Proposition 8.1.8.**  *$\mathbb{N}$  is a transitive set.*

PROOF:

$\langle 1 \rangle 1$ .  $0 \subseteq \mathbb{N}$

$\langle 1 \rangle 2$ .  $\forall n \in \mathbb{N}. n \subseteq \mathbb{N} \Rightarrow n^+ \subseteq \mathbb{N}$

$\langle 1 \rangle 3$ .  $\forall n \in \mathbb{N}. n \subseteq \mathbb{N}$

PROOF: From  $\langle 1 \rangle 1$  and  $\langle 1 \rangle 2$  by induction.

$\square$

**Proposition 8.1.9** (Dependent Choice). *Let  $A$  be a nonempty set and  $R$  a relation on  $A$  such that  $\forall x \in A. \exists y \in A. (y, x) \in R$ . Then there exists a function  $f : \mathbb{N} \rightarrow A$  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  $f(n+1) = F(\{y \in A \mid (y, f(n)) \in R\})$ .

$\square$

## 8.2 Ordering on $\mathbb{N}$

**Proposition 8.2.1.** *For any natural numbers  $m$  and  $n$ , we have  $m < n$  if and only if  $m^+ < n^+$ .*

PROOF:

- $\langle 1 \rangle 1$ . For any natural numbers  $m$  and  $n$ , if  $m < n$  then  $m^+ < n^+$ .
- $\langle 2 \rangle 1$ . For any natural number  $m$ , if  $m < 0$  then  $m^+ < 0^+$   
 PROOF: Vacuous.
- $\langle 2 \rangle 2$ . For any natural number  $n$ , if  $\forall m < n. m^+ < n^+$  then  $\forall m < n^+. m^+ < n^{++}$ 
  - $\langle 3 \rangle 1$ . LET:  $m < n^+$
  - $\langle 3 \rangle 2$ .  $m < n$  or  $m = n$
  - $\langle 3 \rangle 3$ . CASE:  $m < n$ 
    - $\langle 4 \rangle 1$ .  $m^+ < n^+$   
 PROOF: Induction hypothesis.
    - $\langle 4 \rangle 2$ .  $m^+ < n^{++}$
  - $\langle 3 \rangle 4$ . CASE:  $m = n$   
 PROOF:  $m^+ = n^+ < n^{++}$ .
- $\langle 1 \rangle 2$ . For any natural numbers  $m$  and  $n$ , if  $m^+ < n^+$  then  $m < n$ .
  - $\langle 2 \rangle 1$ . We never have  $m^+ < 0^+$ .
    - $\langle 3 \rangle 1$ .  $m^+ \not< 0$
    - $\langle 3 \rangle 2$ .  $m^+ \neq 0$
    - $\langle 3 \rangle 3$ .  $m^+ \not< 0^+$
  - $\langle 2 \rangle 2$ . For any natural number  $n$ , if  $\forall m. m^+ < n^+ \Rightarrow m < n$ , then  $\forall m. m^+ < n^{++} \Rightarrow m < n^+$ .
    - $\langle 3 \rangle 1$ . LET:  $n$  be a natural number.
    - $\langle 3 \rangle 2$ . ASSUME:  $\forall m. m^+ < n^+ \Rightarrow m < n$
    - $\langle 3 \rangle 3$ . LET:  $m$  be a natural number.
    - $\langle 3 \rangle 4$ . ASSUME:  $m^+ < n^{++}$
    - $\langle 3 \rangle 5$ .  $m^+ < n^+$  or  $m^+ = n^+$
    - $\langle 3 \rangle 6$ . CASE:  $m^+ < n^+$ 
      - $\langle 4 \rangle 1$ .  $m < n$   
 PROOF: Induction hypothesis.
      - $\langle 4 \rangle 2$ .  $m < n^+$
    - $\langle 3 \rangle 7$ . CASE:  $m^+ = n^+$   
 PROOF:  $m = n < n^+$  by Proposition 8.1.7.

□

**Corollary 8.2.1.1.** *For natural numbers  $m$  and  $n$ , we have  $m \leq n$  if and only if  $m \subseteq n$ .*

PROOF:

- $\langle 1 \rangle 1$ . If  $m \leq n$  then  $m \subseteq n$ 
  - $\langle 2 \rangle 1$ . ASSUME:  $m \leq n$
  - $\langle 2 \rangle 2$ . LET:  $p \in m$
  - $\langle 2 \rangle 3$ . CASE:  $m < n$   
 PROOF: Then  $p \in n$  by Proposition 8.1.6.
  - $\langle 2 \rangle 4$ . CASE:  $m = n$   
 PROOF: Then  $p \in n$  immediately.
- $\langle 1 \rangle 2$ . If  $m \subseteq n$  then  $m \leq n$ 
  - $\langle 2 \rangle 1$ . ASSUME:  $m \subseteq n$

⟨2⟩2.  $n \not\leq m$

PROOF: If  $n < m$  then  $n \in n$  contradicting the Axiom of Regularity.

⟨2⟩3.  $m \leq n$

PROOF: By trichotomy.

□

### 8.3 Recursion

**Theorem 8.3.1.** *Let  $<$  be a linear ordering on  $A$ . Then  $<$  is a well ordering on  $A$  if and only if there does not exist a function  $f : \mathbb{N} \rightarrow A$  such that  $\forall n \in \mathbb{N}. f(n+1) < f(n)$ .*

PROOF:

⟨1⟩1. If there exists a function  $f : \mathbb{N} \rightarrow A$  such that  $\forall n \in \mathbb{N}. f(n+1) < f(n)$  then  $<$  is not a well ordering on  $A$ .

PROOF:  $\text{ran } f$  is a nonempty subset of  $A$  with no least element.

⟨1⟩2. If  $<$  is not a well ordering on  $A$  then there exists a function  $f : \mathbb{N} \rightarrow A$  such that  $\forall n \in \mathbb{N}. f(n+1) < f(n)$ .

⟨2⟩1. ASSUME:  $<$  is not a well ordering on  $A$ .

⟨2⟩2. PICK a nonempty subset  $B \subseteq A$  that has no least element.

⟨2⟩3.  $\forall x \in B. \exists y \in B. y < x$

⟨2⟩4. Choose a function  $g : B \rightarrow B$  such that  $\forall x \in B. g(x) < x$

⟨2⟩5. PICK  $b \in B$

⟨2⟩6. Define  $f : \mathbb{N} \rightarrow A$  recursively by  $f(0) = b$  and  $\forall n \in \mathbb{N}. f(n+1) = g(f(n))$

⟨2⟩7.  $\forall n \in \mathbb{N}. f(n+1) < f(n)$

□

### 8.4 Cardinality

**Theorem 8.4.1** (Schröder-Bernstein). *For any cardinal numbers  $\kappa$  and  $\lambda$ , if  $\kappa \leq \lambda$  and  $\lambda \leq \kappa$  then  $\kappa = \lambda$ .*

PROOF:

⟨1⟩1. LET:  $f : A \rightarrow B$  and  $g : B \rightarrow A$  be injections.

PROVE:  $A \approx B$

⟨1⟩2. Define the sets  $C_n$  for  $n \in \mathbb{N}$  by recursion:

$$C_0 := A - \text{ran } g$$

$$C_{n+1} := g(f(C_n))$$

⟨1⟩3. LET:  $h : A \rightarrow B$  be the function

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

⟨1⟩4. For  $n \in \mathbb{N}$ ,

LET:  $D_n = f(C_n)$

⟨1⟩5.  $h$  is injective.

- ⟨2⟩1. LET:  $x, x' \in A$
- ⟨2⟩2. ASSUME:  $h(x) = h(x')$
- ⟨2⟩3. CASE:  $x \in C_m$  and  $x' \in C_n$   
 PROOF: We have  $f(x) = f(x')$  so  $x = x'$ .
- ⟨2⟩4. CASE:  $x \in C_m$  and  $\forall n. x' \notin C_n$   
 PROOF: We have  $f(x) = g^{-1}(x')$  so  $x' = g(f(x)) \in C_{m+1}$  which is a contradiction.
- ⟨2⟩5. CASE:  $\forall n. x \notin C_n$  and  $x' \in C_n$   
 PROOF: Similar.
- ⟨2⟩6. CASE:  $\forall n. x \notin C_n$  and  $\forall n. x' \notin C_n$   
 PROOF: We have  $g^{-1}(x) = g^{-1}(x')$  so  $x = x'$ .
- ⟨1⟩6.  $h$  is surjective.
- ⟨2⟩1. LET:  $y \in B$
- ⟨2⟩2. CASE:  $y \in D_n$ 
  - ⟨3⟩1. PICK  $x \in C_n$  such that  $y = f(x)$
  - ⟨3⟩2.  $y = h(x)$
- ⟨2⟩3. CASE:  $\forall n. y \notin D_n$ 
  - ⟨3⟩1.  $\forall n. g(y) \notin C_n$
  - ⟨3⟩2.  $h(g(y)) = y$

□

**Definition 8.4.2** (Finite). A set is *finite* iff it is equinumerous to some natural number; otherwise it is *infinite*.

**Theorem 8.4.3** (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
 
$$\hat{f}(p) = f(n)$$

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

$\langle 3 \rangle 3.$   $\hat{f}$  is one-to-one  
 $\langle 3 \rangle 4.$   $\text{ran } \hat{f} = n$   
 PROOF:  $\langle 2 \rangle 1$   
 $\langle 3 \rangle 5.$   $\text{ran } f = n + 1$   
 $\langle 1 \rangle 4.$  For every natural number  $n$ ,  $P(n)$ .  
 $\square$

**Corollary 8.4.3.1.** *No finite set is equinumerous to a proper subset of itself.*

**Corollary 8.4.3.2.** *Every natural number is a cardinal number.*

PROOF: For any natural number  $n$ , we have that  $n$  is the least ordinal such that  $n \approx n$ .  $\square$

**Corollary 8.4.3.3.**  $\mathbb{N}$  is infinite.

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

**Proposition 8.4.4.** *If  $C$  is a proper subset of a natural number  $n$ , then there exists  $m < n$  such that  $C \approx m$ .*

PROOF:

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

**Corollary 8.4.4.1.** *Any subset of a finite set is finite.*

**Proposition 8.4.5.** *For any natural numbers  $m$  and  $n$  we have  $m + n^+ = (m + n)^+$ .*

PROOF:

$\langle 1 \rangle 1.$  PICK disjoint sets  $A$  and  $B$  of cardinalities  $m$  and  $n$ .



$\langle 1 \rangle 2$ . PICK an element  $e \notin A \cup B$

$\langle 1 \rangle 3$ .  $A \cup B \cup \{e\} \approx m + n^+$

$\langle 1 \rangle 4$ .  $A \cup B \cup \{e\} \approx (m + n)^+$

□

**Proposition 8.4.6.** *For any natural numbers  $m$  and  $n$  we have  $m + n$  is a natural number.*

PROOF: Induction on  $n$ . □

**Proposition 8.4.7.** *For any natural numbers  $m$  and  $n$  we have  $m \cdot n^+ = mn + m$ .*

PROOF:

$\langle 1 \rangle 1$ . PICK sets  $A$  and  $B$  of cardinality  $m$  and  $n$  respectively.

$\langle 1 \rangle 2$ . PICK  $e \notin B$

$\langle 1 \rangle 3$ .  $A \times (B \cup \{e\}) = (A \times B) \cup (A \times \{e\})$

□

**Corollary 8.4.7.1.** *For any natural numbers  $m$  and  $n$ , we have  $mn$  is a natural number.*

**Corollary 8.4.7.2.** *If  $A$  and  $B$  are finite sets then  $A \times B$  is finite.*

**Proposition 8.4.8.** *The union of a finite set of finite sets is finite.*

PROOF: By induction on the number of elements. □

**Proposition 8.4.9.**  $\mathbb{N}^2 \approx \mathbb{N}$

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

**Corollary 8.4.9.1.** *For any natural numbers  $m$  and  $n$ , we have  $m^n$  is a natural number.*

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

**Corollary 8.4.9.2.** *If  $A$  and  $B$  are finite sets then  $A^B$  are finite.*

**Definition 8.4.10.** Let  $\aleph_0 := |\mathbb{N}|$ .

**Proposition 8.4.11.** *For any infinite cardinal  $\kappa$  we have  $\aleph_0 \leq \kappa$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $A$  be an infinite set.

PROVE:  $\aleph_0 \preceq A$

$\langle 1 \rangle 2$ . 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  $g(m) \neq g(n)$ .

□

## 8.5 Countable Sets

**Definition 8.5.1** (Countable). A set  $A$  is *countable* iff  $|A| \leq \aleph_0$ .

**Theorem 8.5.2.** *The union of a countable set of countable sets is countable.*

PROOF: Proposition 7.2.11.  $\square$

## 8.6 Arithmetic

**Definition 8.6.1** (Even). A natural number  $n$  is *even* iff there exists  $m \in \mathbb{N}$  such that  $n = 2m$ .

**Definition 8.6.2** (Odd). A natural number  $n$  is *odd* iff there exists  $p \in \mathbb{N}$  such that  $n = 2p + 1$ .

**Proposition 8.6.3** (Division Algorithm). *Let  $m$  be a natural number and  $d$  a nonzero natural number. Then there exist natural numbers  $q$  and  $r$  such that  $m = dq + r$  and  $r < d$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $d$  be a nonzero natural number.

$\langle 1 \rangle 2$ .  $\exists q, r. 0 = dq + r \wedge r < d$

PROOF: Take  $q = r = 0$ .

$\langle 1 \rangle 3$ . For any natural number  $m$ , if  $\exists q, r. m = dq + r \wedge r < d$  then  $\exists q, r. m^+ = dq + r \wedge r < d$

$\langle 2 \rangle 1$ . LET:  $m$  be a natural number.

$\langle 2 \rangle 2$ . ASSUME:  $m = dq + r$  and  $r < d$

$\langle 2 \rangle 3$ .  $r^+ \leq d$

$\langle 2 \rangle 4$ . CASE:  $r^+ < d$

PROOF: In this case we have  $m^+ = dq + r^+$ .

$\langle 2 \rangle 5$ . CASE:  $r^+ = d$

PROOF: In this case we have  $m^+ = dq^+ + 0$ .

$\square$

**Proposition 8.6.4.** *Every natural number is either even or odd.*

PROOF:

$\langle 1 \rangle 1$ . 0 is even.

PROOF:  $0 = 2 \times 0$ .

$\langle 1 \rangle 2$ . For any natural number  $n$ , if  $n$  is either even or odd then  $n^+$  is either even or odd.

PROOF:

$\langle 2 \rangle 1$ . LET:  $n \in \mathbb{N}$

$\langle 2 \rangle 2$ . If  $n$  is even then  $n^+$  is odd.

PROOF: If  $n = 2p$  then  $n^+ = 2p + 1$ .

$\langle 2 \rangle 3$ . If  $n$  is odd then  $n^+$  is even.

PROOF: If  $n = 2p + 1$  then  $n^+ = 2(p + 1)$ .

□

**Proposition 8.6.5.** *No natural number is both even and odd.*

PROOF:

⟨1⟩1. 0 is not odd.

PROOF: For any  $p$  we have  $2p + 1 = (2p)^+ \neq 0$ .

⟨1⟩2. For any natural number  $n$ , if  $n$  is not both even and odd, then  $n^+$  is not both even and odd.

⟨2⟩1. LET:  $n$  be a natural number.

⟨2⟩2. If  $n^+$  is even then  $n$  is odd.

⟨3⟩1. ASSUME:  $n^+$  is even.

⟨3⟩2. PICK  $p$  such that  $n^+ = 2p$

⟨3⟩3.  $p \neq 0$

PROOF: Since  $n^+ \neq 0$ .

⟨3⟩4. PICK  $q$  such that  $p = q^+$

PROOF: Theorem 8.1.5.

⟨3⟩5.  $n^+ = 2q + 2$

PROOF: ⟨3⟩2, ⟨3⟩4.

⟨3⟩6.  $n = 2q + 1$

PROOF: Proposition 8.1.7, ⟨3⟩5

⟨3⟩7.  $n$  is odd.

⟨2⟩3. If  $n^+$  is odd then  $n$  is even.

⟨3⟩1. ASSUME:  $n^+$  is odd.

⟨3⟩2. PICK  $p$  such that  $n^+ = 2p + 1$

⟨3⟩3.  $n = 2p$

PROOF: Proposition 8.1.7, ⟨3⟩2

⟨3⟩4.  $n$  is even.

□

**Proposition 8.6.6.** *For any natural numbers  $m$  and  $n$ , we have  $m < n$  if and only if there exists  $p \in \mathbb{N}$  such that  $n = m + p^+$ .*

PROOF:

⟨1⟩1. For any natural numbers  $m$  and  $p$  we have  $m < m + p^+$ .

⟨2⟩1.  $\forall m. m < m + 0^+$

PROOF: Since  $m \in m^+ = m + 0^+$ .

⟨2⟩2. For any natural number  $p$ , if  $\forall m. m < m + p^+$  then  $\forall m. m < m + p^{++}$

PROOF: If  $m \in m + p^+$  then  $m \in (m + p^+)^+ = m + p^{++}$ .

⟨1⟩2. For any natural numbers  $m$  and  $n$ , if  $m < n$  then there exists  $p$  such that  $n = m + p^+$ .

⟨2⟩1.  $\forall m < 0. \exists p. 0 = m + p^+$

PROOF: Vacuous.

⟨2⟩2. For any natural number  $n$ , if  $\forall m < n. \exists p. n = m + p^+$ , then  $\forall m < n^+. \exists p. n^+ = m + p^+$ .

⟨3⟩1. LET:  $n$  be a natural number.

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

- $\langle 3 \rangle 3$ . LET:  $m < n^+$
- $\langle 3 \rangle 4$ .  $m < n$  or  $m = n$
- $\langle 3 \rangle 5$ . CASE:  $m < n$ 
  - $\langle 4 \rangle 1$ . PICK  $p$  such that  $n = m + p^+$
  - $\langle 4 \rangle 2$ .  $n^+ = m + p^{++}$
- $\langle 3 \rangle 6$ . CASE:  $m = n$

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

□

**Theorem 8.6.7.** For natural numbers  $m$ ,  $n$  and  $p$ , if  $m + p = n + p$  then  $m = n$ .

PROOF: By trichotomy. □

**Theorem 8.6.8.** For natural numbers  $m$ ,  $n$  and  $p$ , if  $m < n$  and  $p \neq 0$  then  $mp < np$ .

PROOF:

$\langle 1 \rangle 1$ . LET:  $m$  and  $n$  be natural numbers.

$\langle 1 \rangle 2$ . ASSUME:  $m < n$

PROVE:  $\forall p. mp^+ < np^+$

$\langle 1 \rangle 3$ .  $m0^+ < n0^+$

PROOF: Proposition ??.

$\langle 1 \rangle 4$ . For any natural number  $p$ , if  $mp < np$  then  $mp^+ < np^+$

PROOF:

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

□

**Corollary 8.6.8.1.** For natural numbers  $m$ ,  $n$  and  $p$ , if  $p \neq 0$  then  $m < n$  if and only if  $mp < np$ .

PROOF: Proposition 5.0.29. □

**Corollary 8.6.8.2.** For natural numbers  $m$ ,  $n$  and  $p$ , if  $mp = np$  and  $p \neq 0$  then  $m = n$ .

PROOF: By trichotomy. □

**Proposition 8.6.9.** 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  $m + n < p + q$ .

$\langle 1 \rangle 2$ . If  $q < n$  then  $m < p$ .

PROOF: Similar.

□

**Proposition 8.6.10.** *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:

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

□

## 8.7 Sequences

**Definition 8.7.1** (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 8.7.2.** *If  $A$  is countable then  $A^*$  is countable.*

PROOF: For any  $n$ , the set  $A^n$  is countable, and  $A^*$  is equinumerous with  $\bigcup_n A^n$ .

□



## Chapter 9

# Group Theory

### 9.1 Groups

**Definition 9.1.1** (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 9.1.2.** *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 9.1.3.** We write  $x^{-1}$  for the inverse of  $x$ .

**Proposition 9.1.4.** *In any group, if  $ab = ac$  then  $b = c$ .*

PROOF:

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

□

## 9.2 Abelian Groups

**Definition 9.2.1** (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 10

# Ring Theory

### 10.1 Rings

**Definition 10.1.1** (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 10.1.2.** *In any commutative ring,  $0x = 0$ .*

PROOF:

$$\begin{aligned}(0 + 0)x &= 0x \\ \therefore 0x + 0x &= 0x + 0 \\ \therefore 0x &= 0 && \text{(Proposition 9.1.4)} \square\end{aligned}$$

**Proposition 10.1.3.** *In any commutative ring,  $(-a)b = -(ab)$ .*

PROOF:

$$\begin{aligned}ab + (-a)b &= (a + (-a))b \\ &= 0b \\ &= 0 && \text{(Proposition 10.1.2)} \square\end{aligned}$$

### 10.2 Ordered Rings

**Definition 10.2.1** (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 10.2.2.** *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 10.2.3.** *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  $z = (x + y)/2$ .  $\square$

### 10.3 Integral Domains

**Definition 10.3.1** (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 10.3.2.** *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 10.3.3** (Ordered Integral Domain). An *ordered integral domain* is an ordered commutative ring that is an integral domain.

# Chapter 11

## Field Theory

### 11.1 Fields

**Definition 11.1.1** (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 11.1.2.** *Every field is an integral domain.*

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

**Proposition 11.1.3.** *In any field  $F$ , we have  $F - \{0\}$  is an Abelian group under multiplication.*

PROOF: Immediate from the definition.  $\square$

**Definition 11.1.4** (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 10.3.2.

□

$\langle 1 \rangle 2$ . 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 11.1.5.** 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 11.1.6** (Characteristic Zero). A field  $F$  has *characteristic 0* iff  $0 \notin N(F)$ .

**Proposition 11.1.7.** 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 11.1.8.** In any field  $F$ , let

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

**Definition 11.1.9.** In any field  $F$ , let

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

**Proposition 11.1.10.**  $Q(F)$  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 11.1.11.** 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.  $\phi$  is a bijection.  
 PROOF: Similar to Proposition 11.1.7.
- (1)3.  $\forall x, y \in N(F). \phi(x+y) = \phi(x) + \phi(y)$   
 PROOF: Induction on  $y$ .
- (1)4.  $\forall x, y \in N(F). \phi(xy) = \phi(x)\phi(y)$   
 PROOF: Induction on  $y$ .
- (1)5. Extend  $\phi$  to a bijection  $I(F) \cong I(G)$  such that  $\forall x, y \in I(F). \phi(x+y) = \phi(x) + \phi(y)$  and  $\forall x, y \in I(F). \phi(xy) = \phi(x)\phi(y)$
- (2)1. Define  $\phi(0) = 0$  and  $\phi(-x) = -\phi(x)$  for  $x \in N(F)$
- (3)1.  $0 \notin N(F)$
- (3)2. For all  $x \in N(F)$  we have  $-x \notin N(F)$   
 PROOF: Then we would have  $x + -x = 0 \in N(F)$ .
- (3)3. For all  $x \in N(F)$  we have  $-x \neq 0$
- (2)2. For all  $x, y \in I(F)$  we have  $\phi(x+y) = \phi(x) + \phi(y)$   
 PROOF: Case analysis on  $x$  and  $y$ .
- (2)3. For all  $x, y \in I(F)$  we have  $\phi(xy) = \phi(x)\phi(y)$   
 PROOF: Case analysis on  $x$  and  $y$ .
- (1)6. Extend  $\phi$  to a bijection  $Q(F) \cong Q(G)$  such that  $\forall x, y \in Q(F). \phi(x+y) = \phi(x) + \phi(y)$  and  $\forall x, y \in Q(F). \phi(xy) = \phi(x)\phi(y)$
- (2)1. Define  $\phi(x/y) = \phi(x)/\phi(y)$
- (1)7.  $\phi$  is unique.
- (2)1. LET:  $\theta$  satisfy the theorem.
- (2)2. For all  $x \in N(F)$  we have  $\theta(x) = \phi(x)$
- (2)3. For all  $x \in I(F)$  we have  $\theta(x) = \phi(x)$
- (2)4. For all  $x \in Q(F)$  we have  $\theta(x) = \phi(x)$

□

## 11.2 Ordered Fields

**Definition 11.2.1** (Ordered Field). An *ordered field* is an ordered commutative ring that is a field.

**Proposition 11.2.2.** Every ordered field  $F$  has characteristic 0.

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

**Proposition 11.2.3.** 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 11.2.3.1.** Let  $F$  and  $G$  be ordered fields. Let  $\phi$  be the unique field isomorphism between  $Q(F)$  and  $Q(G)$ . Then  $\phi$  is an ordered field isomorphism.

**Definition 11.2.4** (Archimedean). An ordered field  $F$  is *Archimedean* iff

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

**Proposition 11.2.5.** *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 11.2.6.** *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 11.2.5.

$\langle 2 \rangle 2$ .  $ny > 1 + nx$

$\langle 2 \rangle 3$ . 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 11.2.7** (Complete). An ordered field  $F$  is *complete* iff every nonempty subset of  $F$  bounded above has a least upper bound.

**Proposition 11.2.8.** *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 11.2.9.** *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.  $\phi$  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.  $b^2 = a$   
 $\square$

**Theorem 11.2.10** (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 11.2.3.1.

- ⟨1⟩2.  $Q(F)$  intersects every interval in  $F$ .

PROOF: Proposition 11.2.6.

- ⟨1⟩3.  $Q(G)$  intersects every interval in  $G$ .

PROOF: Proposition 11.2.6.

- ⟨1⟩4. PICK an order isomorphism  $\psi : F \cong G$  that extends  $\phi$ .

PROOF: Theorem 5.0.22.

- ⟨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 11.1.11.

- $\langle 2 \rangle 2. \theta \text{ is strictly monotone.}$

- $\langle 3 \rangle 1. \text{LET: } x, y \in F \text{ with } x < y$

- $\langle 3 \rangle 2. y - x > 0$

- $\langle 3 \rangle 3. \text{PICK } z \in F \text{ such that } z^2 = y - x$

- $\langle 3 \rangle 4. \theta(z)^2 = \theta(y) - \theta(x)$

- $\langle 3 \rangle 5. \theta(y) - \theta(x) > 0$

- $\langle 3 \rangle 6. \theta(x) < \theta(y)$

- $\langle 2 \rangle 3. \theta = \psi$

PROOF: By the uniqueness of  $\psi$ .

□



## Chapter 12

# Number Systems

### 12.1 The Integers

**Definition 12.1.1.** 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: Corollary ??.

□

**Definition 12.1.2** (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 12.1.3.** *Addition on  $\mathbb{Z}$  is commutative.*

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

□

**Proposition 12.1.4.** *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 12.1.5.** *Given natural numbers  $m$  and  $n$ , we have  $[(m, 0)] = [(n, 0)]$  iff  $m = n$ .*

PROOF: Immediate from definitions.  $\square$

**Definition 12.1.6.** We identify any natural number  $n$  with the integer  $[(n, 0)]$ .

**Proposition 12.1.7.** *Addition on integers agrees with addition on natural numbers.*

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

**Proposition 12.1.8.** *For all  $a \in \mathbb{Z}$  we have  $a + 0 = a$ .*

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

**Proposition 12.1.9.** *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 12.1.10.** *The integers form an Abelian group under addition.*

PROOF: Proposition 12.1.3, 12.1.4, 12.1.8, 12.1.9.  $\square$

**Definition 12.1.11.** 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: Corollary ??.

$\square$

**Proposition 12.1.12.** *Multiplication on integers agrees with multiplication on natural numbers.*

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

**Proposition 12.1.13.** *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 12.1.14.** *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 12.1.15.** *Multiplication distributes over addition.*

PROOF:

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

**Proposition 12.1.16.** *For any integer  $a$  we have  $a1 = a$ .*

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

**Proposition 12.1.17.** *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:  $m < n$

$\langle 2 \rangle 1$ .  $p \not< q$

PROOF: If  $p < q$  then  $mq + np < mp + nq$  by Proposition 8.6.10.

$\langle 2 \rangle 2$ .  $q \not< p$

PROOF: If  $q < p$  then  $mp + nq < mq + np$  by Proposition 8.6.10.

$\langle 2 \rangle 3$ .  $p = q$

PROOF: By trichotomy.

$\langle 1 \rangle 6$ . CASE:  $n < m$

PROOF: Similar.

$\square$

**Proposition 12.1.18.** *The integers  $\mathbb{Z}$  form an integral domain.*

PROOF: Propositions 12.1.13, 12.1.14, 12.1.15, 12.1.16, 12.1.17, 12.1.10.  $\square$

**Definition 12.1.19.** 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:

$$m + q < n + p \Leftrightarrow m + n' + q < n + n' + p \quad (\text{Theorem ??})$$

$$\Leftrightarrow m' + n + q < n + n' + p$$

$$\Leftrightarrow m' + q < n' + p \quad (\text{Theorem ??})$$

$$\Leftrightarrow m' + q + p' < n' + p + p' \quad (\text{Theorem ??})$$

$$\Leftrightarrow m' + q' + p < n' + p + p'$$

$$\Leftrightarrow m' + q' < n' + p' \quad (\text{Theorem ??}) \square$$

**Proposition 12.1.20.** *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 12.1.21.**  *$<$  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: Theorem ??.

$\langle 1 \rangle 3$ .  $<$  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 12.1.22** (Positive). An integer  $a$  is *positive* iff  $a > 0$ .

**Theorem 12.1.23.** *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 5.0.29.

□

**Proposition 12.1.24.** *Let  $a$ ,  $b$  and  $c$  be integers. If  $0 < c$ , then  $a < b$  if and only if  $ac < bc$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $c = [(r, s)]$

$\langle 1 \rangle 2$ . ASSUME:  $0 < c$

$\langle 1 \rangle 3$ .  $s < r$

$\langle 1 \rangle 4$ . For all integers  $a$  and  $b$ , if  $a < b$  then  $ac < bc$

$\langle 2 \rangle 1$ . LET:  $a = [(m, n)]$ ,  $b = [(p, q)]$ .

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

$\langle 2 \rangle 3$ .  $m + q < n + p$

$\langle 2 \rangle 4$ .  $(m + q)r + (p + n)s < (m + q)s + (p + n)r$

PROOF: Proposition 8.6.10,  $\langle 1 \rangle 3$ ,  $\langle 2 \rangle 3$ .

$\langle 2 \rangle 5$ .  $mr + ns + ps + qr < ms + nr + pr + qs$

$\langle 2 \rangle 6$ .  $[(mr + ns, ms + nr)] < [(pr + qs, ps + qr)]$

$\langle 2 \rangle 7$ .  $ac < bc$

$\langle 1 \rangle 5$ . For all integers  $a$  and  $b$ , if  $ac < bc$  then  $a < b$

PROOF: From  $\langle 1 \rangle 4$  and Proposition 5.0.29.

□

**Proposition 12.1.25.** *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  $k = b + 1$ .

□

## 12.2 The Rationals

**Definition 12.2.1** (Rational Numbers). The set  $\mathbb{Q}$  of *rational numbers* is the field of fractions over the integers.

**Proposition 12.2.2.** *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 12.2.3.** *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 12.2.4.** *Multiplication on the rationals agrees with multiplication on the integers.*

PROOF:  $[(a, 1)][(b, 1)] = [(ab, 1)]$   $\square$

**Definition 12.2.5.** 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 12.2.6.** *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 12.2.7.** *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 12.2.8.** *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 12.2.8.1.** *For any rational  $r$ , we have  $r < 0$  if and only if  $0 < -r$ .*

**Definition 12.2.9** (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 12.2.10.** *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 12.2.10.1.** *The rationals form an ordered field.*

**Proposition 12.2.11.** *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 12.1.25.

$\langle 1 \rangle 3$ .  $r < pk$

□

**Proposition 12.2.12.**  $\mathbb{Q} \approx \mathbb{N}$

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. □

## 12.3 The Real Numbers

**Definition 12.3.1** (Cauchy Sequence). A *Cauchy sequence* is a sequence  $(q_n)$  of rationals such that, for every positive rational  $\epsilon$ , there exists  $k \in \mathbb{N}$  such that  $\forall m, n > k. |q_m - q_n| < \epsilon$ .

**Definition 12.3.2** (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 12.3.3.** 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 12.3.4.** 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.

(1)4. If  $q < r$  then  $q \downarrow \neq r \downarrow$

PROOF: We have  $q \in r \downarrow$  and  $q \notin q \downarrow$ .

(1)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 12.3.5.** Define the ordering  $<$  on  $\mathbb{R}$  by:  $x < y$  iff  $x \subsetneq y$ .

**Proposition 12.3.6.** *The ordering on the reals agrees with the ordering on the rationals.*

PROOF:

(1)1. LET:  $q, r \in \mathbb{Q}$

(1)2. LET:  $q \downarrow = \{s \in \mathbb{Q} \mid s < q\}$ .

(1)3. LET:  $r \downarrow = \{s \in \mathbb{Q} \mid s < r\}$ .

PROVE:  $q < r$  iff  $q \downarrow \subsetneq r \downarrow$

(1)4. If  $q < r$  then  $q \downarrow \subsetneq r \downarrow$

(2)1. ASSUME:  $q < r$

(2)2.  $q \downarrow \subseteq r \downarrow$

PROOF: If  $s < q$  then  $s < r$ .

(2)3.  $q \downarrow \neq r \downarrow$

PROOF: Proposition 12.3.4.

(1)5. If  $q \downarrow \subsetneq r \downarrow$  then  $q < r$

(2)1. ASSUME:  $q \downarrow \subsetneq r \downarrow$

(2)2. PICK  $s \in r \downarrow$  such that  $s \notin q \downarrow$

(2)3.  $q \leq s < r$

□

**Proposition 12.3.7.** *The ordering  $<$  is a linear ordering on  $\mathbb{R}$ .*

PROOF:

(1)1.  $<$  is irreflexive.

PROOF: No set is a proper subset of itself.

(1)2.  $<$  is transitive.

PROOF: Since the relationship  $\subsetneq$  is transitive on the class of all sets.

(1)3.  $<$  is total.

(2)1. LET:  $x, y$  be Dedekind cuts.

(2)2. ASSUME:  $x \not\subseteq y$

PROVE:  $y \subsetneq x$

(2)3. PICK  $q \in x$  such that  $q \notin y$

(2)4. LET:  $r \in y$

PROVE:  $r \in x$

(2)5.  $q \not\leq r$

PROOF: Since  $y$  is closed downwards.

(2)6.  $r < q$

(2)7.  $r \in x$

PROOF: Since  $x$  is closed downwards.

□

**Proposition 12.3.8.** *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 12.3.9** (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 12.3.10.** *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 12.3.11.** *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 12.3.12.** *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 12.3.13.** *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 12.3.14.** For  $x \in \mathbb{R}$ , define  $-x := \{q \in \mathbb{Q} \mid \exists r > q. -r \notin x\}$ .

**Proposition 12.3.15.** *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 12.3.16.** *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 12.2.11.
  - $\langle 2 \rangle 3$ .  $q_1 < q_0 + kp$
  - $\langle 2 \rangle 4$ .  $q_0 + kp \notin x$
- $\langle 1 \rangle 3$ . 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 12.3.17.** *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 12.3.16.
  - $\langle 2 \rangle 4$ . 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 12.3.17.1.** *The reals form an Abelian group under addition.*

**Proposition 12.3.18.** *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 9.1.4.

⟨1⟩3.  $\forall x, y, z \in \mathbb{R}. x < y \Rightarrow x + z < y + z$

⟨1⟩4. Q.E.D.

PROOF: Proposition 5.0.29.

□

**Definition 12.3.19** (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 12.3.20** (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 12.3.21.** *Multiplication is commutative.*

PROOF: Immediate from definition. □

**Proposition 12.3.22.** *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 12.3.23.** *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 12.3.24.** *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 12.3.25.** *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 12.2.11.  
 ⟨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 12.3.26.** *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 12.3.25.
  - ⟨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  $x$



PROOF: There are countably many integer polynomials, each with finitely many roots.  $\square$

**Corollary 12.3.30.1.** *There are uncountably many transcendental numbers.*

**Proposition 12.3.31.** *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 12.3.32.** *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 13

# Complex Analysis

**Definition 13.0.1.** For  $p \geq 1$ , let  $l^p$  be the set of all sequences of complex numbers  $(x_n)$  such that  $\sum_{n=1}^{\infty} |x_n|^p < \infty$ .

**Proposition 13.0.2.** If  $(x_n), (y_n) \in l^p$  then  $(x_n + y_n) \in l^p$ .

PROOF:

$\langle 1 \rangle 1$ . LET:  $(x_n), (y_n) \in l^p$

$\langle 1 \rangle 2$ .  $\sum_{n=1}^{\infty} |x_n + y_n|^p \leq 2^p (\sum_{n=1}^{\infty} |x_n|^p + \sum_{n=1}^{\infty} |y_n|^p)$

PROOF:

$\langle 2 \rangle 1$ . For all  $n \in \mathbb{N}$  we have  $|x_n + y_n|^p \leq 2^p (|x_n|^p + |y_n|^p)$ .

PROOF:

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

□

**Theorem 13.0.3** (Hölder's Inequality). Let  $p$  and  $q$  be reals such that  $p > 1$ ,  $q > 1$  and  $1/p + 1/q = 1$ . Let  $(x_n) \in l^p$  and  $(y_n) \in l^q$ . Then

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

PROOF:

$\langle 1 \rangle 1$ . ASSUME: w.l.o.g. neither  $(x_n)$  nor  $(y_n)$  are all zero.

$\langle 1 \rangle 2$ . For  $0 \leq x \leq 1$  we have

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

$\langle 2 \rangle 1$ . LET:  $f(x) = x/p + 1/q - x^{1/p}$

$\langle 2 \rangle 2$ .  $f'(x) = 1/p(1 - x^{(1-p)/p})$

$\langle 2 \rangle 3$ .  $f'(x) \geq 0$  for all  $x \in [0, 1]$

$\langle 2 \rangle 4$ .  $f$  is a monotonically decreasing function on  $[0, 1]$

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

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

- ⟨2⟩1. CASE:  $a^p \leq b^q$   
 ⟨3⟩1.  $ab^{-q/p} \leq \frac{1}{p} \frac{a^p}{b^q} + \frac{1}{q}$   
 PROOF: Substituting  $x = a^p/b^q$  in ⟨1⟩2.  
 ⟨3⟩2.  $ab^{1-q} \leq \frac{1}{p} \frac{a^p}{b^q} + \frac{1}{q}$   
 PROOF: From ⟨3⟩1 since  $1 - q = -q/p$ .  
 ⟨3⟩3.  $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$   
 PROOF: Multiplying ⟨3⟩2 by  $b^q$ .  
 ⟨2⟩2. CASE:  $b^q \leq a^p$   
 PROOF: Similar.

- ⟨1⟩4. For any integers  $1 \leq j \leq n$ , we have

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

PROOF: From ⟨1⟩3 substituting

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

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

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

PROOF:

$$\frac{\sum_{j=1}^n |x_j| |y_j|}{(\sum_{k=1}^n |x_k|^p)^{1/p} (\sum_{k=1}^n |y_k|^q)^{1/q}} \leq \frac{1}{p} + \frac{1}{q} \quad (\text{Summing } \langle 1 \rangle 4 \text{ from } j = 1 \text{ to } n)$$

$$= 1$$

- ⟨1⟩6.

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

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

□

**Theorem 13.0.4** (Minkowski's Inequality). *Let  $p \geq 1$ . Let  $(x_n), (y_n) \in l^p$ . Then*

$$\left( \sum_{n=1}^{\infty} |x_n + y_n|^p \right)^{1/p} \leq \left( \sum_{n=1}^{\infty} |x_n|^p \right)^{1/p} + \left( \sum_{n=1}^{\infty} |y_n|^p \right)^{1/p}$$

PROOF:

- ⟨1⟩1. CASE:  $p = 1$

PROOF: This is just the Triangle Inequality.

- ⟨1⟩2. CASE:  $p > 1$

- ⟨2⟩1. LET:  $q = p/(p-1)$

⟨2⟩2.

$$\begin{aligned} \sum_{n=1}^{\infty} |x_n + y_n|^p &\leq \left( \sum_{n=1}^{\infty} |x_n|^p \right)^{1/p} \left( \sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \\ &\quad + \left( \sum_{n=1}^{\infty} |y_n|^p \right)^{1/p} \left( \sum_{n=1}^{\infty} |x_n + y_n|^{q(p-1)} \right)^{1/q} \end{aligned}$$

PROOF:

⟨3⟩1.  $(|x_n + y_n|^{p-1}) \in l^q$

PROOF:

$$\sum_{n=1}^{\infty} |x_n + y_n|^{(p-1)q} = \sum_{n=1}^{\infty} |x_n + y_n|^p \quad (\langle 2 \rangle 2)$$

$$< \infty$$

(Proposition 13.0.2)

⟨3⟩2. Q.E.D.

PROOF:

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

⟨2⟩3.

$$\sum_{n=1}^{\infty} |x_n + y_n|^p \leq \left\{ \left( \sum_{n=1}^{\infty} |x_n|^p \right)^{1/p} + \left( \sum_{n=1}^{\infty} |y_n|^p \right)^{1/p} \right\} \left( \sum_{n=1}^{\infty} |x_n + y_n|^p \right)^{1/q}$$

⟨3⟩1.  $q(p-1) = p$

PROOF: ⟨2⟩2

⟨3⟩2. Q.E.D.

PROOF: From ⟨2⟩2, ⟨3⟩1.

□



**Part I**

**Linear Algebra**



# Chapter 14

## Vector Spaces

### 14.1 Vector Spaces

**Definition 14.1.1** (Vector Space). Let  $K$  be either  $\mathbb{R}$  or  $\mathbb{C}$ . A *vector space* over  $K$  is a triple  $(V, +, \cdot)$  such that:

- $V$  is a nonempty set, whose elements are called *vectors*;
- $+: V^2 \rightarrow V$
- $\cdot: K \times V \rightarrow V$

such that the following hold for all  $u, v, w \in V$  and  $\alpha, \beta \in K$ :

1.  $u + v = v + u$
2.  $u + (v + w) = (u + v) + w$
3. For every  $u, v \in V$  there exists  $w \in V$  such that  $u + w = v$
4.  $\alpha(\beta v) = (\alpha\beta)v$
5.  $(\alpha + \beta)v = \alpha v + \beta v$
6.  $\alpha(u + v) = \alpha u + \alpha v$
7.  $1v = v$

Elements of  $K$  are called *scalars*.

We write *real vector space* for 'vector space over  $\mathbb{R}$ ', and *complex vector space* for 'vector space over  $\mathbb{C}$ '.

**Proposition 14.1.2.** *Let  $K$  be either  $\mathbb{R}$  and  $\mathbb{C}$ . The set  $\{0\}$  is a vector space over  $K$  under the unique functions  $+: \{0\}^2 \rightarrow \{0\}$ ,  $\cdot: K \times \{0\} \rightarrow \{0\}$ .*

PROOF: Each axiom holds trivially because  $x = y$  holds for all  $x, y \in \{0\}$ .  $\square$

**Proposition 14.1.3.** *The set  $\mathbb{R}$  is a real vector space under real addition and real multiplication.*

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

**Proposition 14.1.4.** *The set  $\mathbb{C}$  is a real vector space under complex addition and complex multiplication.*

PROOF: TODO

**Proposition 14.1.5.** *The set  $\mathbb{C}$  is a complex vector space under complex addition and complex multiplication.*

PROOF: TODO

**Proposition 14.1.6.** *Let  $K$  be either  $\mathbb{R}$  or  $\mathbb{C}$ . Let  $\{V_i\}_{i \in I}$  be a family of vector spaces over  $K$ . Then  $\prod_{i \in I} V_i$  is a vector space over  $K$  under the operations given by*

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

PROOF: Each axiom follows from the corresponding axiom in  $V_i$ .  $\square$

**Corollary 14.1.6.1.** *Let  $V$  be a vector space over  $K$ . For any set  $I$ , we have  $V^I$  is a vector space over  $K$ .*

**Corollary 14.1.6.2.** *Let  $n \in \mathbb{Z}_+$ . Then  $\mathbb{R}^n$  is a real vector space, and  $\mathbb{C}^n$  is both a real and a complex vector space, under*

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

**Proposition 14.1.7.** *Let  $V$  be a vector space over  $K$ . Then there exists a unique  $0 \in V$  such that, for all  $v \in V$ , we have  $v + 0 = v$ .*

PROOF:

$\langle 1 \rangle 1$ . There exists  $0 \in V$  such that  $\forall v \in V. v + 0 = v$

$\langle 2 \rangle 1$ . Pick  $v \in V$

$\langle 2 \rangle 2$ . Pick  $0 \in V$  such that  $v + 0 = v$

PROOF: Axiom 3.

$\langle 2 \rangle 3$ . For all  $u \in V$ , we have  $u + 0 = u$

$\langle 3 \rangle 1$ . LET:  $u \in V$

$\langle 3 \rangle 2$ . PICK  $u' \in V$  such that  $v + u' = u$

PROOF: Axiom 3.

$\langle 3 \rangle 3$ .  $u + 0 = u$

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



$\langle 1 \rangle 2$ . If  $0, 0' \in V$  are such that  $\forall v \in V. v + 0 = v$  and  $\forall v \in V. v + 0' = v$ , then  $0 = 0'$ .

$\langle 2 \rangle 1$ . LET:  $0, 0' \in V$

$\langle 2 \rangle 2$ . ASSUME:  $\forall v \in V. v + 0 = v$

$\langle 2 \rangle 3$ . ASSUME:  $\forall v \in V. v + 0' = v$

$\langle 2 \rangle 4$ .  $0 = 0'$

$$0 = 0 + 0' \quad (\langle 2 \rangle 2)$$

$$= 0' \quad (\langle 2 \rangle 3)$$

□

**Proposition 14.1.8.** *Let  $V$  be a vector space. For any  $v \in V$ , there exists a unique  $-v \in V$  such that  $v + (-v) = 0$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $v \in V$

$\langle 1 \rangle 2$ . There exists  $-v \in V$  such that  $v + (-v) = u$

PROOF: Axiom 3.

$\langle 1 \rangle 3$ . If  $v + x = 0$  and  $v + y = 0$  then  $x = y$

$\langle 2 \rangle 1$ . ASSUME:  $v + x = 0$

$\langle 2 \rangle 2$ . ASSUME:  $v + y = 0$

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

PROOF:

$$x = x + 0 \quad (\text{Proposition 14.1.7})$$

$$= x + v + y \quad (\langle 2 \rangle 2)$$

$$= 0 + y \quad (\langle 2 \rangle 1)$$

$$= y \quad (\text{Proposition 14.1.7})$$

□

**Proposition 14.1.9.** *Let  $V$  be a vector space. For any  $u, v \in V$ , there exists a unique  $u - v \in V$  such that  $v + (u - v) = u$ , namely  $u - v = u + (-v)$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $u, v \in V$

$\langle 1 \rangle 2$ .  $v + (u + (-v)) = u$

PROOF:

$$v + u + (-v) = u + 0 \quad (\text{Proposition 14.1.8})$$

$$= u \quad (\text{Proposition 14.1.7})$$

$\langle 1 \rangle 3$ . For all  $x \in V$ , if  $v + x = u$  then  $x = u + (-v)$ .

$\langle 2 \rangle 1$ . LET:  $x \in V$

$\langle 2 \rangle 2$ . ASSUME:  $v + x = u$

$\langle 2 \rangle 3$ .  $x = u + (-v)$

PROOF:

$$u + (-v) = v + x + (-v) \quad (\langle 2 \rangle 2)$$

$$= x + 0 \quad (\text{Proposition 14.1.8})$$

$$= x \quad (\text{Proposition 14.1.7})$$

□

**Proposition 14.1.10.** *Let  $V$  be a vector space over  $K$ . Let  $u, v, w \in V$ . If  $u + v = u + w$  then  $v = w$ .*

PROOF:

$\langle 1 \rangle 1.$  ASSUME:  $u + v = u + w$

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

PROOF:

$$\begin{aligned}
 v &= v + 0 && \text{(Proposition 14.1.7)} \\
 &= v + u + (-u) && \text{(Proposition 14.1.8)} \\
 &= w + u + (-u) && ((1)1) \\
 &= w + 0 && \text{(Proposition 14.1.8)} \\
 &= w && \text{(Proposition 14.1.7)}
 \end{aligned}$$

**Proposition 14.1.11.** *Let  $V$  be a vector space over  $K$ . Let  $\lambda \in K$ . Then  $\lambda 0 = 0$ .*

PROOF:

$\langle 1 \rangle 1.$   $\lambda 0 + \lambda 0 = \lambda 0 + 0$

PROOF:

$$\begin{aligned}
 \lambda 0 + \lambda 0 &= \lambda(0 + 0) && \text{(Axiom 6)} \\
 &= \lambda 0 && \text{(Proposition 14.1.7)}
 \end{aligned}$$

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

PROOF: Proposition 14.1.10.

□

**Proposition 14.1.12.** *Let  $V$  be a vector space over  $K$ . Let  $\lambda \in K$  and  $v \in V$ . If  $\lambda v = 0$  then  $\lambda = 0$  or  $v = 0$ .*

PROOF:

$\langle 1 \rangle 1.$  ASSUME:  $\lambda \neq 0$

$\langle 1 \rangle 2.$  ASSUME:  $\lambda v = 0$

$\langle 1 \rangle 3.$   $v = 0$

PROOF:

$$\begin{aligned}
 v &= 1v && \text{(Axiom 7)} \\
 &= \lambda^{-1}\lambda v \\
 &= \lambda^{-1}0 && ((1)2) \\
 &= 0
 \end{aligned}$$

□

**Proposition 14.1.13.** *Let  $V$  be a vector space over  $K$ . For all  $v \in V$  we have  $0v = 0$ .*

PROOF:

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

$$\begin{aligned}
0v + 0 &= 0v && \text{(Proposition 14.1.7)} \\
&= (0 + 0)v \\
&= 0v + 0v && \text{(Axiom 5)}
\end{aligned}$$

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

PROOF: Proposition 14.1.10,  $\langle 1 \rangle 1.$

□

**Proposition 14.1.14.** *Let  $V$  be a vector space over  $K$ . Let  $v \in V$ . Then  $(-1)v = -v$ .*

PROOF:

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

PROOF:

$$\begin{aligned}
v + (-1)v &= 1v + (-1)v && \text{(Axiom 7)} \\
&= (1 + (-1))v && \text{(Axiom 5)} \\
&= 0v \\
&= 0 && \text{(Proposition 14.1.13)}
\end{aligned}$$

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

PROOF: Proposition 14.1.8.

□

## 14.2 Subspaces

**Definition 14.2.1** (Subspace). Let  $V$  be a vector space over  $K$  and  $U \subseteq V$ . Then  $U$  is a *subspace* of  $V$  iff  $\forall \alpha, \beta \in K. \forall u, v \in U. \alpha u + \beta v \in U$ . It is a *proper* subspace iff in addition  $U \neq V$ .

**Proposition 14.2.2.** *Let  $V$  be a vector space over  $K$  and  $U$  a subspace of  $V$ . Then  $U$  is a vector space over  $K$  under the restrictions of the operations of  $V$ .*

PROOF: Each of the axioms follows from the corresponding axiom in  $V$ . For axiom 3, we have if  $u, v \in U$  then  $v - u = 1v + (-1)u \in U$ . □

**Proposition 14.2.3.** *Every vector space is a subspace of itself.*

PROOF: Trivial. □

**Proposition 14.2.4.** *Let  $\Omega$  be a subset of  $\mathbb{R}^N$ . Let  $\mathcal{C}(\Omega)$  be the set of all continuous functions  $\Omega \rightarrow \mathbb{C}$ . Then  $\mathcal{C}(\Omega)$  is a subspace of  $\mathbb{C}^\Omega$ .*

PROOF: If  $f, g : \Omega \rightarrow \mathbb{C}$  are continuous then so is  $\alpha f + \beta g$ . □

**Proposition 14.2.5.** *Let  $\Omega$  be an open set in  $\mathbb{R}^N$ . Let  $\mathcal{C}^k(\Omega)$  be the set of all continuous functions  $\Omega \rightarrow \mathbb{C}$  with continuous partial derivatives of order  $k$ . Then  $\mathcal{C}^k(\Omega)$  is a subspace of  $\mathbb{C}^\Omega$ .*

PROOF: If  $f, g : \Omega \rightarrow \mathbb{C}$  have continuous partial derivatives of order  $k$  then so does  $\alpha f + \beta g$ .  $\square$

**Proposition 14.2.6.** *Let  $\Omega$  be an open set in  $\mathbb{R}^N$ . Let  $\mathcal{C}^\infty(\Omega)$  be the set of all infinitely differentiable functions  $\Omega \rightarrow \mathbb{C}$ . Then  $\mathcal{C}^\infty(\Omega)$  is a subspace of  $\mathbb{C}^\Omega$ .*

PROOF: If  $f, g : \Omega \rightarrow \mathbb{C}$  are infinitely differentiable then so is  $\alpha f + \beta g$ .  $\square$

**Proposition 14.2.7.** *Let  $\Omega$  be an open set in  $\mathbb{R}^N$ . Let  $\mathcal{P}(\Omega)$  be the set of all polynomials in  $N$  variables considered as functions  $\Omega \rightarrow \mathbb{C}$ . Then  $\mathcal{P}(\Omega)$  is a subspace of  $\mathbb{C}^\Omega$ .*

PROOF: If  $f, g : \Omega \rightarrow \mathbb{C}$  are polynomials in  $N$  variables then so is  $\alpha f + \beta g$ .  $\square$

**Proposition 14.2.8.** *Let  $V$  be a vector space and  $U_1, U_2$  subspaces of  $V$ . If  $U_1 \subseteq U_2$  then  $U_1$  is a subspace of  $U_2$ .*

PROOF: Trivial.  $\square$

**Proposition 14.2.9.** *Let  $V$  be a vector space over  $K$ . The intersection of a set of subspaces of  $V$  is a subspace of  $V$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\mathcal{U}$  be a set of subspaces of  $V$ .

$\langle 1 \rangle 2$ . LET:  $u, v \in \bigcap \mathcal{U}$  and  $\lambda, \mu \in K$

$\langle 1 \rangle 3$ .  $\lambda u + \mu v \in \bigcap \mathcal{U}$

$\langle 2 \rangle 1$ . LET:  $U \in \mathcal{U}$

$\langle 2 \rangle 2$ .  $u, v \in U$

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

$\langle 2 \rangle 3$ .  $\lambda u + \beta v \in U$

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

$\square$

**Proposition 14.2.10.** *The set of all bounded complex sequences is a proper subspace of  $\mathbb{C}^\mathbb{N}$ .*

PROOF: If  $(x_n)$  and  $(y_n)$  are bounded then so is  $(\lambda x_n + \mu y_n)$ .  $\square$

**Proposition 14.2.11.** *The set of all convergent complex sequences is a proper subspace of the space of all bounded complex sequences.*

PROOF: If  $(x_n)$  and  $(y_n)$  converge then so does  $(\lambda x_n + \mu y_n)$ .  $\square$

**Proposition 14.2.12.** *The set  $l^p$  of all sequences  $(x_n)$  in  $\mathbb{C}$  such that  $\sum_n |x_n|^p < \infty$  is a subspace of  $\mathbb{C}^\mathbb{N}$ .*

PROOF: It is closed under addition by Proposition 13.0.2, and it is easy to see that it is closed under scalar multiplication.  $\square$

## 14.3 Linear Independence and Bases

**Definition 14.3.1** (Linear Combination). Let  $V$  be a vector space over  $K$ . Let  $v, v_1, \dots, v_n \in V$ . Then  $v$  is a *linear combination* of  $v_1, \dots, v_n$  iff there exist scalars  $\lambda_1, \dots, \lambda_n \in K$  such that

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

**Definition 14.3.2** (Linearly Independent). Let  $V$  be a vector space over  $K$ . Let  $A \subseteq V$ . Then  $A$  is *linearly independent* iff, for all  $\lambda_1, \dots, \lambda_n \in K$  and  $v_1, \dots, v_n \in A$ , if  $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$  then  $\lambda_1 = \dots = \lambda_n = 0$ .

**Definition 14.3.3** (Span). Let  $V$  be a vector space over  $K$  and  $A \subseteq V$ . The *span* of  $A$ , or the subspace of  $V$  *spanned* by  $A$ , is the set of all linear combinations of vectors in  $A$ .

**Proposition 14.3.4.** Let  $V$  be a vector space over  $K$  and  $A \subseteq V$ . Then  $\text{span } A$  is a subspace of  $V$ .

PROOF: Given  $\alpha, \beta \in K$  and  $\lambda_1 u_1 + \dots + \lambda_m u_m, \mu_1 v_1 + \dots + \mu_n v_n \in \text{span } A$ , we have

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

**Definition 14.3.5** (Basis). Let  $V$  be a vector space over  $K$  and  $B \subseteq V$ . Then  $B$  is a *basis* for  $V$  iff  $B$  is linearly independent and  $\text{span } B = V$ .

**Definition 14.3.6** (Finite Dimensional). A vector space is *finite dimensional* iff there exists a finite basis; otherwise it is *infinite dimensional*.

**Proposition 14.3.7.** In a finite dimensional space, any two bases have the same size.

TODO

**Definition 14.3.8** (Dimension). The *dimension* of a finite dimensional vector space  $V$ ,  $\dim V$ , is the number of vectors in any basis.

**Proposition 14.3.9.** Let  $K$  be either  $\mathbb{R}$  or  $\mathbb{C}$ . Then  $K^n$  as a vector space over  $K$  has dimension  $n$ .

PROOF: The vectors with one component 1 and all other components 0 form a basis.  $\square$

**Proposition 14.3.10.** As a real vector space,  $\mathbb{C}^n$  has dimension  $2n$ .

PROOF: The vectors with one component either 1 or  $i$  and all other components 0 form a basis.  $\square$

**Proposition 14.3.11.** *Let  $\Omega$  be a nonempty open set in  $\mathbb{R}^n$ . The space  $\mathcal{C}(\Omega)$  is infinite dimensional.*

PROOF: Let  $\pi_1 : \mathbb{R}^n \rightarrow \mathbb{R}$  be the first projection. The functions  $1, \pi_1(x), \pi_1(x)^2, \pi_1(x)^3, \dots$  form an infinite linearly independent set in  $\mathcal{C}(\Omega)$ .  $\square$

**Proposition 14.3.12.** *The spaces  $\mathcal{C}^k(\mathbb{R}^n)$  and  $\mathcal{C}^\infty(\mathbb{R}^n)$  are infinite dimensional.*

PROOF: The monomials  $1, x, x^2, \dots$  form an infinite linearly independent set.  $\square$

## 14.4 Linear Mappings

**Definition 14.4.1** (Kernel). Let  $U$  and  $V$  be vector spaces and  $T : U \rightarrow V$ . The *kernel* of  $T$  is

$$\ker T := \{u \in U \mid T(u) = 0\} .$$

**Definition 14.4.2** (Linear Mapping). Let  $U$  and  $V$  be vector spaces over  $K$ . A function  $L : U \rightarrow V$  is a *linear mapping* iff  $\forall x, y \in U. \forall \alpha, \beta \in K. L(\alpha x + \beta y) = \alpha L(x) + \beta L(y)$ .

**Proposition 14.4.3.** *Let  $U$  and  $V$  be vector spaces over  $K$ . The set of linear mappings from  $U$  to  $V$  is a subspace of  $V^U$ .*

## 14.5 Eigenvalues and Eigenvectors

**Definition 14.5.1** (Eigenvalue and Eigenvector). Let  $V$  be a vector space over  $K$ . Let  $A : V \rightarrow V$  be a linear transformation. Let  $v \in V$  and  $\lambda \in K$ . Then  $v$  is an *eigenvector* of  $A$  with *eigenvalue*  $\lambda$  iff  $A(v) = \lambda v$ .

# Chapter 15

## Normed Spaces

**Definition 15.0.1** (Norm). Let  $K$  be either  $\mathbb{R}$  or  $\mathbb{C}$ . Let  $V$  be a vector space over  $K$ . A *norm* on  $V$  is a function  $\| \cdot \| : V \rightarrow \mathbb{R}$  such that, for all  $u, v \in V$  and  $\lambda \in K$ :

1. If  $\|v\| = 0$  then  $v = 0$ .
2.  $\|\lambda v\| = |\lambda| \|v\|$
3. (*Triangle Inequality*)  $\|u + v\| \leq \|u\| + \|v\|$

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

**Proposition 15.0.2.** *In a normed space,  $\|0\| = 0$ .*

PROOF:  $\|0\| = |0| \|0\| = 0$  by Axiom 2.  $\square$

**Proposition 15.0.3.** *Let  $V$  be a normed vector space over  $K$ . For all  $v \in V$  we have  $\|v\| \geq 0$ .*

PROOF:

$$\begin{aligned}
 0 &= \|0\| && \text{(Proposition 15.0.2)} \\
 &= \|v - v\| \\
 &\leq \|v\| + \|-v\| && \text{(Triangle Inequality)} \\
 &= 2\|v\| && \text{(Axiom 2)}
 \end{aligned}$$

**Proposition 15.0.4.** *Let  $V$  be a normed space. Let  $u, v \in V$ . Then*

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

PROOF:

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

**Definition 15.0.5** (Euclidean Norm). The *Euclidean norm* on  $K^n$  is defined by

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

**Proposition 15.0.6.** The Euclidean norm on  $K^n$  is a norm.

PROOF:

$\langle 1 \rangle 1.$  If  $\|\vec{x}\| = 0$  then  $\vec{x} = \vec{0}$

PROOF: If  $\sqrt{|x_1|^2 + \dots + |x_n|^2} = 0$  then  $x_1 = \dots = x_n = 0$ .

$\langle 1 \rangle 2.$   $\|\lambda \vec{x}\| = |\lambda| \|\vec{x}\|$

PROOF:

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

$\langle 1 \rangle 3.$   $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$

PROOF:

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

□

**Corollary 15.0.6.1.** The absolute value function  $|\cdot|$  is a norm on  $K$ .

**Proposition 15.0.7.** The function  $\|\vec{x}\| = |x_1| + \dots + |x_n|$  is a norm on  $\mathbb{C}^n$ .

PROOF:

$\langle 1 \rangle 1.$  If  $\|\vec{x}\| = 0$  then  $\vec{x} = \vec{0}$

PROOF: If  $|x_1| + \dots + |x_n| = 0$  then  $x_1 = \dots = x_n = 0$ .

$\langle 1 \rangle 2.$   $\|\lambda \vec{x}\| = |\lambda| \|\vec{x}\|$



PROOF:

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

$\langle 1 \rangle 3. \|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$

PROOF:

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

□

**Proposition 15.0.8.** *The function  $\|\vec{x}\| = \max(|x_1|, \dots, |x_n|)$  is a norm on  $\mathbb{C}^n$ .*

PROOF:

$\langle 1 \rangle 1.$  If  $\|\vec{x}\| = 0$  then  $\vec{x} = \vec{0}$

PROOF: If  $\max(|x_1|, \dots, |x_n|) = 0$  then  $x_1 = \cdots = x_n = 0$ .

$\langle 1 \rangle 2. \|\lambda \vec{x}\| = |\lambda| \|\vec{x}\|$

PROOF:

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

$\langle 1 \rangle 3. \|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$

PROOF:

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

□

**Definition 15.0.9** (Uniform Convergence Norm). Let  $\Omega$  be a closed bounded subset of  $\mathbb{R}^n$ . The *uniform convergence norm* on  $\mathcal{C}(\Omega)$  is the function defined by  $\|f\| = \max_{x \in \Omega} |f(x)|$ .

**Proposition 15.0.10.** *Let  $\Omega$  be a closed bounded subset of  $\mathbb{R}^n$ . The uniform convergence norm is a norm on  $\mathcal{C}(\Omega)$ .*

PROOF:

$\langle 1 \rangle 1.$  If  $\|f\| = 0$  then  $f = 0$

PROOF: If  $\max_x |f(x)| = 0$  then  $f(x) = 0$  for all  $x$ .

$\langle 1 \rangle 2. \|\lambda f\| = |\lambda| \|f\|$

PROOF:

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

⟨1⟩3.  $\|f + g\| \leq \|f\| + \|g\|$

PROOF:

$$\begin{aligned}\|f + g\| &= \max_x |f(x) + g(x)| \\ &\leq \max_x (|f(x)| + |g(x)|) \\ &\leq \max_x |f(x)| + \max_x |g(x)| \\ &= \|f\| + \|g\|\end{aligned}$$

□

**Proposition 15.0.11.** *Let  $p \geq 1$ . The function  $\|(z_n)\| = (\sum_{n=1}^{\infty} |z_n|^p)^{1/p}$  is a norm on  $l^p$ .*

PROOF:

⟨1⟩1. If  $\|(z_n)\| = 0$  then  $(z_n) = (0)$

PROOF: If  $(\sum_n |z_n|^p)^{1/p} = 0$  then  $\sum_n |z_n|^p = 0$  so  $|z_n|^p = 0$  for all  $n$ , and so  $z_n = 0$  for all  $n$ .

⟨1⟩2.  $\|(\lambda z_n)\| = |\lambda| \|(z_n)\|$

PROOF:

$$\begin{aligned}\|(\lambda z_n)\| &= \left( \sum_n |\lambda z_n|^p \right)^{1/p} \\ &= |\lambda| \left( \sum_n |z_n|^p \right)^{1/p} \\ &= |\lambda| \|(z_n)\|\end{aligned}$$

⟨1⟩3. The triangle inequality holds.

PROOF: This is Minkowski's Inequality. □

**Proposition 15.0.12.** *Let  $V$  be a normed space and  $U$  a vector subspace of  $V$ . Then  $U$  is a normed space under the restriction of the norm to  $U$ .*

PROOF: Each axiom follows from the fact it holds in  $V$ . □

**Proposition 15.0.13.** *Let  $V$  be a normed space over  $K$ . Let  $x_1, \dots, x_n$  be linearly independent elements of  $V$ . Then there exists a real number  $c > 0$  such that, for all  $\alpha_1, \dots, \alpha_n \in K$ , we have*

$$\|\alpha_1 x_1 + \dots + \alpha_n x_n\| \geq c(|\alpha_1| + \dots + |\alpha_n|) .$$

PROOF:

⟨1⟩1. Define  $f : K^n \rightarrow \mathbb{R}$  by

$$f(\alpha_1, \dots, \alpha_n) = \|\alpha_1 x_1 + \dots + \alpha_n x_n\|$$

⟨1⟩2.  $f$  is continuous.

⟨2⟩1. LET:  $(\alpha_1, \dots, \alpha_n) \in K^n$  and  $\epsilon > 0$

⟨2⟩2. LET:  $\delta = \epsilon / (\|x_1\| + \dots + \|x_n\|)$

PROOF:  $x_1, \dots, x_n$  are not all zero because they are linearly independent.

⟨2⟩3. LET:  $(\beta_1, \dots, \beta_n)$  with  $|\alpha_i - \beta_i| < \delta$  for all  $i$

$$\langle 2 \rangle 4. \|(\alpha_1 x_1 + \cdots + \alpha_n x_n) - (\beta_1 x_1 + \beta_n x_n)\| < \epsilon$$

PROOF:

$$\|(\alpha_1 x_1 + \cdots + \alpha_n x_n) - (\beta_1 x_1 + \beta_n x_n)\|$$

$$\leq |\alpha_1 - \beta_1| \|x_1\| + \cdots + |\alpha_n - \beta_n| \|x_n\| \quad (\text{Axioms 2 and 3})$$

$$< \delta(\|x_1\| + \cdots + \|x_n\|) \quad (\langle 2 \rangle 3)$$

$$= \epsilon \quad (\langle 2 \rangle 2)$$

$\langle 1 \rangle 3.$  PICK  $(\beta_1, \dots, \beta_n) \in \{(\beta_1, \dots, \beta_n) \in K^n \mid |\beta_1| + \cdots + |\beta_n| = 1\}$  at which  $f$  attains its minimum.

PROOF: Extreme Value Theorem.

$\langle 1 \rangle 4.$  Let  $c = f(\beta_1, \dots, \beta_n)$

$\langle 1 \rangle 5.$   $c > 0$

PROOF: Linear independence.

$\langle 1 \rangle 6.$  LET:  $\alpha_1, \dots, \alpha_n \in K$

$\langle 1 \rangle 7.$   $\|\alpha_1 x_1 + \cdots + \alpha_n x_n\| \geq c(|\alpha_1| + \cdots + |\alpha_n|)$

$\langle 2 \rangle 1.$  ASSUME: w.l.o.g.  $\alpha_1, \dots, \alpha_n$  are not all zero.

$\langle 2 \rangle 2.$  LET:  $\beta_i = \alpha_i / (|\alpha_1| + \cdots + |\alpha_n|)$  for  $i = 1, \dots, n$

$\langle 2 \rangle 3.$   $|\beta_1| + \cdots + |\beta_n| = 1$

$\langle 2 \rangle 4.$   $f(\beta_1, \dots, \beta_n) \geq c$

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

PROOF: Multiply both sides by  $|\alpha_1| + \cdots + |\alpha_n|$ .

□

**Proposition 15.0.14.** 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:

$\langle 1 \rangle 1.$  For all  $x, y \in V$  we have  $d(x, y) \geq 0$

PROOF: Proposition 15.0.3.

$\langle 1 \rangle 2.$  For all  $x, y \in V$  we have  $d(x, y) = 0$  iff  $x = y$

$\langle 2 \rangle 1.$  If  $d(x, y) = 0$  then  $x = y$

PROOF: Axiom 1.

$\langle 2 \rangle 2.$  If  $x = y$  then  $d(x, y) = 0$

PROOF: Proposition 15.0.2.

$\langle 1 \rangle 3.$   $\forall x, y \in V. d(x, y) = d(y, x)$

PROOF: By Axiom 2.

$\langle 1 \rangle 4.$   $\forall x, y, z \in V. d(x, z) \leq d(x, y) + d(y, z)$

PROOF: By Axiom 3.

□

Henceforth we identify any normed space with this metric space.

## 15.1 Convergence

**Proposition 15.1.1.** Let  $V$  be a normed space over  $K$ . Let  $(x_n)$  be a sequence in  $V$  and  $l \in V$ . Then  $x_n \rightarrow l$  as  $n \rightarrow \infty$  in  $V$  if and only if  $\|x_n - l\| \rightarrow 0$  as  $n \rightarrow \infty$  in  $\mathbb{R}$ .

PROOF: Immediate from definitions.  $\square$

**Proposition 15.1.2.** *In a normed space, a sequence has at most one limit.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a vector space over  $K$ .

$\langle 1 \rangle 2$ . ASSUME:  $x_n \rightarrow l$  and  $x_n \rightarrow m$  as  $n \rightarrow \infty$ .

$\langle 1 \rangle 3$ . ASSUME: for a contradiction  $l \neq m$

$\langle 1 \rangle 4$ . LET:  $\epsilon = \|l - m\|/2$

$\langle 1 \rangle 5$ . PICK  $N$  such that  $\forall n \geq N, \|x_n - l\| < \epsilon$  and  $\forall n \geq N, \|x_n - m\| < \epsilon$

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

$\langle 1 \rangle 6$ .  $\|l - m\| < \|l - m\|$

PROOF:

$$\|l - m\| \leq \|x_N - l\| + \|x_N - m\| \quad (\text{Triangle Inequality})$$

$$< 2\epsilon \quad (\langle 1 \rangle 5)$$

$$= \|l - m\| \quad (\langle 1 \rangle 4)$$

$\langle 1 \rangle 7$ . Q.E.D.

PROOF: This is a contradiction.

$\square$

**Definition 15.1.3** (Bounded). Let  $V$  be a normed space over  $K$ . A sequence  $(x_n)$  in  $V$  is *bounded* iff there exists  $B$  such that  $\forall n, \|x_n\| < B$ .

**Proposition 15.1.4.** *Every convergent sequence is bounded.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $x_n \rightarrow l$  as  $n \rightarrow \infty$

$\langle 1 \rangle 2$ . PICK  $N$  such that  $\forall n \geq N, \|x_n - l\| < 1$

$\langle 1 \rangle 3$ . LET:  $B = \max(\|x_1\|, \|x_2\|, \dots, \|x_{N-1}\|, \|l\| + 1)$

$\langle 1 \rangle 4$ . LET:  $n \in \mathbb{N}$

$\langle 1 \rangle 5$ .  $\|x_n\| \leq B$

$\langle 2 \rangle 1$ . CASE:  $n < N$

PROOF:  $\|x_n\| \leq B$  from  $\langle 1 \rangle 3$ .

$\langle 2 \rangle 2$ . CASE:  $n \geq N$

PROOF:

$$\|x_n\| \leq \|l\| + \|x_n - l\| \quad (\text{Triangle Inequality})$$

$$< \|l\| + 1 \quad (\langle 1 \rangle 2)$$

$$\leq B \quad (\langle 1 \rangle 3)$$

$\square$

**Proposition 15.1.5.** *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:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $x_n \rightarrow l$  as  $n \rightarrow \infty$

$\langle 1 \rangle 3$ . LET:  $\lambda_n \rightarrow \lambda$  as  $n \rightarrow \infty$

- (1)4. LET:  $\epsilon > 0$   
 (1)5. PICK  $N$  such that, for all  $n \geq N$ , we have  $\|x_n - l\| < \epsilon/2|\lambda|$  and  $|\lambda_n - \lambda| < \sqrt{\epsilon/2}$  and  $\|x_n\| < \sqrt{\epsilon/2}$   
 (1)6. LET:  $n \geq N$   
 (1)7.  $\|\lambda_n x_n - \lambda l\| < \epsilon$

PROOF:

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

□

**Proposition 15.1.6.** *Let  $V$  be a normed space over  $K$ . If  $x_n \rightarrow l$  and  $y_n \rightarrow m$  as  $n \rightarrow \infty$ , then  $x_n + y_n \rightarrow l + m$  as  $n \rightarrow \infty$ .*

PROOF:

- (1)1. LET:  $\epsilon > 0$   
 (1)2. PICK  $N$  such that, for all  $n \geq N$ , we have  $\|x_n - l\| < \epsilon/2$  and  $\|y_n - m\| < \epsilon/2$   
 (1)3. LET:  $n \geq N$   
 (1)4.  $\|(x_n + y_n) - (l + m)\| < \epsilon$

PROOF:

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

□

**Definition 15.1.7** (Uniform Convergence). Let  $\Omega$  be a closed bounded subset of  $\mathbb{R}^n$ . Let  $(f_n)$  be a sequence in  $\mathcal{C}(\Omega)$  and  $f \in \mathcal{C}(\Omega)$ . Then  $(f_n)$  *converges uniformly* to  $f$  iff, for every  $\epsilon > 0$ , there exists  $N$  such that  $\forall x \in \Omega. \forall n \geq N. |f_n(x) - f(x)| < \epsilon$ .

**Proposition 15.1.8.** *Let  $\Omega$  be a closed bounded subset of  $\mathbb{R}^n$ . Let  $(f_n)$  be a sequence in  $\mathcal{C}(\Omega)$  and  $f \in \mathcal{C}(\Omega)$ . Then  $(f_n)$  converges uniformly to  $f$  iff  $f_n$  converges to  $f$  under the uniform convergence norm.*

PROOF:

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

□

**Definition 15.1.9** (Pointwise Convergence). Let  $(f_n)$  be a sequence in  $\mathcal{C}([0, 1])$  and  $f \in \mathcal{C}([0, 1])$ . Then  $(f_n)$  *converges pointwise* to  $f$  iff, for all  $t \in [0, 1]$ , we have  $|f_n(t) - f(t)| \rightarrow 0$  as  $n \rightarrow \infty$ .

**Proposition 15.1.10.** *There is no norm  $n$  on  $\mathcal{C}([0, 1])$  such that, for every sequence  $(f_n)$  and function  $f$  in  $\mathcal{C}([0, 1])$ , we have  $(f_n)$  converges pointwise to  $f$  if and only if  $(f_n)$  converges to  $f$  under  $n$ .*

PROOF:

(1)1. ASSUME: for a contradiction  $\| \cdot \|$  is a norm on  $\mathcal{C}([0, 1])$  such that, for every sequence  $(f_n)$  and function  $f$  in  $\mathcal{C}([0, 1])$ , we have  $(f_n)$  converges pointwise to  $f$  if and only if  $(f_n)$  converges to  $f$  under  $\| \cdot \|$ .

(1)2. For  $n \in \mathbb{Z}_+$ , define  $g_n \in \mathcal{C}([0, 1])$  by

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

(1)3. For all  $n$ ,  $\|g_n\| \neq 0$

PROOF: Axiom 1.

(1)4. For  $n \in \mathbb{Z}_+$ , define  $f_n \in \mathcal{C}([0, 1])$  by  $f_n = g_n / \|g_n\|$

(1)5. For all  $n$ ,  $\|f_n\| = 1$

PROOF: Axiom 2.

(1)6.  $(f_n)$  does not converge under  $\| \cdot \|$

(1)7.  $(f_n)$  converges pointwise to 0.

(1)8. This is a contradiction.

□

**Definition 15.1.11** (Equivalence of Norms). Let  $\| \cdot \|_1$  and  $\| \cdot \|_2$  be two norms on the same vector space  $V$ . Then the norms are *equivalent* if and only if, for any sequence  $(x_n)$  in  $V$  and  $l \in V$ , we have that  $(x_n)$  converges to  $l$  under  $\| \cdot \|_1$  if and only if  $(x_n)$  converges to  $l$  under  $\| \cdot \|_2$ .

**Theorem 15.1.12.** Let  $\| \cdot \|_1$  and  $\| \cdot \|_2$  be two norms on the same vector space  $E$  over  $K$ . Then  $\| \cdot \|_1$  and  $\| \cdot \|_2$  are equivalent if and only if there exist positive real numbers  $\alpha$  and  $\beta$  such that, for all  $x \in E$ ,

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

PROOF:

(1)1. If  $\| \cdot \|_1$  and  $\| \cdot \|_2$  are equivalent then there exist positive real numbers  $\alpha$  and  $\beta$  such that, for all  $x \in E$ ,  $\alpha \|x\|_1 \leq \|x\|_2 \leq \beta \|x\|_1$ .

(2)1. ASSUME:  $\| \cdot \|_1$  and  $\| \cdot \|_2$  are equivalent.

(2)2. There exists  $\alpha > 0$  such that, for all  $x \in E$ , we have  $\alpha \|x\|_1 \leq \|x\|_2$

(3)1. ASSUME: for a contradiction there is no  $\alpha > 0$  such that, for all  $x \in E$ , we have  $\alpha \|x\|_1 \leq \|x\|_2$ .

(3)2. For all  $n \in \mathbb{Z}_+$ , PICK  $x_n \in E$  such that  $1/n \|x_n\|_1 > \|x_n\|_2$

(3)3. For all  $n \in \mathbb{Z}_+$ ,

LET:

$$y_n = \frac{1}{\sqrt{n}} \frac{x_n}{\|x_n\|_2}$$

(3)4.  $(y_n)$  converges to 0 under  $\| \cdot \|_2$

(3)5.  $(y_n)$  converges to 0 under  $\| \cdot \|_1$

(3)6. For all  $n \in \mathbb{Z}_+$ , we have  $\|y_n\| > \sqrt{n}$

(3)7. This is a contradiction.

(2)3. There exists  $\beta > 0$  such that, for all  $x \in E$ , we have  $\|x\|_2 \leq \beta \|x\|_1$

PROOF: Similar.

- (1)2. If there exist positive real numbers  $\alpha$  and  $\beta$  such that, for all  $x \in E$ ,  
 $\alpha\|x\|_1 \leq \|x\|_2 \leq \beta\|x\|_1$ , then  $\|\cdot\|_1$  and  $\|\cdot\|_2$  are equivalent.  
 (2)1. ASSUME:  $\alpha$  and  $\beta$  are positive reals with  $\forall x \in E. \alpha\|x\|_1 \leq \|x\|_2 \leq \beta\|x\|_1$ .  
 (2)2. Let  $(x_n)$  be a sequence in  $E$  and  $l \in E$   
 (2)3. If  $(x_n)$  converges to  $l$  under  $\|\cdot\|_1$  then  $(x_n)$  converges to  $l$  under  $\|\cdot\|_2$ .  
 (3)1. ASSUME:  $(x_n)$  converges to  $l$  under  $\|\cdot\|_1$   
 (3)2. LET:  $\epsilon > 0$   
 (3)3. PICK  $N$  such that  $\forall n \geq N. \|x_n - l\|_1 < \epsilon/\beta$   
 (3)4.  $\forall n \geq N. \|x_n - l\|_2 < \epsilon$   
 (2)4. If  $(x_n)$  converges to  $l$  under  $\|\cdot\|_2$  then  $(x_n)$  converges to  $l$  under  $\|\cdot\|_1$ .  
 PROOF: Similar.

□

**Theorem 15.1.13.** *Any two norms on a finite dimensional vector space are equivalent.*

PROOF:

- (1)1. LET:  $V$  be a finite dimensional vector space over  $K$ .  
 (1)2. ASSUME: w.l.o.g.  $\dim V > 0$   
 (1)3. PICK a basis  $\{e_1, \dots, e_n\}$  for  $V$ .  
 (1)4. 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)5.  $\|\cdot\|_0$  is a norm.  
 (2)1. If  $\|v\|_0 = 0$  then  $v = 0$   
 PROOF: If  $|\alpha_1| + \dots + |\alpha_n| = 0$  then  $\alpha_1 = \dots = \alpha_n = 0$  so  $\alpha_1 e_1 + \dots + \alpha_n e_n = 0$ .  
 (2)2.  $\|\lambda v\|_0 = |\lambda| \|v\|_0$   
 PROOF:  

$$\begin{aligned} \|\lambda(\alpha_1 e_1 + \dots + \alpha_n e_n)\|_0 &= \|\lambda \alpha_1 e_1 + \dots + \lambda \alpha_n e_n\|_0 \\ &= |\lambda \alpha_1| + \dots + |\lambda \alpha_n| & (\langle 1 \rangle 4) \\ &= |\lambda|(|\alpha_1| + \dots + |\alpha_n|) \\ &= |\lambda| \|\alpha_1 e_1 + \dots + \alpha_n e_n\|_0 & (\langle 1 \rangle 4) \end{aligned}$$
  
 (2)3.  $\|u + v\|_0 \leq \|u\|_0 + \|v\|_0$   
 PROOF:  

$$\begin{aligned} \|(\alpha_1 e_1 + \dots + \alpha_n e_n) + (\beta_1 e_1 + \dots + \beta_n e_n)\| &= |\alpha_1 + \beta_1| + \dots + |\alpha_n + \beta_n| \\ &\leq |\alpha_1| + \dots + |\alpha_n| + |\beta_1| + \dots + |\beta_n| \\ &= \|\alpha_1 e_1 + \dots + \alpha_n e_n\|_0 + \|\beta_1 e_1 + \dots + \beta_n e_n\|_0 \end{aligned}$$
  
 (1)6. Any norm on  $V$  is equivalent to  $\|\cdot\|_0$ .  
 (2)1. LET:  $\|\cdot\|$  be any norm on  $V$ .  
 (2)2. PICK  $\alpha > 0$  such that, for all  $\alpha_1, \dots, \alpha_n \in K$ , we have  $\|\alpha_1 e_1 + \dots + \alpha_n e_n\| \geq \alpha(|\alpha_1| + \dots + |\alpha_n|)$   
 PROOF: Proposition 15.0.13, (2)1, (1)3.  
 (2)3. LET:  $\beta = \max(\|e_1\|, \dots, \|e_n\|)$   
 (2)4.  $\beta > 0$   
 PROOF:  $e_1, \dots, e_n$  cannot all be zero by (1)3.

$\langle 2 \rangle 5$ . For all  $x \in V$  we have  $\alpha \|x\|_0 \leq \|x\| \leq \beta \|x\|_0$

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

$\langle 3 \rangle 2$ .  $\alpha \|x\|_0 \leq \|x\|$

PROOF:  $\langle 1 \rangle 3$ ,  $\langle 1 \rangle 4$ ,  $\langle 2 \rangle 2$ .

$\langle 3 \rangle 3$ .  $\|x\| \leq \beta \|x\|_0$

$\langle 4 \rangle 1$ . LET:  $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$

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

PROOF:

$$\|x\| = \|\alpha_1 e_1 + \cdots + \alpha_n e_n\| \quad (\langle 4 \rangle 1)$$

$$\leq |\alpha_1| \|e_1\| + \cdots + |\alpha_n| \|e_n\| \quad (\langle 2 \rangle 1)$$

$$\leq \beta(|\alpha_1| + \cdots + |\alpha_n|) \quad (\langle 2 \rangle 3)$$

$$= \beta \|x\|_0 \quad (\langle 1 \rangle 4)$$

$\langle 2 \rangle 6$ . Q.E.D.

PROOF: Theorem 15.1.12,  $\langle 1 \rangle 5$ ,  $\langle 2 \rangle 1$ ,  $\langle 2 \rangle 2$ ,  $\langle 2 \rangle 4$ ,  $\langle 2 \rangle 5$ .

□

**Definition 15.1.14** (Open Ball). Let  $V$  be a normed space over  $K$ . Let  $x \in V$ . Let  $r > 0$ . The *open ball* with *centre*  $x$  and *radius*  $r$  is

$$B(x, r) := \{y \in V \mid \|y - x\| < r\} .$$

**Definition 15.1.15** (Closed Ball). Let  $V$  be a normed space over  $K$ . Let  $x \in V$ . Let  $r > 0$ . The *closed ball* with *centre*  $x$  and *radius*  $r$  is

$$\overline{B}(x, r) := \{y \in V \mid \|y - x\| \leq r\} .$$

**Definition 15.1.16** (Sphere). Let  $V$  be a normed space over  $K$ . Let  $x \in V$ . Let  $r > 0$ . The *sphere* with *centre*  $x$  and *radius*  $r$  is

$$S(x, r) := \{y \in V \mid \|y - x\| = r\} .$$

**Definition 15.1.17** (Open Set). Let  $V$  be a normed space over  $K$ . A set  $S \subseteq V$  is *open* iff, for all  $x \in S$ , there exists  $\epsilon > 0$  such that  $B(x, \epsilon) \subseteq S$ .

**Proposition 15.1.18**. *Equivalent norms define the same set of open sets.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $\|\cdot\|_1$  and  $\|\cdot\|_2$  be equivalent norms on  $V$ .

$\langle 1 \rangle 3$ . PICK reals  $\alpha, \beta > 0$  such that, for all  $x \in V$ , we have  $\alpha \|x\|_1 \leq \|x\|_2 \leq \beta \|x\|_1$

$\langle 1 \rangle 4$ . LET:  $S \subseteq V$

$\langle 1 \rangle 5$ . If  $S$  is open under  $\|\cdot\|_1$  then  $S$  is open under  $\|\cdot\|_2$ .

$\langle 2 \rangle 1$ . ASSUME:  $S$  is open under  $\|\cdot\|_1$ .

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

$\langle 2 \rangle 3$ . PICK  $\epsilon > 0$  such that  $\{y \in V \mid \|x - y\|_1 < \epsilon\} \subseteq S$ .

$\langle 2 \rangle 4$ . LET:  $\delta = \alpha \epsilon$



- $\langle 2 \rangle 5. \{y \in V \mid \|x - y\|_2 < \delta\} \subseteq S$   
 $\langle 1 \rangle 6. \text{ If } S \text{ is open under } \|\cdot\|_2 \text{ then } S \text{ is open under } \|\cdot\|_1.$

PROOF: Similar.

□

**Proposition 15.1.19.** *Every open ball is open.*

PROOF:

$\langle 1 \rangle 1. \text{ LET: } V \text{ be a normed space over } K.$

$\langle 1 \rangle 2. \text{ LET: } c \in V \text{ and } r > 0$

PROVE:  $B(c, r)$  is open.

$\langle 1 \rangle 3. \text{ LET: } x \in B(c, r)$

$\langle 1 \rangle 4. \text{ LET: } \epsilon = r - \|x - c\|$

PROVE:  $B(x, \epsilon) \subseteq B(c, r)$

$\langle 1 \rangle 5. \text{ LET: } y \in B(x, \epsilon)$

PROVE:  $y \in B(c, r)$

$\langle 1 \rangle 6. \|y - c\| < r$

PROOF:

$$\begin{aligned} \|y - c\| &\leq \|y - x\| + \|x - c\| && \text{(Triangle Inequality)} \\ &< \epsilon + \|x - c\| && (\langle 1 \rangle 5) \\ &= r && (\langle 1 \rangle 4) \end{aligned}$$

□

**Proposition 15.1.20.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$ . Then  $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega. g(x) < f(x)\}$  is open.*

PROOF:

$\langle 1 \rangle 1. \text{ LET: } g \in U$

$\langle 1 \rangle 2. \text{ LET: } \epsilon = \max_{x \in \Omega} (f(x) - g(x))$

PROVE:  $B(g, \epsilon) \subseteq U$

$\langle 1 \rangle 3. \epsilon > 0$

$\langle 1 \rangle 4. \text{ LET: } h \in B(g, \epsilon/2)$

PROVE:  $h \in U$

$\langle 1 \rangle 5. \text{ LET: } x \in \Omega$

$\langle 1 \rangle 6. h(x) < f(x)$

PROOF:

$$\begin{aligned} h(x) &\leq g(x) + \epsilon/2 && (\langle 1 \rangle 4) \\ &< g(x) + \epsilon && (\langle 1 \rangle 3) \\ &\leq f(x) && (\langle 1 \rangle 2) \end{aligned}$$

□

**Proposition 15.1.21.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$ . Then  $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega. g(x) > f(x)\}$  is open.*

PROOF: Given  $g \in U$ , let  $\epsilon = \max_x (g(x) - f(x))/2$ . Then  $B(g, \epsilon) \subseteq U$ . □

**Proposition 15.1.22.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$  be such that  $f(x) > 0$  for all  $x \in \Omega$ . Then  $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega. |g(x)| < f(x)\}$  is open.*

PROOF: Given  $g \in U$ , let  $\epsilon = \max_x (f(x) - |g(x)|)/2$ . Then  $B(g, \epsilon) \subseteq U$ .  $\square$

**Proposition 15.1.23.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$  be such that  $f(x) > 0$  for all  $x \in \Omega$ . Then  $U = \{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega, |g(x)| > f(x)\}$  is open.*

PROOF: Given  $g \in U$ , let  $\epsilon = \max_x (|g(x)| - f(x))/2$ . Then  $B(g, \epsilon) \subseteq U$ .  $\square$

**Proposition 15.1.24.** *The union of a set of open sets is open.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $\mathcal{U}$  be a set of open sets in  $V$ .

$\langle 1 \rangle 3$ . LET:  $x \in \bigcup \mathcal{U}$

$\langle 1 \rangle 4$ . PICK  $U \in \mathcal{U}$  such that  $x \in U$ .

$\langle 1 \rangle 5$ . PICK  $\epsilon > 0$  such that  $B(x, \epsilon) \subseteq U$

$\langle 1 \rangle 6$ .  $B(x, \epsilon) \subseteq \bigcup \mathcal{U}$

$\square$

**Proposition 15.1.25.** *The intersection of two open sets is open.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $U_1$  and  $U_2$  be open sets in  $V$ .

$\langle 1 \rangle 3$ . LET:  $x \in U_1 \cap U_2$

$\langle 1 \rangle 4$ . PICK  $\epsilon_1 > 0$  such that  $B(x, \epsilon_1) \subseteq U_1$

$\langle 1 \rangle 5$ . PICK  $\epsilon_2 > 0$  such that  $B(x, \epsilon_2) \subseteq U_2$

$\langle 1 \rangle 6$ . LET:  $\epsilon = \min(\epsilon_1, \epsilon_2)$

$\langle 1 \rangle 7$ .  $B(x, \epsilon) \subseteq U_1 \cap U_2$

$\square$

**Proposition 15.1.26.** *In any normed space,  $\emptyset$  is open.*

PROOF: Vacuous.  $\square$

**Proposition 15.1.27.** *In any normed space  $V$ , the whole space  $V$  is open.*

PROOF: For any  $x \in V$  we have  $B(x, 1) \subseteq V$ .  $\square$

**Definition 15.1.28** (Closed Set). Let  $V$  be a normed space over  $K$ . A set  $S \subseteq V$  is *closed* iff  $V - S$  is open.

**Proposition 15.1.29.** *Every closed ball is closed.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $c \in V$  and  $r > 0$

PROVE:  $\overline{B}(c, r)$  is closed.

$\langle 1 \rangle 3$ . LET:  $x \in V - \overline{B}(c, r)$

$\langle 1 \rangle 4$ . LET:  $\epsilon = \|x - c\| - r$

PROVE:  $B(x, \epsilon) \subseteq V - \overline{B}(c, r)$

$\langle 1 \rangle 5. \epsilon > 0$

PROOF: Since  $\|x - c\| > r$  by  $\langle 1 \rangle 3$ .

$\langle 1 \rangle 6. \text{ LET: } y \in B(x, \epsilon)$

$\langle 1 \rangle 7. \|y - c\| > r$

PROOF:

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

□

**Proposition 15.1.30.** *The intersection of a set of closed sets is closed.*

PROOF: From Proposition 15.1.24. □

**Proposition 15.1.31.** *The union of two closed sets is closed.*

PROOF: From Proposition 15.1.25. □

**Proposition 15.1.32.** *Every sphere is closed.*

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

**Proposition 15.1.33.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$ . Then  $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega, g(x) \leq f(x)\}$  is closed.*

PROOF: It is  $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega, g(x) > f(x)\}$ . □

**Proposition 15.1.34.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$ . Then  $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega, g(x) \geq f(x)\}$  is closed.*

PROOF: It is  $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega, g(x) < f(x)\}$ . □

**Proposition 15.1.35.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$ . Then  $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega, |g(x)| \leq f(x)\}$  is closed.*

PROOF: It is  $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega, |g(x)| > f(x)\}$ . □

**Proposition 15.1.36.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $f \in \mathcal{C}(\Omega)$ . Then  $\{g \in \mathcal{C}(\Omega) \mid \forall x \in \Omega, |g(x)| \geq f(x)\}$  is closed.*

PROOF: It is  $\mathcal{C}(\Omega) - \{g \mid \forall x \in \Omega, |g(x)| < f(x)\}$ . □

**Proposition 15.1.37.** *Let  $\Omega$  be a closed bounded set in  $\mathbb{R}^n$ . Let  $x_0 \in \Omega$  and  $\lambda \in \mathbb{C}$ . Then  $C = \{g \in \mathcal{C}(\Omega) \mid g(x_0) = \lambda\}$  is closed.*

PROOF: Given  $g \in \mathcal{C}(\Omega) - C$ , let  $\epsilon = |g(x_0) - \lambda|/2$ . Then  $B(g, \epsilon) \subseteq \mathcal{C}(\Omega) - C$ . □

**Proposition 15.1.38.** *In any normed space  $V$ , we have  $\emptyset$  is closed.*

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

**Proposition 15.1.39.** *In any normed space  $V$ , the whole space  $V$  is closed.*

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

**Theorem 15.1.40.** *Let  $V$  be a normed space over  $K$ . Let  $S$  be a subset of  $V$ . Then  $S$  is closed if and only if, for any sequence  $(x_n)$  in  $S$ , if  $x_n \rightarrow l$  as  $n \rightarrow \infty$  then  $l \in S$ .*

PROOF:

- (1)1. If  $S$  is closed then, for any sequence  $(x_n)$  in  $S$ , if  $x_n \rightarrow l$  as  $n \rightarrow \infty$  then  $l \in S$ .
  - (2)1. ASSUME:  $S$  is closed.
  - (2)2. LET:  $(x_n)$  be a sequence in  $S$ .
  - (2)3. ASSUME:  $x_n \rightarrow l$  as  $n \rightarrow \infty$ .
  - (2)4. ASSUME: for a contradiction  $l \notin S$ .
  - (2)5. PICK  $\epsilon > 0$  such that  $B(l, \epsilon) \subseteq V - S$
  - (2)6. PICK  $N$  such that  $\forall n \geq N. x_n \in B(l, \epsilon)$
  - (2)7.  $x_N \in V - S$
  - (2)8. This contradicts (2)2.
- (1)2. If, for any sequence  $(x_n)$  in  $S$ , if  $x_n \rightarrow l$  as  $n \rightarrow \infty$  then  $l \in S$ , then  $S$  is closed.
  - (2)1. ASSUME: for any sequence  $(x_n)$  in  $S$ , if  $x_n \rightarrow l$  as  $n \rightarrow \infty$  then  $l \in S$ .
  - (2)2. LET:  $x \in V - S$
  - (2)3. ASSUME: for a contradiction there is no  $\epsilon > 0$  such that  $B(x, \epsilon) \subseteq V - S$ .
  - (2)4. For  $n \in \mathbb{Z}_+$ , PICK  $x_n \in B(x, 1/n) \cap S$
  - (2)5.  $x_n \rightarrow x$  as  $n \rightarrow \infty$
  - (2)6.  $x \in S$
  - (2)7. This contradicts (2)2.

$\square$

**Definition 15.1.41** (Closure). Let  $V$  be a normed space over  $K$ . Let  $S$  be a subset of  $V$ . The *closure* of  $S$ ,  $\text{cl } S$ , is the intersection of the set of closed sets that include  $S$ .

**Proposition 15.1.42.** *Let  $V$  be a normed space over  $K$ . Let  $S$  be a subset of  $V$ . Then the closure of  $S$  is the smallest closed set that includes  $S$ .*

PROOF: Proposition 15.1.30.  $\square$

**Theorem 15.1.43.** *Let  $V$  be a normed space over  $K$ . Let  $S$  be a subset of  $V$ . Then*

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

PROOF:

- (1)1. For all  $l \in \text{cl } S$ , there exists a sequence  $(x_n)$  in  $S$  such that  $x_n \rightarrow l$  as  $n \rightarrow \infty$ .
    - (2)1. LET:  $l \in \text{cl } S$
    - (2)2. For  $n \in \mathbb{Z}_+$ , pick  $x_n \in B(l, 1/n) \cap S$
- PROOF: There must be such an  $x_n$  otherwise  $S - B(l, 1/n)$  would be a smaller closed set that includes  $S$ .

- ⟨2⟩3.  $x_n \rightarrow l$  as  $n \rightarrow \infty$   
 ⟨1⟩2. For any sequence  $(x_n)$  in  $S$ , if  $x_n \rightarrow l$  as  $n \rightarrow \infty$  then  $l \in \text{cl } S$ .  
 PROOF: Theorem 15.1.40.

□

**Definition 15.1.44** (Dense). Let  $V$  be a normed space over  $K$ . Let  $S \subseteq V$ . Then  $S$  is *dense* if and only if  $\text{cl } S = V$ .

**Theorem 15.1.45** (Weierstrass Approximation Theorem). Let  $a$  and  $b$  be real numbers with  $a < b$ . In  $\mathcal{C}([a, b])$ , the set of polynomials is dense.

PROOF: TODO

**Proposition 15.1.46.** Let  $p \geq 1$ . The set of all sequences that have only finitely many non-zero terms is dense in  $l^p$ .

PROOF:

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

PROOF:

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

$$< \epsilon \quad (\langle 1 \rangle 2)$$

□

**Theorem 15.1.47.** Let  $V$  be a normed space over  $K$ . Let  $S \subseteq V$ . Then the following are equivalent.

1.  $S$  is dense.
2. For all  $l \in V$ , there exists a sequence  $(x_n)$  in  $S$  such that  $x_n \rightarrow l$  as  $n \rightarrow \infty$ .
3. Every nonempty open subset of  $V$  intersects  $S$ .

PROOF:

- ⟨1⟩1.  $1 \Leftrightarrow 2$   
 PROOF: Theorem 15.1.43.  
 ⟨1⟩2.  $1 \Rightarrow 3$   
 ⟨2⟩1. ASSUME:  $S$  is dense.  
 ⟨2⟩2. LET:  $U$  be a nonempty open subset of  $V$ .  
 ⟨2⟩3.  $X - U$  does not include  $S$ .

PROOF: Lest we have  $\text{cl } S \subseteq X - U$ .

$\langle 2 \rangle 4$ .  $U$  intersects  $S$ .

$\langle 1 \rangle 3$ .  $3 \Rightarrow 1$

$\langle 2 \rangle 1$ . ASSUME: Every nonempty subset of  $V$  intersects  $S$ .

$\langle 2 \rangle 2$ . Every closed proper subset of  $V$  does not include  $S$ .

$\langle 2 \rangle 3$ .  $\text{cl } S = V$

□

**Definition 15.1.48** (Compact). Let  $V$  be a normed space over  $K$  and  $S \subseteq V$ . Then  $S$  is *compact* if and only if every sequence in  $S$  has a convergent subsequence whose limit is in  $S$ .

**Proposition 15.1.49.** *In  $K^n$ , a set is compact if and only if it is bounded and closed.*

PROOF: TODO

**Definition 15.1.50** (Bounded). Let  $V$  be a normed space over  $K$  and  $S \subseteq V$ . Then  $S$  is *bounded* iff there exists  $r > 0$  such that  $S \subseteq B(0, r)$ .

**Theorem 15.1.51.** *Every compact set is closed and bounded.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $S \subseteq V$  be compact.

$\langle 1 \rangle 3$ .  $S$  is closed.

$\langle 2 \rangle 1$ . LET:  $(x_n)$  be a sequence in  $S$  that converges to  $l$

$\langle 2 \rangle 2$ . PICK a sequence  $(x_{n_r})$  that converges to  $x \in S$

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

$\langle 2 \rangle 3$ .  $x_{n_r} \rightarrow l$  as  $n \rightarrow \infty$

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

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

PROOF: Proposition 15.1.2.

$\langle 2 \rangle 5$ .  $l \in S$

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

$\langle 2 \rangle 6$ . Q.E.D.

PROOF: Theorem 15.1.40.

$\langle 1 \rangle 4$ .  $S$  is bounded.

$\langle 2 \rangle 1$ . ASSUME: for a contradiction  $S$  is unbounded.

$\langle 2 \rangle 2$ . For  $n \in \mathbb{Z}_+$ , PICK  $x_n \in S - B(0, n)$

$\langle 2 \rangle 3$ . PICK a convergent subsequence  $(x_{n_r})$  that converges to  $l$ , say.

$\langle 2 \rangle 4$ . PICK  $N \in \mathbb{Z}_+$  such that  $\|l\| < N$

$\langle 2 \rangle 5$ . PICK  $r$  such that  $n_r > N$  and  $\|x_{n_r} - l\| < N - \|l\|$

$\langle 2 \rangle 6$ .  $\|x_{n_r}\| < N < n_r$

$\langle 2 \rangle 7$ . This contradicts  $\langle 2 \rangle 2$ .

□

**Proposition 15.1.52.** *In  $\mathcal{C}([0, 1])$ , the closed ball  $\overline{B}(0, 1)$  is closed and bounded but not compact.*

PROOF: The sequence of functions  $(x^n)$  is in  $\overline{B}(0,1)$  but has no convergent subsequence.  $\square$

**Theorem 15.1.53** (Riesz's Lemma). *Let  $V$  be a normed vector space over  $K$ . Let  $X$  be a closed proper subspace of  $V$ . Let  $0 < \epsilon < 1$ . Then there exists  $x \in V$  such that  $\|x\| = 1$  and  $\forall y \in X, \|x - y\| \geq \epsilon$ .*

PROOF:

$\langle 1 \rangle 1$ . PICK  $z \in V - X$

$\langle 1 \rangle 2$ . LET:  $d = \inf_{x \in X} \|z - x\|$

$\langle 1 \rangle 3$ .  $d > 0$

PROOF: Since  $X$  is closed, there exists  $e > 0$  such that  $B(z, d) \subseteq V - X$  and hence  $\|z - x\| \geq d$  for all  $x \in X$ .

$\langle 1 \rangle 4$ . PICK  $x_0 \in X$  such that  $d \leq \|z - x_0\| \leq d/\epsilon$

PROOF: One exists since  $d/\epsilon$  is not a lower bound for  $\{\|z - x\| \mid x \in X\}$ .

$\langle 1 \rangle 5$ . LET:  $x = (z - x_0)/\|z - x_0\|$

$\langle 1 \rangle 6$ . LET:  $y \in X$

$\langle 1 \rangle 7$ .  $\|x - y\| \geq \epsilon$

PROOF:

$$\|x - y\| = \left\| \frac{z - x_0}{\|z - x_0\|} - y \right\| \quad (\langle 1 \rangle 5)$$

$$= \frac{1}{\|z - x_0\|} \|z - (x_0 + \|z - x_0\|y)\|$$

$$\geq \frac{1}{\|z - x_0\|} d \quad (\langle 1 \rangle 2)$$

$$\geq \epsilon \quad (\langle 1 \rangle 4)$$

$\square$

**Theorem 15.1.54.** *Let  $V$  be a normed space over  $K$ . Then  $V$  is finite dimensional if and only if  $\overline{B}(0,1)$  is compact.*

PROOF:

$\langle 1 \rangle 1$ . If  $V$  is finite dimensional then  $\overline{B}(0,1)$  is compact.

$\langle 2 \rangle 1$ . ASSUME:  $V$  is finite dimensional.

$\langle 2 \rangle 2$ . PICK a basis  $\{e_1, \dots, e_n\}$

$\langle 2 \rangle 3$ . ASSUME: w.l.o.g.  $\|\alpha_1 e_1 + \dots + \alpha_n e_n\| = |\alpha_1| + \dots + |\alpha_n|$

$\langle 2 \rangle 4$ . LET:  $(\alpha_{k1} e_1 + \dots + \alpha_{kn} e_n)$  be a sequence in  $\overline{B}(0,1)$

$\langle 2 \rangle 5$ . PICK a convergent subsequence  $(\alpha_{k_r,1})$  of  $(\alpha_{k1})$ , a convergent subsequence  $(\alpha_{k_r',2})$  of  $(\alpha_{k_r,2})$ ,  $\dots$ , a convergent subsequence  $(\alpha_{k_r'',n})$ .

$\langle 2 \rangle 6$ .  $(\alpha_{k_r'',1} e_1 + \dots + \alpha_{k_r'',n} e_n)$  converges.

$\langle 1 \rangle 2$ . If  $V$  is infinite dimensional then  $\overline{B}(0,1)$  is not compact.

$\langle 2 \rangle 1$ . ASSUME:  $V$  is infinite dimensional.

$\langle 2 \rangle 2$ . Choose a sequence  $(x_n)$  with  $\|x_n\| = 1$  and  $\|x_m - x_n\| \geq 1/2$  for  $m \neq n$

$\langle 3 \rangle 1$ . ASSUME:  $x_1, \dots, x_n$  satisfy  $\|x_i\| = 1$  and  $\|x_i - x_j\| \geq 1/2$  for  $i \neq j$

$\langle 3 \rangle 2$ . PICK  $x_{n+1} \in V$  such that  $\|x_{n+1}\| = 1$  and for all  $y \in \text{span}\{x_1, \dots, x_n\}$  we have  $\|x_{n+1} - y\| \geq 1/2$

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

**Proposition 15.1.55.** *Let  $V$  be a normed space. The closure of a subspace of  $V$  is a subspace.*

PROOF:

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

## 15.2 Continuous Linear Mappings

**Definition 15.2.1** (Continuous). Let  $U$  and  $V$  be normed spaces. Let  $f : U \rightarrow V$  and  $x \in U$ . Then  $f$  is *continuous at  $x$*  iff, for any sequence  $(x_n)$  in  $U$ , if  $x_n \rightarrow x$  as  $n \rightarrow \infty$  then  $f(x_n) \rightarrow f(x)$  as  $n \rightarrow \infty$ . The function  $f$  is *continuous* iff  $f$  is continuous at every point.

**Proposition 15.2.2.** *Let  $V$  be a normed space. Then the norm is a continuous function  $V \rightarrow \mathbb{R}$ .*

PROOF: From Proposition 15.0.4. □

**Proposition 15.2.3.** *Let  $U$  and  $V$  be normed space. Let  $f : U \rightarrow V$ . Then the following are equivalent.*

1.  $f$  is continuous.
2. For any open set  $S$  in  $V$ , we have  $f^{-1}(S)$  is open in  $U$ .



3. For any closed set  $C$  in  $V$ , we have  $f^{-1}(C)$  is closed in  $U$ .

**Proposition 15.2.4.** *Let  $U$  and  $V$  be normed spaces over  $K$ . Let  $T : U \rightarrow V$  be a linear transformation. If  $T$  is continuous at some point, then it is continuous.*

PROOF:

- $\langle 1 \rangle 1$ . ASSUME:  $T$  is continuous at  $u_0$
- $\langle 1 \rangle 2$ . LET:  $x_n \rightarrow l$  as  $n \rightarrow \infty$  in  $U$
- $\langle 1 \rangle 3$ .  $x_n - l + u_0 \rightarrow u_0$  as  $n \rightarrow \infty$ .
- $\langle 1 \rangle 4$ .  $T(x_n - l + u_0) \rightarrow T(u_0)$  as  $n \rightarrow \infty$ .
- $\langle 1 \rangle 5$ .  $T(x_n) - T(l) + T(u_0) \rightarrow T(u_0)$  as  $n \rightarrow \infty$ .
- $\langle 1 \rangle 6$ .  $T(x_n) \rightarrow T(l)$  as  $n \rightarrow \infty$ .

□

**Definition 15.2.5** (Bounded). Let  $U$  and  $V$  be normed spaces over  $K$ . Let  $T : U \rightarrow V$  be a linear transformation. Then  $T$  is *bounded* iff there exists  $\alpha > 0$  such that, for all  $x \in U$ , we have  $\|T(x)\| \leq \alpha\|x\|$ .

**Theorem 15.2.6.** *Let  $U$  and  $V$  be normed spaces over  $K$ . Let  $T : U \rightarrow V$  be a linear transformation. Then  $T$  is continuous if and only if it is bounded.*

PROOF:

- $\langle 1 \rangle 1$ . If  $T$  is continuous then  $T$  is bounded.
- $\langle 2 \rangle 1$ . ASSUME:  $T$  is not bounded.
- $\langle 2 \rangle 2$ . For  $n \in \mathbb{Z}_+$ , PICK  $x_n \in U$  such that  $\|T(x_n)\| > n\|x_n\|$ .
- $\langle 2 \rangle 3$ . For  $n \in \mathbb{Z}_+$ ,  
LET:

$$y_n = \frac{x_n}{n\|x_n\|}$$

- $\langle 2 \rangle 4$ .  $y_n \rightarrow 0$  as  $n \rightarrow \infty$
- $\langle 2 \rangle 5$ .  $T(y_n) \not\rightarrow 0$  as  $n \rightarrow \infty$
- $\langle 2 \rangle 6$ .  $T$  is not continuous.
- $\langle 1 \rangle 2$ . If  $T$  is bounded then  $T$  is continuous.
- $\langle 2 \rangle 1$ . ASSUME:  $T$  is bounded.
- $\langle 2 \rangle 2$ . PICK  $\alpha > 0$  such that  $\forall x \in U, \|T(x)\| \leq \alpha\|x\|$ .
- $\langle 2 \rangle 3$ .  $T$  is continuous at 0.
- $\langle 3 \rangle 1$ . LET:  $(x_n)$  be a sequence that converges to 0 in  $U$
- $\langle 3 \rangle 2$ .  $T(x_n) \rightarrow 0$  as  $n \rightarrow \infty$

PROOF:

$$\begin{aligned} \|T(x_n)\| &\leq \alpha\|x_n\| && (\langle 2 \rangle 2) \\ &\rightarrow 0 && \text{as } n \rightarrow \infty \end{aligned}$$

- $\langle 2 \rangle 4$ .  $T$  is continuous.

PROOF: Proposition 15.2.4.

□

**Proposition 15.2.7.** *Let  $U$  and  $V$  be normed spaces over  $K$  where  $U$  is finite dimensional. Let  $T : U \rightarrow V$  be a linear transformation. Then  $T$  is bounded.*

PROOF:

- ⟨1⟩1. PICK a basis  $\{e_1, \dots, e_n\}$  of unit vectors for  $U$ .  
 ⟨1⟩2. LET:  $M = \max(\|T(e_1)\|, \dots, \|T(e_n)\|)$   
 ⟨1⟩3. PICK  $C > 0$  such that, for all  $\alpha_1, \dots, \alpha_n \in K$ , we have  $|\alpha_1| + \dots + |\alpha_n| \leq C\|\alpha_1 e_1 + \dots + \alpha_n e_n\|$

PROOF: Theorem 15.1.13.

- ⟨1⟩4. LET:  $x \in U$   
 PROVE:  $\|T(x)\| \leq CM\|x\|$   
 ⟨1⟩5. LET:  $x = \alpha_1 e_1 + \dots + \alpha_n e_n$   
 ⟨1⟩6.  $\|T(x)\| \leq CM\|x\|$

PROOF:

$$\begin{aligned}
 \|T(x)\| &= \|\alpha_1 T(e_1) + \dots + \alpha_n T(e_n)\| && (T \text{ linear}) \\
 &\leq |\alpha_1| \|T(e_1)\| + \dots + |\alpha_n| \|T(e_n)\| && (\text{Triangle inequality}) \\
 &\leq M(|\alpha_1| + \dots + |\alpha_n|) && (\langle 1 \rangle 2) \\
 &\leq CM\|x\| && (\langle 1 \rangle 3)
 \end{aligned}$$

□

**Corollary 15.2.7.1.** *Let  $U$  and  $V$  be normed spaces over  $K$  where  $U$  is finite dimensional. Let  $T : U \rightarrow V$  be a linear transformation. Then  $T$  is continuous.*

**Proposition 15.2.8.** *Let  $U$  and  $V$  be normed spaces over  $K$ . Let  $T : U \rightarrow V$  be a linear transformation. If  $T$  is continuous, then  $T$  is uniformly continuous.*

PROOF:

- ⟨1⟩1. ASSUME:  $T$  is continuous  
 ⟨1⟩2. PICK  $B > 0$  such that  $\forall x \in U. \|T(x)\| \leq B\|x\|$   
 ⟨1⟩3. LET:  $\epsilon > 0$   
 ⟨1⟩4. LET:  $\delta = \epsilon/B$   
 ⟨1⟩5. LET:  $x, y \in U$   
 ⟨1⟩6. ASSUME:  $\|x - y\| < \delta$   
 ⟨1⟩7.  $\|T(x) - T(y)\| < \epsilon$

PROOF:

$$\begin{aligned}
 \|T(x) - T(y)\| &= \|T(x - y)\| && (T \text{ linear}) \\
 &\leq B\|x - y\| && (\langle 1 \rangle 2) \\
 &< B\delta && (\langle 1 \rangle 6) \\
 &= \epsilon && (\langle 1 \rangle 4)
 \end{aligned}$$

□

**Proposition 15.2.9.** *Let  $U$  and  $V$  be normed spaces over  $K$ . The set  $\mathcal{B}(U, V)$  of all bounded linear maps from  $U$  to  $V$  forms a subspace of the space of all linear maps from  $U$  to  $V$ .*

PROOF:

- ⟨1⟩1. LET:  $S, T : U \rightarrow V$  be bounded linear maps and  $\alpha, \beta \in K$ .  
 PROVE:  $\alpha S + \beta T$  is bounded.  
 ⟨1⟩2. PICK  $B, C > 0$  such that  $\forall x \in U. \|S(x)\| \leq B\|x\|$  and  $\|T(x)\| \leq C\|x\|$   
 ⟨1⟩3.  $\forall x \in U. \|(\alpha S + \beta T)(x)\| \leq (|\alpha|B + |\beta|C)\|x\|$

□

**Proposition 15.2.10.** *Let  $U$  and  $V$  be normed spaces over  $K$ . Define the operator norm  $\| \cdot \|$  on  $\mathcal{B}(U, V)$  by  $\|T\| := \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\}$ . Then  $\| \cdot \|$  is a norm on  $\mathcal{B}(U, V)$ .*

PROOF:

$\langle 1 \rangle 1$ . For all  $T \in \mathcal{B}(U, V)$ , the set  $\{\|T(x)\| \mid x \in U, \|x\| = 1\}$  is bounded above.

$\langle 2 \rangle 1$ . LET:  $T \in \mathcal{B}(U, V)$

$\langle 2 \rangle 2$ . PICK  $B$  such that  $\forall x \in U, \|T(x)\| \leq B\|x\|$ .

$\langle 2 \rangle 3$ .  $B$  is an upper bound for  $\{\|T(x)\| \mid x \in U, \|x\| = 1\}$ .

$\langle 1 \rangle 2$ . If  $\|T\| = 0$  then  $T = 0$ .

$\langle 2 \rangle 1$ . ASSUME:  $\|T\| = 0$

$\langle 2 \rangle 2$ . LET:  $x \in U$

PROVE:  $T(x) = 0$

$\langle 2 \rangle 3$ . ASSUME: w.l.o.g.  $\|x\| \neq 0$

$\langle 2 \rangle 4$ . LET:  $y = x/\|x\|$

$\langle 2 \rangle 5$ .  $\|y\| = 1$

$\langle 2 \rangle 6$ .  $\|T(y)\| = 0$

$\langle 2 \rangle 7$ .  $T(y) = 0$

$\langle 2 \rangle 8$ .  $T(x) = 0$

$\langle 1 \rangle 3$ . For all  $\lambda \in K$  and  $T \in \mathcal{B}(U, V)$ , we have  $\|\lambda T\| = |\lambda|\|T\|$

$\langle 2 \rangle 1$ . LET:  $\lambda \in K$  and  $T \in \mathcal{B}(U, V)$

$\langle 2 \rangle 2$ .  $\|\lambda T\| = |\lambda|\|T\|$

PROOF:

$$\begin{aligned} \|\lambda T\| &= \sup\{\|\lambda T(x)\| \mid x \in U, \|x\| = 1\} \\ &= \sup\{|\lambda|\|T(x)\| \mid x \in U, \|x\| = 1\} \\ &= |\lambda| \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\} \\ &= |\lambda|\|T\| \end{aligned}$$

$\langle 1 \rangle 4$ . For all  $S, T \in \mathcal{B}(U, V)$ , we have  $\|S + T\| \leq \|S\| + \|T\|$ .

$\langle 2 \rangle 1$ . LET:  $S, T \in \mathcal{B}(U, V)$

$\langle 2 \rangle 2$ .  $\|S + T\| \leq \|S\| + \|T\|$

PROOF:

$$\begin{aligned} \|S + T\| &= \sup\{\|S(x) + T(x)\| \mid x \in U, \|x\| = 1\} \\ &\leq \sup\{\|S(x)\| + \|T(x)\| \mid x \in U, \|x\| = 1\} \\ &\leq \sup\{\|S(x)\| \mid x \in U, \|x\| = 1\} + \sup\{\|T(x)\| \mid x \in U, \|x\| = 1\} \\ &= \|S\| + \|T\| \end{aligned}$$

□

**Proposition 15.2.11.** *Let  $U$  and  $V$  be normed spaces. Let  $T \in \mathcal{B}(U, V)$ . Then  $\|T\|$  is the least number such that  $\forall u \in U, \|T(u)\| \leq \|T\|\|u\|$ .*

PROOF:

$\langle 1 \rangle 1$ .  $\forall u \in U, \|T(u)\| \leq \|T\|\|u\|$

$\langle 2 \rangle 1$ . LET:  $u \in U$

$\langle 2 \rangle 2$ . LET:  $v = u/\|u\|$

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

□

**Proposition 15.2.12.** *Let  $V$  be a normed space. Then  $\text{id}_V$  is a bounded linear function  $V \rightarrow V$ , and  $\|\text{id}_V\| = 1$ .*

**Proposition 15.2.13.** *Let  $U$  and  $V$  be normed spaces. The constant zero function  $U \rightarrow V$  is a bounded linear transformation with norm 0.*

**Proposition 15.2.14.** *Let  $N \in \mathbb{N}$ . Let  $T : \mathbb{C}^N \rightarrow \mathbb{C}^N$  be a linear transformation with matrix  $A = (a_{ij})$ . Then  $T$  is bounded and*

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

**Definition 15.2.15** (Uniform Convergence). *Let  $U$  and  $V$  be normed spaces. Let  $(T_n)$  be a sequence in  $\mathcal{B}(U, V)$  and  $T \in \mathcal{B}(U, V)$ . Then  $(T_n)$  converges uniformly to  $T$  iff  $(T_n)$  converges to  $T$  under the standard norm defined above.*

**Theorem 15.2.16.** *Let  $U$  and  $V$  be normed spaces. Let  $T : U \rightarrow V$  be a continuous linear function. Then  $\ker T$  is a closed subspace of  $U$ .*

PROOF:

⟨1⟩1.  $\ker T$  is a subspace of  $U$

PROOF: If  $x, y \in \ker T$  and  $\alpha, \beta \in K$  then  $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) = 0$ .

⟨1⟩2.  $\ker T$  is closed.

PROOF: Let  $(x_n)$  be a sequence in  $\ker T$  and  $x_n \rightarrow l$ . Then  $T(l) = \lim_{n \rightarrow \infty} T(x_n) = 0$ .

□

**Theorem 15.2.17.** *Let  $U$  and  $V$  be normed spaces. Let  $W$  be a closed subspace of  $U$  and  $T : W \rightarrow V$  be a continuous linear mapping. Then the graph  $G = \{(x, T(x)) \mid x \in W\}$  is closed in  $U \times V$ .*

PROOF:

⟨1⟩1. ASSUME: w.l.o.g.  $T \neq 0$

⟨1⟩2. LET:  $(x, y) \in (U \times V) - G$ , i.e.  $y \neq T(x)$

⟨1⟩3. LET:  $\epsilon = \|y - T(x)\| > 0$

⟨1⟩4. LET:  $x' \in W$  with  $\|x - x'\| < \epsilon/3\|T\|$

⟨1⟩5. LET:  $y' \in V$  with  $\|y - y'\| < \epsilon/3$

⟨1⟩6.  $y' \neq T(x')$

PROOF:

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

□

**Theorem 15.2.18** (Diagonal Theorem). *Let  $E$  be a normed space over  $K$ . Let  $(x_{ij})$  be an infinite matrix of elements of  $V$ . If:*

1. *For all  $j \in \mathbb{Z}_+$ , we have  $x_{ij} \rightarrow 0$  as  $i \rightarrow \infty$ ;*
2. *Every increasing sequence of positive integers  $(p_j)$  has a subsequence  $(p_{j_r})$  such that*

$$\sum_{s=1}^{\infty} x_{p_{j_r} p_{j_s}} \rightarrow 0 \text{ as } r \rightarrow \infty$$

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

PROOF:

- (1)1. ASSUME: for a contradiction  $x_{ii} \not\rightarrow 0$  as  $i \rightarrow \infty$
- (1)2. PICK  $\epsilon > 0$  such that, for all  $N$ , there exists  $n \geq N$  such that  $\|x_{nn}\| \geq \epsilon$
- (1)3. PICK an increasing sequence of integers  $(p_j)$  such that  $\|x_{p_j p_j}\| \geq \epsilon$  for all  $j$ .
- (1)4. PICK a subsequence  $(q_i)$  such that  $\sum_{j=1}^{\infty} x_{q_i q_j} \rightarrow 0$  as  $i \rightarrow \infty$
- (1)5. For all  $i$ , we have  $x_{q_i q_j} \rightarrow 0$  as  $j \rightarrow \infty$
- (1)6. For all  $j$ , we have  $x_{q_i q_j} \rightarrow 0$  as  $i \rightarrow \infty$
- (1)7. Define a subsequence  $(r_n)$  of  $(q_i)$  by  $r_1 = q_1$  and, for all  $n$ ,  $r_{n+1}$  is the first entry such that  $r_{n+1} > r_n$ ,  $\|x_{q_i r_n}\| < \epsilon/2^{n+1}$  for all  $q_i \geq r_{n+1}$ , and  $\|x_{r_j r_{n+1}}\| < \epsilon/2^{n+2}$  for  $j = 1, \dots, n$ .
- (1)8.  $\|x_{r_i r_j}\| < \epsilon/2^{j+1}$  for all  $i, j$  such that  $i \neq j$
- (1)9. PICK a subsequence  $(s_j)$  of  $(r_j)$  such that  $\sum_{j=1}^{\infty} x_{s_i s_j} \rightarrow 0$  as  $i \rightarrow \infty$
- (1)10. For all  $i$  we have  $\|\sum_{j=1}^{\infty} x_{s_i s_j}\| \geq \epsilon/2$

PROOF:

$$\begin{aligned}\left\| \sum_{j=1}^{\infty} x_{s_i s_j} \right\| &= \left\| x_{s_i s_i} + \sum_{i \neq j} x_{s_i s_j} \right\| \\ &\geq \left| \|x_{s_i s_i}\| - \left\| \sum_{i \neq j} x_{s_i s_j} \right\| \right| && \text{(Proposition 15.0.4)} \\ &\geq \left| \|x_{s_i s_i}\| - \sum_{i \neq j} \|x_{s_i s_j}\| \right| \\ &\geq \epsilon/2 && ((1)2, (1)8)\end{aligned}$$

(1)11. Q.E.D.

PROOF: (1)9 and (1)10 form a contradiction.

□

### 15.3 Banach Spaces

**Definition 15.3.1** (Cauchy Sequence). Let  $V$  be a normed space over  $K$ . A *Cauchy sequence* is a sequence of points  $(x_n)$  such that, for every  $\epsilon > 0$ , there exists  $N$  such that  $\forall m, n \geq N, \|x_m - x_n\| < \epsilon$ .

**Theorem 15.3.2.** Let  $V$  be a normed space over  $K$ . Let  $(x_n)$  be a sequence in  $V$ . The following are equivalent.

1.  $(x_n)$  is Cauchy.
2. For every pair of increasing sequences of positive integers  $(p_n)$  and  $(q_n)$ , we have  $\|x_{p_n} - x_{q_n}\| \rightarrow 0$  as  $n \rightarrow \infty$ .
3. For every increasing sequence of positive integers  $(p_n)$ , we have  $\|x_{p_n} - x_n\| \rightarrow 0$  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  $(q_n)$  are increasing sequences of positive integers.
- $\langle 2 \rangle 3$ . LET:  $\epsilon > 0$
- $\langle 2 \rangle 4$ . PICK  $N$  such that  $\forall m, n \geq N, \|x_m - x_n\| < \epsilon$
- $\langle 2 \rangle 5$ .  $\forall n \geq N, \|x_{p_n} - x_{q_n}\| < \epsilon$

PROOF: Since  $p_n, q_n \geq n \geq N$ .

$\langle 1 \rangle 2. 2 \Rightarrow 3$

PROOF: Trivial.

$\langle 1 \rangle 3. 2 \Rightarrow 1$

- $\langle 2 \rangle 1$ . ASSUME:  $(x_n)$  is not Cauchy
- $\langle 2 \rangle 2$ . Pick  $\epsilon > 0$  such that, for every  $N \in \mathbb{Z}_+$ , there exist  $m_N, n_N \geq N$  such that  $\|x_{m_N} - x_{n_N}\| \geq \epsilon$
- $\langle 2 \rangle 3$ . ASSUME: w.l.o.g.  $(m_N)$  and  $(n_N)$  are increasing sequences.
- $\langle 2 \rangle 4$ .  $\|x_{m_N} - x_{n_N}\| \not\rightarrow 0$  as  $N \rightarrow \infty$ .

$\langle 1 \rangle 4. 3 \Rightarrow 2$

- $\langle 2 \rangle 1$ . ASSUME: 3
- $\langle 2 \rangle 2$ . LET:  $(p_n)$  and  $(q_n)$  be increasing sequences of positive integers.
- $\langle 2 \rangle 3$ . LET:  $\epsilon > 0$
- $\langle 2 \rangle 4$ . PICK  $N$  such that  $\forall n \geq N, \|x_{p_n} - x_n\| < \epsilon/2$  and  $\forall n \geq N, \|x_{q_n} - x_n\| < \epsilon/2$
- $\langle 2 \rangle 5$ .  $\forall n \geq N, \|x_{p_n} - x_{q_n}\| < \epsilon$

□

**Proposition 15.3.3.** Every convergent sequence is Cauchy.

PROOF:

- $\langle 1 \rangle 1$ . LET:  $x_n \rightarrow l$  as  $n \rightarrow \infty$ .
- $\langle 1 \rangle 2$ . LET:  $\epsilon > 0$
- $\langle 1 \rangle 3$ . PICK  $N$  such that  $\forall n \geq N, \|x_n - l\| < \epsilon/2$

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

**Proposition 15.3.4.** *In  $\mathcal{P}([0, 1])$ , let*

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

*Then  $(P_n)$  is Cauchy but does not converge.*

PROOF: It converges to  $e^x$  in  $\mathcal{C}([0, 1])$ , therefore it is Cauchy in  $\mathcal{C}([0, 1])$ , hence Cauchy in  $\mathcal{P}([0, 1])$ . Since  $e^x \notin \mathcal{P}([0, 1])$ , it does not converge in that space.  $\square$

**Proposition 15.3.5.** *Let  $V$  be a normed space over  $K$ . Let  $(x_n)$  be a Cauchy sequence in  $V$ . Then  $(\|x_n\|)$  converges in  $\mathbb{R}$ .*

PROOF:

⟨1⟩1.  $(\|x_n\|)$  is Cauchy.

⟨2⟩1. LET:  $\epsilon > 0$

⟨2⟩2. PICK  $N$  such that  $\forall m, n \geq N. \|x_m - x_n\| < \epsilon$

⟨2⟩3.  $\forall m, n \geq N. \|\|x_m\| - \|x_n\|\| < \epsilon$

PROOF: Proposition 15.0.4.

⟨1⟩2. Q.E.D.

PROOF: Since every Cauchy sequence in  $\mathbb{R}$  converges.

$\square$

**Proposition 15.3.6.** *Every Cauchy sequence is bounded.*

PROOF:

⟨1⟩1. LET:  $V$  be a normed space over  $K$ .

⟨1⟩2. LET:  $(x_n)$  be a Cauchy sequence in  $V$ .

⟨1⟩3. PICK  $N$  such that  $\forall m, n \geq N. \|x_m - x_n\| < 1$ .

⟨1⟩4. LET:  $B = \max(\|x_1\|, \dots, \|x_{N-1}\|, \|x_N\|) + 1$

⟨1⟩5.  $\forall n. \|x_n\| \leq B$

$\square$

**Definition 15.3.7** (Banach Space). A normed space  $V$  over  $K$  is *complete* or a *Banach space* iff every Cauchy sequence converges.

**Proposition 15.3.8.**  *$l^2$  is complete.*

PROOF:

⟨1⟩1. LET:  $(a_n)$  be a Cauchy sequence in  $l^2$  where  $a_n = (\alpha_{n1}, \alpha_{n2}, \dots)$ .

⟨1⟩2. For all  $\epsilon > 0$ , there exists  $n_0 \in \mathbb{Z}_+$  such that  $\forall m, n \geq n_0. \sum_{k=1}^{\infty} |\alpha_{mk} - \alpha_{nk}|^2 < \epsilon^2$ .

⟨1⟩3. For every  $k \in \mathbb{Z}_+$  and  $\epsilon > 0$ , there exists  $n_0 \in \mathbb{Z}_+$  such that  $\forall m, n \geq n_0. |\alpha_{mk} - \alpha_{nk}| < \epsilon$ .

⟨1⟩4. For every  $k \in \mathbb{Z}_+$ ,  $(\alpha_{nk})$  is Cauchy in  $\mathbb{C}$ .

⟨1⟩5. For every  $k \in \mathbb{Z}_+$ ,  $(\alpha_{nk})$  converges in  $\mathbb{C}$ .

⟨1⟩6. For  $k \in \mathbb{Z}_+$ ,

- LET:  $\alpha_k = \lim_{n \rightarrow \infty} \alpha_{nk}$
- ⟨1⟩7. Let  $a$  be the sequence  $(\alpha_k)$
- ⟨1⟩8. For all  $\epsilon > 0$ , there exists  $n_0$  such that  $\forall n \geq n_0. \sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2 \leq \epsilon^2$ .
- PROOF: Letting  $m \rightarrow \infty$  in ⟨1⟩2.
- ⟨1⟩9.  $a \in l^2$
- ⟨2⟩1. PICK  $n_0$  such that  $\forall n \geq n_0. \sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2 \leq 1$
- PROOF: ⟨1⟩8
- ⟨2⟩2.  $(\alpha_k - \alpha_{n_0 k}) \in l^2$
- ⟨2⟩3.  $(\alpha_{n_0 k}) \in l^2$
- PROOF: By ⟨1⟩1 since the sequence is  $a_{n_0}$ .
- ⟨2⟩4.  $(\alpha_k) \in l^2$
- PROOF: Proposition 13.0.2.
- ⟨1⟩10.  $a_n \rightarrow a$  as  $n \rightarrow \infty$
- PROOF: By ⟨1⟩8 since  $\|a - a_n\| = \sqrt{\sum_{k=1}^{\infty} |\alpha_k - \alpha_{nk}|^2}$ .
- 

**Proposition 15.3.9.** *Let  $a$  and  $b$  be real numbers with  $a < b$ . The space  $\mathcal{C}([a, b])$  is complete.*

PROOF:

- ⟨1⟩1. LET:  $X = [a, b]$
- ⟨1⟩2. LET:  $(f_n)$  be a Cauchy sequence in  $\mathcal{C}([a, b])$ .
- ⟨1⟩3. For all  $\epsilon > 0$ , there exists  $n_0$  such that  $\forall n, m \geq n_0. \|f_n - f_m\| < \epsilon$ .
- ⟨1⟩4. For all  $\epsilon > 0$ , there exists  $n_0$  such that  $\forall n, m \geq n_0. \forall x \in X. |f_n(x) - f_m(x)| < \epsilon$ .
- ⟨1⟩5. For all  $x \in [a, b]$ ,  $(f_n(x))$  is Cauchy.
- ⟨1⟩6. Define  $f : [a, b] \rightarrow \mathbb{C}$  by  $f(x) = \lim_{n \rightarrow \infty} f_n(x)$ .
- ⟨1⟩7. For all  $\epsilon > 0$ , there exists  $n_0$  such that  $\forall n \geq n_0. \forall x \in X. |f_n(x) - f(x)| < \epsilon$
- PROOF: Letting  $m \rightarrow \infty$  in ⟨1⟩4.
- ⟨1⟩8.  $f$  is continuous
- ⟨2⟩1. LET:  $x_0 \in X$
- ⟨2⟩2. LET:  $\epsilon > 0$
- ⟨2⟩3. PICK  $n_0$  such that  $\forall n \geq n_0. \forall x \in X. |f_n(x) - f(x)| < \epsilon/3$
- PROOF: By ⟨1⟩7.
- ⟨2⟩4. PICK  $\delta > 0$  such that  $\forall x \in X. |x - x_0| < \delta \Rightarrow |f_{n_0}(x) - f_{n_0}(x_0)| < \epsilon/3$
- PROOF: Since  $f_{n_0}$  is continuous.
- ⟨2⟩5. LET:  $x \in X$
- ⟨2⟩6. ASSUME:  $|x - x_0| < \delta$
- ⟨2⟩7.  $|f(x) - f(x_0)| < \epsilon$
- PROOF:
- $$|f(x) - f(x_0)| \leq |f(x) - f_{n_0}(x)| + |f_{n_0}(x) - f_{n_0}(x_0)| + |f_{n_0}(x_0) - f(x_0)| \quad (\text{Triangle Inequality})$$
- $$< \epsilon/3 + \epsilon/3 + \epsilon/3 \quad (\langle 2 \rangle 3, \langle 2 \rangle 4)$$
- $$= \epsilon$$
- ⟨1⟩9.  $(f_n)$  converges to  $f$  uniformly.
- PROOF: From ⟨1⟩7
-



**Definition 15.3.10** (Series). Let  $V$  be a normed space over  $K$ . A *convergent series* in  $V$  is a sequence  $(x_n)$  in  $V$  such that  $(x_1 + \cdots + x_n)$  is a convergent sequence, in which case we write  $\sum_{n=1}^{\infty} x_n$  for its limit.

**Definition 15.3.11** (Absolutely Convergent Series). Let  $V$  be a normed space over  $K$ . An *absolutely convergent series* in  $V$  is a sequence  $(x_n)$  such that  $\sum_{n=1}^{\infty} \|x_n\| < \infty$ .

**Proposition 15.3.12.** In  $\mathcal{P}([0, 1])$ , the series  $\sum_{n=0}^{\infty} x^n/n!$  is absolutely convergent but not convergent.

PROOF: Proposition 15.3.4.  $\square$

**Theorem 15.3.13.** A normed space is complete if and only if every absolutely convergent series is convergent.

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a normed space over  $K$ .

$\langle 1 \rangle 2$ . If  $V$  is complete then every absolutely convergent series is convergent.

$\langle 2 \rangle 1$ . ASSUME:  $V$  is complete.

$\langle 2 \rangle 2$ . LET:  $\sum_{n=1}^{\infty} a_n$  be absolutely convergent in  $V$ .

$\langle 2 \rangle 3$ . For  $n \in \mathbb{Z}_+$ ,  
LET:  $s_n = \sum_{k=1}^n a_k$

$\langle 2 \rangle 4$ .  $(s_n)$  is Cauchy.

$\langle 3 \rangle 1$ . LET:  $\epsilon > 0$

$\langle 3 \rangle 2$ . PICK  $k$  such that  $\sum_{n=k+1}^{\infty} \|a_n\| < \epsilon$

$\langle 3 \rangle 3$ . LET:  $m > n > k$

$\langle 3 \rangle 4$ .  $\|s_m - s_n\| < \epsilon$

PROOF:

$$\begin{aligned} \|s_m - s_n\| &= \left\| \sum_{i=n+1}^m a_i \right\| && (\langle 2 \rangle 3, \langle 3 \rangle 3) \\ &\leq \sum_{i=n+1}^m \|a_i\| && (\text{Triangle inequality}) \\ &\leq \sum_{i=k+1}^{\infty} \|a_i\| \\ &< \epsilon && (\langle 3 \rangle 2, \langle 3 \rangle 3) \end{aligned}$$

$\langle 2 \rangle 5$ .  $(s_n)$  converges.

$\langle 1 \rangle 3$ . If every absolutely convergent series is convergent then  $V$  is complete.

$\langle 2 \rangle 1$ . ASSUME: Every absolutely convergent series in  $V$  is convergent.

$\langle 2 \rangle 2$ . LET:  $(a_n)$  be a Cauchy sequence in  $V$ .

$\langle 2 \rangle 3$ . PICK a strictly increasing sequence of positive integers  $(p_n)$  such that  
 $\forall k. \forall m, n \geq p_k. \|x_m - x_n\| < 2^{-k}$ .

$\langle 2 \rangle 4$ .  $\sum_{k=1}^{\infty} (x_{p_{k+1}} - x_{p_k})$  is absolutely convergent.

PROOF:

$$\sum_{k=1}^{\infty} \|x_{p_{k+1}} - x_{p_k}\| < \sum_{k=1}^{\infty} 2^{-k} \quad (\langle 2 \rangle 3)$$

$$< \infty$$

$\langle 2 \rangle 5$ .  $\sum_{k=1}^{\infty} (x_{p_{k+1}} - x_{p_k})$  is convergent.

PROOF:  $\langle 2 \rangle 1$ ,  $\langle 2 \rangle 5$

$\langle 2 \rangle 6$ . LET:  $s = \sum_{k=1}^{\infty} (x_{p_{k+1}} - x_{p_k})$

$\langle 2 \rangle 7$ .  $x_{p_k} \rightarrow s + x_{p_1}$  as  $k \rightarrow \infty$ .

$\langle 3 \rangle 1$ .  $\sum_{i=1}^k (x_{p_{i+1}} - x_{p_i}) \rightarrow s$  as  $k \rightarrow \infty$

PROOF:  $\langle 2 \rangle 6$

$\langle 3 \rangle 2$ .  $x_{p_{k+1}} - x_{p_1} \rightarrow s$  as  $k \rightarrow \infty$

$\langle 2 \rangle 8$ .  $x_n \rightarrow s + x_{p_1}$  as  $k \rightarrow \infty$ .

PROOF:

$\langle 3 \rangle 1$ . LET:  $\epsilon > 0$

$\langle 3 \rangle 2$ . PICK  $N$  such that  $\forall k \geq N, \|x_{p_k} - (s + x_{p_1})\| < \epsilon/2$  and  $\forall m, n \geq N, \|x_m - x_n\| < \epsilon/2$

PROOF:  $\langle 2 \rangle 2$ ,  $\langle 2 \rangle 7$

$\langle 3 \rangle 3$ .  $\forall n \geq N, \|x_n - (s + x_{p_1})\| < \epsilon$

□

**Theorem 15.3.14.** *A closed vector subspace of a Banach space is a Banach space.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $V$  be a Banach space over  $K$ .

$\langle 1 \rangle 2$ . LET:  $U$  be a closed vector subspace of  $V$ .

$\langle 1 \rangle 3$ . LET:  $(a_n)$  be a Cauchy sequence in  $U$ .

$\langle 1 \rangle 4$ .  $(a_n)$  is a Cauchy sequence in  $V$ .

$\langle 1 \rangle 5$ . LET:  $l = \lim_{n \rightarrow \infty} a_n$

$\langle 1 \rangle 6$ .  $l \in U$

PROOF: Theorem 15.1.40.

$\langle 1 \rangle 7$ .  $a_n \rightarrow l$  as  $n \rightarrow \infty$  in  $U$ .

□

**Definition 15.3.15** (Completion). Let  $V$  be a normed space over  $K$ . A *completion* of  $V$  consists of a normed space  $W$  over  $K$  and an injection  $\phi : V \rightarrow W$  such that:

$$1. \forall x, y \in V, \forall \alpha, \beta \in K, \phi(\alpha x + \beta y) = \alpha \phi(x) + \beta \phi(y)$$

$$2. \forall x \in V, \|\phi(x)\| = \|x\|$$

3.  $\phi(V)$  is dense in  $W$ .

4.  $W$  is complete.

**Proposition 15.3.16.** *Every normed space has a completion.*

PROOF:

- (1)1. LET:  $V$  be a normed space over  $K$ .  
 (1)2. Let us say two Cauchy sequences  $(x_n), (y_n)$  are *equivalent* iff  $x_n - y_n \rightarrow 0$  as  $n \rightarrow \infty$ .  
 (1)3. Equivalence is an equivalence relation on the set of Cauchy sequences.  
 (1)4. LET:  $W$  be the set of Cauchy sequences in  $V$  quotiented by equivalence.  
 (1)5. Define addition and multiplication on  $W$  by

$$\begin{aligned}
 [(x_n)] + [(y_n)] &= [(x_n + y_n)] \\
 \lambda[(x_n)] &= [(\lambda x_n)]
 \end{aligned}$$

- (1)6. Define a norm on  $W$  by  $\|[(x_n)]\| = \lim_{n \rightarrow \infty} \|x_n\|$   
 (1)7. Define  $\phi : V \rightarrow W$  by  $\phi(v) = [(v)]$ .  
 (1)8.  $\phi$  is injective.  
 (1)9.  $\forall x, y \in V. \forall \alpha, \beta \in K. \phi(\alpha x + \beta y) = \alpha \phi(x) + \beta \phi(y)$   
 (1)10.  $\forall x \in V. \|\phi(x)\| = \|x\|$   
 (1)11.  $\phi(V)$  is dense in  $W$ .

- (2)1. LET:  $[(a_n)] \in W$  and  $\epsilon > 0$ .

PROVE:  $B([(a_n)], \epsilon)$  intersects  $\phi(V)$ .

- (2)2. PICK  $N$  such that  $\forall m, n \geq N. \|a_m - a_n\| < \epsilon/2$

- (2)3.  $\phi(a_N) \in B([(a_n)], \epsilon)$

PROOF:

$$\begin{aligned}
 \|[(a_n)] - \phi(a_N)\| &= \lim_{n \rightarrow \infty} \|a_n - a_N\| \\
 &\leq \epsilon/2 & (\langle 2 \rangle 2) \\
 &< \epsilon
 \end{aligned}$$

- (1)12.  $W$  is complete.

- (2)1. LET:  $(X_n)$  be a Cauchy sequence in  $W$ .

- (2)2. For  $n \in \mathbb{Z}_+$ , PICK  $x_n \in V$  such that

$$\|\phi(x_n) - X_n\| < 1/n.$$

- (2)3.  $(x_n)$  is Cauchy in  $V$ .

- (3)1. LET:  $\epsilon > 0$

- (3)2. PICK  $N$  such that  $\forall m, n \geq N. \|X_n - X_m\| < \epsilon/3$  and  $1/N < \epsilon/3$

- (3)3. LET:  $m, n \geq N$

- (3)4.  $\|x_m - x_n\| < \epsilon$

PROOF:

$$\begin{aligned}
 \|x_m - x_n\| &= \|\phi(x_m) - \phi(x_n)\| \\
 &\leq \|\phi(x_m) - X_m\| + \|X_m - X_n\| + \|X_n - \phi(x_n)\| \\
 &< \|X_m - X_n\| + 1/m + 1/n \\
 &< \epsilon
 \end{aligned}$$

- (2)4. LET:  $X = [(x_n)]$

- (2)5.  $X_n \rightarrow X$  as  $n \rightarrow \infty$

PROOF:

$$\begin{aligned}
 \|X_n - X\| &\leq \|X_n - \phi(x_n)\| + \|\phi(x_n) - X\| \\
 &< \|\phi(x_n) - X\| + 1/n \\
 &\rightarrow 0
 \end{aligned}$$

as  $n \rightarrow \infty$

□

**Proposition 15.3.17.** *Let  $U$  be a normed space and  $V$  a Banach space. Then  $\mathcal{B}(U, V)$  is a Banach space.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $(T_n)$  be a Cauchy sequence in  $\mathcal{B}(U, V)$

$\langle 1 \rangle 2$ . For all  $u \in U$ ,  $(T_n(u))$  is a Cauchy sequence in  $V$ .

$\langle 2 \rangle 1$ . LET:  $u \in U$

$\langle 2 \rangle 2$ . LET:  $\epsilon > 0$

PROVE:  $\exists N. \forall m, n \geq N. \|T_m(u) - T_n(u)\| < \epsilon$

$\langle 2 \rangle 3$ . ASSUME: w.l.o.g.  $u \neq 0$

$\langle 2 \rangle 4$ . PICK  $N$  such that  $\forall m, n \geq N. \|T_m - T_n\| < \epsilon/\|u\|$

$\langle 2 \rangle 5$ . LET:  $m, n \geq N$

$\langle 2 \rangle 6$ .  $\|T_m(u) - T_n(u)\| < \epsilon$

PROOF:

$$\|T_m(u) - T_n(u)\| \leq \|T_m - T_n\| \|u\| \quad (\text{Proposition 15.2.11})$$

$$< \epsilon$$

$\langle 1 \rangle 3$ . Define  $T : U \rightarrow V$  by  $T(u) = \lim_{n \rightarrow \infty} T_n(u)$

$\langle 1 \rangle 4$ .  $T \in \mathcal{B}(U, V)$

$\langle 2 \rangle 1$ . For all  $x, y \in U$  and  $\alpha, \beta \in K$  we have  $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$

$\langle 3 \rangle 1$ . LET:  $x, y \in U$

$\langle 3 \rangle 2$ . LET:  $\alpha, \beta \in K$

$\langle 3 \rangle 3$ .  $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$

PROOF:

$$\begin{aligned} T(\alpha x + \beta y) &= \lim_{n \rightarrow \infty} T_n(\alpha x + \beta y) \\ &= \lim_{n \rightarrow \infty} (\alpha T_n(x) + \beta T_n(y)) \\ &= \alpha T(x) + \beta T(y) \end{aligned}$$

$\langle 2 \rangle 2$ .  $T$  is bounded.

$\langle 3 \rangle 1$ . PICK  $N$  such that  $\forall n \geq N. \|T_n - T\| < 1$

$\langle 3 \rangle 2$ . PICK  $B > 0$  such that  $\forall x \in U. \|T_N(x)\| \leq B\|x\|$

$\langle 3 \rangle 3$ . LET:  $x \in U$

$\langle 3 \rangle 4$ .  $\|T(x)\| \leq (B + 1)\|x\|$

PROOF:

$$\begin{aligned} \|T(x)\| &\leq \|T_N(x) - T(x)\| + \|T_N(x)\| && (\text{Triangle inequality}) \\ &\leq \|T_N - T\| \|x\| + \|T_N\| \|x\| && (\text{Proposition 15.2.11}) \\ &< \|x\| + B\|x\| && (\langle 3 \rangle 1, \langle 3 \rangle 2) \\ &= (B + 1)\|x\| \end{aligned}$$

$\langle 1 \rangle 5$ .  $T_n \rightarrow T$  as  $n \rightarrow \infty$

$\langle 2 \rangle 1$ . LET:  $\epsilon > 0$

$\langle 2 \rangle 2$ . PICK  $N$  such that  $\forall m, n \geq N. \|T_m - T_n\| < \epsilon/2$

$\langle 2 \rangle 3$ . LET:  $n \geq N$

PROVE:  $\|T_n - T\| < \epsilon$

$\langle 2 \rangle 4$ . LET:  $x \in U$  with  $\|x\| = 1$

$\langle 2 \rangle 5$ .  $\|T_n(x) - T(x)\| \leq \epsilon/2$

PROOF: Let  $n \rightarrow \infty$  in  $\langle 2 \rangle 2$ .

□

**Corollary 15.3.17.1.** *For any normed space  $V$  over  $K$ , the space  $\mathcal{B}(V, K)$  is a Banach space.*

**Theorem 15.3.18.** *Let  $U$  be a normed space and  $V$  a Banach space. Let  $W$  be a subspace of  $U$ . Let  $T : W \rightarrow V$  be a continuous linear transformation. Then  $T$  has a unique extension to a continuous linear transformation  $\text{cl } W \rightarrow V$ .*

PROOF:

- (1)1. Define  $S : \text{cl } W \rightarrow V$  by:  $S(x) = \lim_{n \rightarrow \infty} T(x_n)$ , where  $(x_n)$  is any sequence in  $W$  that converges to  $x$ .
- (2)1. For all  $x \in \text{cl } W$ , there exists a sequence  $(x_n)$  in  $W$  that converges to  $x$ .  
PROOF: Theorem 15.1.43.
- (2)2. If  $(x_n)$  is a Cauchy sequence in  $W$  then  $(T(x_n))$  is Cauchy in  $V$ .
  - (3)1. ASSUME: w.l.o.g.  $T \neq 0$
  - (3)2. LET:  $(x_n)$  be a Cauchy sequence in  $W$ .
  - (3)3. PICK  $B > 0$  such that  $\forall x \in W. \|T(x)\| \leq B\|x\|$
  - (3)4. LET:  $\epsilon > 0$
  - (3)5. PICK  $N$  such that  $\forall m, n \geq N. \|x_m - x_n\| < \epsilon/\|T\|$
  - (3)6. LET:  $m, n \geq N$
  - (3)7.  $\|T(x_m) - T(x_n)\| < \epsilon$
- (2)3. If  $(x_n)$  and  $(y_n)$  are sequences in  $W$  that converge to the same element in  $\text{cl } W$  then  $(T(x_n))$  and  $(T(y_n))$  have the same limit in  $V$ .
  - (3)1. ASSUME: w.l.o.g.  $T \neq 0$
  - (3)2. ASSUME:  $x_n \rightarrow l$  and  $y_n \rightarrow l$  as  $n \rightarrow \infty$
  - (3)3. LET:  $T(x_n) \rightarrow a$  and  $T(y_n) \rightarrow b$  as  $n \rightarrow \infty$
  - (3)4. ASSUME: for a contradiction  $a \neq b$
  - (3)5. LET:  $\epsilon = \|a - b\|$
  - (3)6. PICK  $N$  such that  $\forall n \geq N. \|x_n - l\| < \epsilon/3\|T\|$  and  $\forall n \geq N. \|y_n - l\| < \epsilon/3\|T\|$
  - (3)7.  $\forall n \geq N. \|T(x_n) - T(y_n)\| < 2\epsilon/3$
  - (3)8.  $\|a - b\| \leq 2\epsilon/3$
  - (3)9. This contradicts (3)5.
- (1)2.  $S$  extends  $T$ 
  - (2)1. LET:  $w \in W$
  - (2)2.  $w \rightarrow w$  as  $n \rightarrow \infty$
  - (2)3.  $T(w) \rightarrow T(w)$  as  $n \rightarrow \infty$
  - (2)4.  $S(w) = T(w)$
- (1)3.  $S$  is bounded.
  - (2)1. LET:  $x \in \text{cl } W$   
PROVE:  $\|S(x)\| \leq \|T\|\|x\|$
  - (2)2. PICK a sequence  $(x_n)$  in  $W$  that converges to  $x$ .
  - (2)3.  $\|T(x_n)\| \leq \|T\|\|x_n\|$  for all  $n$ .
  - (2)4.  $\|S(x)\| \leq \|T\|\|x\|$
- PROOF: Taking the limit as  $n \rightarrow \infty$ .
- (1)4.  $S$  is linear.

- ⟨2⟩1. LET:  $x, y \in \text{cl } W$  and  $\alpha, \beta \in K$
- ⟨2⟩2. PICK sequences  $(x_n)$  and  $(y_n)$  in  $W$  that converge to  $x$  and  $y$ .
- ⟨2⟩3.  $T(\alpha x_n + \beta y_n) = \alpha T(x_n) + \beta T(y_n)$  for all  $n$ .
- ⟨2⟩4.  $S(\alpha x + \beta y) = \alpha S(x) + \beta S(y)$

PROOF: Taking the limit as  $n \rightarrow \infty$ .

- ⟨1⟩5.  $S$  is unique.
- ⟨2⟩1. LET:  $S'$  be a continuous linear extension of  $S$  defined on  $\text{cl } W$ .
- ⟨2⟩2. LET:  $x \in W$
- PROVE:  $S(x) = S'(x)$
- ⟨2⟩3. PICK a sequence  $(x_n)$  in  $W$  that converges to  $x$ .
- ⟨2⟩4.  $T(x_n) = S'(x_n) \rightarrow S'(x)$  as  $n \rightarrow \infty$
- ⟨2⟩5.  $S'(x) = S(x)$

□

**Corollary 15.3.18.1.** *Let  $U$  be a normed space and  $V$  a Banach space. Let  $W$  be a dense subspace of  $U$ . Let  $T : W \rightarrow V$  be a continuous linear transformation. Then  $T$  has a unique extension to a continuous linear transformation  $U \rightarrow V$ .*

**Definition 15.3.19** (Functional). Let  $V$  be a normed space over  $K$ . A *functional* on  $V$  is a bounded linear mapping  $V \rightarrow K$ . The *dual space* of  $V$  is the space  $\mathcal{B}(V, K)$  of all functionals.

**Theorem 15.3.20** (Banach-Steinhaus Theorem). *Let  $\mathcal{T}$  be a family of bounded linear mappings from a Banach space  $X$  into a normed space  $Y$ . If, for every  $x \in X$ , there exists a constant  $M_x$  such that  $\forall T \in \mathcal{T}. \|T(x)\| \leq M_x$ , then there exists a constant  $M > 0$  such that  $\forall T \in \mathcal{T}. \|T\| \leq M$ .*

PROOF:

- ⟨1⟩1. ASSUME: for a contradiction no such  $M$  exists.
- ⟨1⟩2. For  $n \in \mathbb{Z}_+$ , PICK  $T_n \in \mathcal{T}$  such that  $\|T_n\| > n2^n$ .
- ⟨1⟩3. For  $n \in \mathbb{Z}_+$ , PICK  $x_n \in X$  such that  $\|x_n\| = 1$  and  $\|T_n(x_n)\| > n2^n$ .
- ⟨1⟩4. For  $n \in \mathbb{Z}_+$ ,

$$\left\| \frac{1}{n} T_n \left( \frac{x_n}{2^n} \right) \right\| > 1 .$$

- ⟨1⟩5. For  $i, j \in \mathbb{Z}_+$ ,  
LET:  $y_{ij} = \frac{1}{i} T_i \left( \frac{x_j}{2^j} \right)$ .
  - ⟨1⟩6. For all  $j \in \mathbb{Z}_+$ ,  $y_{ij} \rightarrow 0$  as  $i \rightarrow \infty$ 
    - ⟨2⟩1. LET:  $j \in \mathbb{Z}_+$
    - ⟨2⟩2. PICK  $M$  such that  $\forall T \in \mathcal{T}. \|T(x_j/2^j)\| \leq M$
    - ⟨2⟩3. For all  $i$ ,  $\|y_{ij}\| \leq M/i$
  - ⟨1⟩7. For any increasing sequence of positive integers  $(p_i)$ , we have  $\sum_{j=1}^{\infty} y_{p_i p_j} \rightarrow 0$  as  $i \rightarrow \infty$ 
    - ⟨2⟩1. LET:  $(p_i)$  be an increasing sequence of positive integers.
    - ⟨2⟩2. LET:  $z = \sum_{j=1}^{\infty} x_{p_j} / 2^{p_j}$
- PROOF: This converges by Theorem 15.3.13.
- ⟨2⟩3. PICK  $C$  such that  $\forall T \in \mathcal{T}. \|T(z)\| \leq C$
  - ⟨2⟩4. For all  $i$ ,  $\|\sum_{j=1}^{\infty} y_{p_i p_j}\| \leq C/p_i$ .

PROOF:

$$\left\| \sum_{j=1}^{\infty} y_{p_i p_j} \right\| = \left\| \sum_{j=1}^{\infty} \frac{1}{p_i} T_{p_i} \left( \frac{x_{p_j}}{2^{p_j}} \right) \right\| \quad (\langle 1 \rangle 5)$$

$$= \frac{1}{p_i} \left\| T_{p_i} \left( \sum_{j=1}^{\infty} \frac{x_{p_j}}{2^{p_j}} \right) \right\| \quad (T_{p_i} \text{ continuous})$$

$$= \frac{1}{p_i} \|T_{p_i}(z)\| \quad (\langle 2 \rangle 2)$$

$$\leq \frac{C}{p_i} \quad (\langle 2 \rangle 3)$$

$$\langle 2 \rangle 5. \sum_{j=1}^{\infty} y_{p_i p_j} \rightarrow 0 \text{ as } i \rightarrow \infty$$

$$\langle 1 \rangle 8. y_{ii} \rightarrow 0 \text{ as } i \rightarrow \infty$$

PROOF: Diagonal Theorem,  $\langle 1 \rangle 6$ ,  $\langle 1 \rangle 7$ . $\langle 1 \rangle 9$ . Q.E.D.PROOF:  $\langle 1 \rangle 4$  and  $\langle 1 \rangle 8$  form a contradiction.

□

## 15.4 Contraction Mappings

**Definition 15.4.1** (Contraction Mapping). Let  $E$  be a normed space over  $K$ . Let  $A \subseteq E$ . A function  $f : A \rightarrow E$  is a *contraction (mapping)* iff there exists a real  $\alpha$  such that  $0 < \alpha < 1$  and

$$\forall x, y \in A. \|f(x) - f(y)\| \leq \alpha \|x - y\| .$$

**Proposition 15.4.2.** *Contraction mappings are uniformly continuous.*

PROOF:

 $\langle 1 \rangle 1$ . LET:  $E$  be a normed space over  $K$ . $\langle 1 \rangle 2$ . LET:  $A \subseteq E$  $\langle 1 \rangle 3$ . LET:  $f : A \rightarrow E$  be a contraction mapping. $\langle 1 \rangle 4$ . PICK  $\alpha$  such that  $0 < \alpha < 1$  and  $\forall x, y \in A. \|f(x) - f(y)\| \leq \alpha \|x - y\|$ . $\langle 1 \rangle 5$ . LET:  $\epsilon > 0$  $\langle 1 \rangle 6$ . LET:  $\delta = \epsilon/\alpha$  $\langle 1 \rangle 7$ . For all  $x, y \in A$ , if  $\|x - y\| < \delta$  then  $\|f(x) - f(y)\| < \epsilon$ .

□

**Theorem 15.4.3** (Banach Fixed Point Theorem). *Let  $E$  be a Banach space over  $K$ . Let  $F$  be a nonempty closed subset of  $E$ . Let  $f : F \rightarrow F$  be a contraction mapping. Then there exists a unique  $z \in F$  such that  $f(z) = z$ .*

PROOF:

 $\langle 1 \rangle 1$ . PICK  $\alpha$  such that  $0 < \alpha < 1$  and

$$\forall x, y \in F. \|f(x) - f(y)\| \leq \alpha \|x - y\| .$$

 $\langle 1 \rangle 2$ . PICK  $x_0 \in F$

$\langle 1 \rangle 3$ . For  $n \in \mathbb{Z}_+$ ,

LET:  $x_n = f^n(x_0)$ .

$\langle 1 \rangle 4$ .  $(x_n)$  is a Cauchy sequence.

$\langle 2 \rangle 1$ . For all  $n \in \mathbb{Z}_+$  we have  $\|x_{n+1} - x_n\| \leq \alpha^n \|x_1 - x_0\|$ .

$\langle 2 \rangle 2$ . For all  $m, n \in \mathbb{Z}_+$  with  $m < n$  we have  $\|x_n - x_m\| < \alpha^m \|x_1 - x_0\| / (1 - \alpha)$ .

PROOF:

$$\|x_n - x_m\| \leq \|x_n - x_{n-1}\| + \|x_{n-1} - x_{n-2}\| + \cdots + \|x_{m+1} - x_m\| \quad (\text{Triangle inequality})$$

$$\leq (\alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha^m) \|x_1 - x_0\| \quad (\langle 2 \rangle 1)$$

$$< \frac{\|x_1 - x_0\|}{1 - \alpha} \alpha^m$$

$\langle 2 \rangle 3$ . LET:  $\epsilon > 0$

$\langle 2 \rangle 4$ . PICK  $N$  such that  $\alpha^N \|x_1 - x_0\| / (1 - \alpha) < \epsilon$

$\langle 2 \rangle 5$ . For all  $m, n \geq N$ , we have  $\|x_n - x_m\| < \epsilon$

$\langle 1 \rangle 5$ . LET:  $z = \lim_{n \rightarrow \infty} x_n$

$\langle 1 \rangle 6$ .  $f(z) = z$

PROOF:

$$\begin{aligned} f(z) &= f\left(\lim_{n \rightarrow \infty} x_n\right) \\ &= \lim_{n \rightarrow \infty} f(x_n) && (\text{Proposition 15.4.2}) \\ &= \lim_{n \rightarrow \infty} x_{n+1} \\ &= z \end{aligned}$$

$\langle 1 \rangle 7$ . For any  $w \in F$ , if  $f(w) = w$  then  $w = z$ .

$\langle 2 \rangle 1$ . LET:  $w \in F$

$\langle 2 \rangle 2$ . ASSUME:  $f(w) = w$

$\langle 2 \rangle 3$ .  $\|z - w\| \leq \alpha \|z - w\|$

PROOF:  $\|z - w\| = \|f(z) - f(w)\| \leq \alpha \|z - w\|$

$\langle 2 \rangle 4$ .  $\|z - w\| = 0$

$\langle 2 \rangle 5$ .  $z = w$

□



## Chapter 16

# Inner Product Spaces

**Definition 16.0.1** (Inner Product Space). Let  $E$  be a complex vector space. An *inner product* on  $E$  is a function  $\langle \cdot, \cdot \rangle : E^2 \rightarrow \mathbb{C}$  such that, for all  $x, y, z \in E$  and  $\alpha, \beta \in \mathbb{C}$ , we have:

1.  $\langle x, y \rangle = \overline{\langle y, x \rangle}$
2.  $\langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle$
3.  $\langle x, x \rangle \geq 0$
4. If  $\langle x, x \rangle = 0$  then  $x = 0$

An *inner product space* consists of a complex vector space  $V$  and an inner product on  $V$ .

**Proposition 16.0.2.** Let  $E$  be an inner product space. For any  $x \in E$ , we have  $\langle x, x \rangle$  is real.

PROOF: Since  $\langle x, x \rangle = \overline{\langle x, x \rangle}$ .  $\square$

**Proposition 16.0.3.**

$$\langle x, \alpha y + \beta z \rangle = \overline{\alpha} \langle x, y \rangle + \overline{\beta} \langle x, z \rangle$$

**Proposition 16.0.4.**

$$\langle 0, y \rangle = \langle x, 0 \rangle = 0$$

**Proposition 16.0.5.** The function  $\langle \vec{x}, \vec{y} \rangle = \sum_{i=1}^n x_i \overline{y_i}$  is an inner product on  $\mathbb{C}^n$ .

**Proposition 16.0.6.** The function  $\langle (x_n), (y_n) \rangle = \sum_{i=1}^{\infty} x_i \overline{y_i}$  is an inner product on  $l^2$ .

**Proposition 16.0.7.** The function  $\langle f, g \rangle = \int_a^b f(x) \overline{g(x)} dx$  is an inner product on  $\mathcal{C}([a, b])$ .

**Proposition 16.0.8.** *Let  $p > 1$  and  $\Omega \subseteq \mathbb{R}^N$ . Let  $L^p(\Omega)$  be the set of all functions  $f : \Omega \rightarrow \mathbb{C}$  such that  $|f|^p$  is Lebesgue integrable.*

*The function  $\langle f, g \rangle = \int_{\Omega} f(x)g(x)dx$  is an inner product on  $L^2(\Omega)$ .*

**Proposition 16.0.9.** *Let  $E_1$  and  $E_2$  be inner product spaces. Then the function  $\langle (e_1, e_2), (e'_1, e'_2) \rangle = \langle e_1, e'_1 \rangle + \langle e_2, e'_2 \rangle$  is an inner product on  $E_1 \times E_2$ .*

**Definition 16.0.10** (Norm). In an inner product space, define  $\|x\| = \sqrt{\langle x, x \rangle}$ .

**Proposition 16.0.11** (Schwarz's Inequality). *In any inner product space,*

$$|\langle x, y \rangle| \leq \|x\| \|y\| .$$

*Equality holds iff  $x$  and  $y$  are linearly dependent.*

PROOF:

$\langle 1 \rangle 1$ . ASSUME: w.l.o.g.  $y \neq 0$

$\langle 1 \rangle 2$ .  $|\langle x, y \rangle| \leq \|x\| \|y\|$

$\langle 2 \rangle 1$ . For all  $\alpha \in \mathbb{C}$  we have  $\langle x, x \rangle + \bar{\alpha} \langle x, y \rangle + \alpha \langle y, x \rangle + |\alpha|^2 \langle y, y \rangle$

PROOF: The right-hand side is  $\langle x + \alpha y, x + \alpha y \rangle$ .

$\langle 2 \rangle 2$ .  $\langle x, x \rangle \langle y, y \rangle - |\langle x, y \rangle|^2 \geq 0$

PROOF: Taking  $\alpha = -\langle x, x \rangle / \langle y, y \rangle$  in  $\langle 2 \rangle 1$ .

$\langle 1 \rangle 3$ . If  $|\langle x, y \rangle| = \|x\| \|y\|$  then  $x$  and  $y$  are linearly dependent.

$\langle 2 \rangle 1$ . ASSUME:  $|\langle x, y \rangle| = \|x\| \|y\|$

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

$\langle 2 \rangle 3$ .  $\langle y, y \rangle x - \langle x, x \rangle y = 0$

PROOF:

$$\begin{aligned} \langle \langle y, y \rangle x - \langle x, x \rangle y, \langle y, y \rangle x - \langle x, x \rangle y \rangle &= \langle y, y \rangle^2 \langle x, x \rangle - \langle y, y \rangle \langle y, x \rangle \langle x, y \rangle - \langle x, y \rangle \langle y, y \rangle \langle y, x \rangle + \langle x, y \rangle \langle y, x \rangle \langle x, x \rangle \\ &= 0 \end{aligned}$$

$\langle 1 \rangle 4$ . If  $x$  and  $y$  are linearly dependent then  $|\langle x, y \rangle| = \|x\| \|y\|$

$\langle 2 \rangle 1$ . ASSUME:  $x$  and  $y$  are linearly dependent.

$\langle 2 \rangle 2$ . LET:  $y = \alpha x$

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

PROOF:

$$\begin{aligned} |\langle x, y \rangle| &= |\langle x, \alpha x \rangle| \\ &= |\alpha| |\langle x, x \rangle| \\ &= |\alpha| \|x\|^2 \\ &= \|x\| \|\alpha x\| \\ &= \|x\| \|y\| \end{aligned}$$

□

**Corollary 16.0.11.1** (Triangle Inequality). *In any inner product space,*

$$\|x + y\| \leq \|x\| + \|y\|$$

PROOF:

$$\begin{aligned}
\|x + y\|^2 &= \langle x + y, x + y \rangle \\
&= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\
&\leq \langle x, x \rangle + 2|\langle x, y \rangle| + \langle y, y \rangle \\
&\leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 && \text{(Schwarz's Inequality)} \\
&= (\|x\| + \|y\|)^2 && \square
\end{aligned}$$

**Corollary 16.0.11.2.** *The norm in an inner product space is a norm.*

**Theorem 16.0.12** (Parallelogram Law). *In any inner product space,*

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

PROOF:

$$\begin{aligned}
\langle 1 \rangle 1. \quad &\|x + y\|^2 = \|x\|^2 + \langle x, y \rangle + \langle y, x \rangle + \|y\|^2 \\
\langle 1 \rangle 2. \quad &\|x - y\|^2 = \|x\|^2 - \langle x, y \rangle - \langle y, x \rangle + \|y\|^2 \\
\langle 1 \rangle 3. \quad &\text{Q.E.D.}
\end{aligned}$$

PROOF: Add  $\langle 1 \rangle 1$  and  $\langle 1 \rangle 2$ .

$\square$

**Proposition 16.0.13.** *Let  $E$  be a normed space over  $\mathbb{C}$ . Then there exists an inner product on  $E$  that induces the norm of  $E$  iff  $E$  satisfies the Parallelogram Law.*

PROOF: If  $E$  satisfies the parallelogram law, define

$$\langle x, y \rangle = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2 + i\|x + iy\|^2 - i\|x - iy\|^2) .$$

**Definition 16.0.14** (Orthogonal). Vectors  $x$  and  $y$  in an inner product space are *orthogonal*,  $x \perp y$ , iff  $\langle x, y \rangle = 0$ .

**Theorem 16.0.15** (Pythagorean Formula). *If  $x$  and  $y$  are orthogonal then*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 .$$

**Definition 16.0.16** (Weak Convergence). Let  $E$  be an inner product space. Let  $(x_n)$  be a sequence in  $E$  and  $l \in E$ . Then  $(x_n)$  *weakly converges* to  $l$ ,  $x_n \xrightarrow{w} l$  as  $n \rightarrow \infty$ , iff  $\forall y \in E. \langle x_n, y \rangle \rightarrow \langle l, y \rangle$  as  $n \rightarrow \infty$ .

**Proposition 16.0.17.** *In any inner product space  $E$ , the inner product  $\langle \cdot, \cdot \rangle : E^2 \rightarrow \mathbb{C}$  is continuous.*

PROOF:

$\langle 1 \rangle 1.$  LET:  $x_n \rightarrow x$  and  $y_n \rightarrow y$  in  $E$ .

$\langle 1 \rangle 2.$   $\langle x_n, y_n \rangle \rightarrow \langle x, y \rangle$

PROOF:

$$\begin{aligned}
|\langle x_n, y_n \rangle - \langle x, y \rangle| &\leq |\langle x_n, y_n \rangle - \langle x_n, y \rangle| + |\langle x_n, y \rangle - \langle x, y \rangle| \\
&= |\langle x_n, y_n - y \rangle| + |\langle x_n - x, y \rangle| \\
&\leq \|x_n\| \|y_n - y\| + \|x_n - x\| \|y\| && \text{(Schwarz's Inequality)} \\
&\rightarrow 0
\end{aligned}$$

using the fact that  $(x_n)$  is bounded.

□

**Theorem 16.0.18.**  $x_n \rightarrow l$  if and only if  $x_n \xrightarrow{w} l$  and  $\|x_n\| \rightarrow \|l\|$ .

PROOF:

⟨1⟩1. If  $x_n \rightarrow l$  then  $x_n \xrightarrow{w} l$  and  $\|x_n\| \rightarrow \|l\|$ .

PROOF: Easy using the fact that the inner product is continuous.

⟨1⟩2. If  $x_n \xrightarrow{w} l$  and  $\|x_n\| \rightarrow \|l\|$  then  $x_n \rightarrow l$ .

⟨2⟩1. ASSUME:  $x_n \xrightarrow{w} l$  and  $\|x_n\| \rightarrow \|l\|$

⟨2⟩2.  $\langle x_n, l \rangle \rightarrow \|l\|^2$

⟨2⟩3.  $\|x_n - l\| \rightarrow 0$

PROOF:

$$\begin{aligned} \|x_n - l\|^2 &= \langle x_n - l, x_n - l \rangle \\ &= \langle x_n, x_n \rangle - \langle x_n, l \rangle - \langle l, x_n \rangle + \langle l, l \rangle \\ &= \|x_n\|^2 - \langle x_n, l \rangle - \overline{\langle x_n, l \rangle} + \|l\|^2 \\ &\rightarrow \|l\|^2 - 2\|l\|^2 + \|l\|^2 \\ &= 0 \end{aligned}$$

□

**Theorem 16.0.19.** Let  $S$  be a subset of an inner product space  $E$  such that  $\text{span } S$  is dense in  $E$ . If  $(x_n)$  is a bounded sequence in  $E$  and, for all  $y \in S$ , we have  $\langle x_n, y \rangle \rightarrow \langle x, y \rangle$  then  $x_n \xrightarrow{w} x$ .

PROOF:

⟨1⟩1. For all  $y \in \text{span } S$ , we have  $\langle x_n, y \rangle \rightarrow \langle x, y \rangle$

⟨1⟩2. LET:  $z \in E$

PROVE:  $\langle x_n, z \rangle \rightarrow \langle x, z \rangle$

⟨1⟩3. LET:  $\epsilon > 0$

PROVE: There exists  $n_0$  such that  $\forall n \geq n_0, |\langle x_n, z \rangle - \langle x, z \rangle| < \epsilon$

⟨1⟩4. PICK  $M > 0$  such that  $\|x\| \leq M$  and  $\forall n \in \mathbb{Z}_+, \|x_n\| \leq M$ .

⟨1⟩5. PICK  $y_0 \in \text{span } S$  such that  $\|z - y_0\| < \epsilon/3M$

⟨1⟩6. PICK  $n_0 \in \mathbb{Z}_+$  such that, for all  $n \geq n_0$ , we have  $|\langle x_n, y_0 \rangle - \langle x, y_0 \rangle| < \epsilon/3$

⟨1⟩7. LET:  $n \geq n_0$

⟨1⟩8.  $|\langle x_n, z \rangle - \langle x, z \rangle| < \epsilon$

PROOF:

$$\begin{aligned} |\langle x_n, z \rangle - \langle x, z \rangle| &\leq |\langle x_n, z \rangle - \langle x_n, y_0 \rangle| + |\langle x_n, y_0 \rangle - \langle x, y_0 \rangle| + |\langle x, y_0 \rangle - \langle x, z \rangle| \\ &< \|x_n\| \|z - y_0\| + \epsilon/3 + \|x\| \|y_0 - z\| \\ &< M(\epsilon/3M) + \epsilon/3 + M(\epsilon/3M) \\ &= \epsilon \end{aligned}$$

□

## 16.1 Orthonormal Bases

**Definition 16.1.1** (Orthogonal). Let  $V$  be an inner product space and  $S \subseteq V$ . Then  $S$  is *orthogonal* iff any two distinct elements of  $S$  are orthogonal.

**Definition 16.1.2** (Orthonormal). Let  $V$  be an inner product space and  $S \subseteq V$ . Then  $S$  is *orthonormal* iff it is orthogonal and  $\forall x \in S, \|x\| = 1$ .

**Proposition 16.1.3.** *Orthonormal sets are linearly independent.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $S$  be orthonormal

$\langle 1 \rangle 2$ . ASSUME:  $\alpha_1 e_1 + \cdots + \alpha_n e_n = 0$  where  $e_1, \dots, e_n \in S$

$\langle 1 \rangle 3$ .  $|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 0$

PROOF:

$$\begin{aligned} 0 &= \sum_{m=1}^n \langle 0, \alpha_m e_m \rangle \\ &= \sum_{m=1}^n \langle \sum_{k=1}^n \alpha_k e_k, \alpha_m e_m \rangle \\ &= \sum_{m=1}^n \sum_{k=1}^n \alpha_k \overline{\alpha_m} \langle e_k, e_m \rangle \\ &= \sum_{k=1}^n |\alpha_k|^2 \end{aligned}$$

$\langle 1 \rangle 4$ .  $\alpha_1 = \cdots = \alpha_n = 0$

□

**Proposition 16.1.4.** *In  $l^2$ , let  $e_n$  be the sequence whose  $n$ th element is 1 and whose other elements are 0. Then  $\{e_n \mid n \in \mathbb{Z}_+\}$  is orthonormal.*

**Proposition 16.1.5.** *In  $L^2([-\pi, \pi])$ , let  $\phi_n(x) = e^{inx}/\sqrt{2\pi}$  for  $n \in \mathbb{Z}$ . Then  $\{\phi_n \mid n \in \mathbb{Z}\}$  is orthonormal.*

**Definition 16.1.6** (Legendre Polynomials). The *Legendre polynomials*  $P_n \in \mathbb{Q}[x]$  for  $n \in \mathbb{N}$  are defined by

$$\begin{aligned} P_0 &= 1 \\ P_n &= \frac{1}{2^n n!} \frac{d^n}{dx^n} (x^2 - 1)^n \end{aligned}$$

**Proposition 16.1.7.** *Let  $P_n$  be the  $n$ th Legendre polynomial. Then  $\{P_n \mid n \in \mathbb{N}\}$  is orthogonal in  $L^2([-1, 1])$ .*

**Definition 16.1.8** (Hermite Polynomial). The *Hermite polynomials*  $H_n \in \mathbb{R}[x]$  for  $n \in \mathbb{N}$  are defined by

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}.$$

**Proposition 16.1.9.** *Let  $H_n$  be the  $n$ th Hermite polynomial. Then  $\{e^{-x^2/2} H_n(x) \mid n \in \mathbb{N}\}$  is orthogonal in  $L^2(\mathbb{R})$ .*

**Theorem 16.1.10.** *Let  $V$  be an inner product space. If  $x_1, \dots, x_n \in V$  are orthogonal then*

$$\left\| \sum_{i=1}^n x_i \right\|^2 = \sum_{i=1}^n \|x_i\|^2 .$$

**Theorem 16.1.11** (Bessel's Equality). *Let  $V$  be an inner product space. Let  $x_1, \dots, x_n \in V$  be orthonormal. Let  $x \in V$ . Then*

$$\left\| x - \sum_{k=1}^n \langle x, x_k \rangle x_k \right\|^2 = \|x\|^2 - \sum_{k=1}^n |\langle x, x_k \rangle|^2 .$$

PROOF:

$$\begin{aligned} \left\| x - \sum_{k=1}^n \langle x, x_k \rangle x_k \right\|^2 &= \left\langle x - \sum_{k=1}^n \langle x, x_k \rangle x_k, x - \sum_{k=1}^n \langle x, x_k \rangle x_k \right\rangle \\ &= \langle x, x \rangle - \left\langle x, \sum_{k=1}^n \langle x, x_k \rangle x_k \right\rangle - \left\langle \sum_{k=1}^n \langle x, x_k \rangle x_k, x \right\rangle \\ &\quad + \left\langle \sum_{k=1}^n \langle x, x_k \rangle x_k, \sum_{k=1}^n \langle x, x_k \rangle x_k \right\rangle \\ &= \langle x, x \rangle - 2 \sum_{k=1}^n \langle x, x_k \rangle \langle x_k, x \rangle + \sum_{i=1}^n \sum_{j=1}^n \langle x, x_i \rangle \langle x_j, x \rangle \langle x_i, x_j \rangle \\ &= \|x\|^2 - 2 \sum_{k=1}^n |\langle x, x_k \rangle|^2 + \sum_{i=1}^n \langle x, x_i \rangle \langle x_i, x \rangle \\ &= \|x\|^2 - \sum_{k=1}^n |\langle x, x_k \rangle|^2 \end{aligned} \quad \square$$

**Corollary 16.1.11.1** (Bessel's Inequality). *Let  $V$  be an inner product space. Let  $x_1, \dots, x_n \in V$  be orthonormal. Let  $x \in E$ . Then*

$$\sum_{k=1}^n |\langle x, x_k \rangle|^2 \leq \|x\|^2 .$$

**Corollary 16.1.11.2.** *Orthonormal sequences are weakly convergent to 0.*

PROOF: Let  $(x_n)$  be an orthonormal sequence. Taking the limit in Bessel's inequality we have  $\sum_{k=1}^{\infty} |\langle x, x_k \rangle|^2 \leq \|x\|^2 < \infty$  and so  $\langle x, x_k \rangle \rightarrow 0$  as  $k \rightarrow \infty$ .  $\square$

**Corollary 16.1.11.3** (Generalized Fourier Series). *Let  $V$  be an inner product space. Let  $(e_n)$  be an orthonormal sequence in  $V$ . For any  $x \in V$ , the generalized Fourier series of  $x$  is*

$$\sum_{n=1}^{\infty} \langle x, e_n \rangle e_n ,$$

and  $\langle x, e_n \rangle$  is called the  $n$ th generalized Fourier coefficient of  $x$  with respect to  $(e_n)$ . We have  $(\langle x, e_n \rangle e_n)_n \in l^2$ .

**Definition 16.1.12** (Complete Orthonormal Sequence). Let  $E$  be an inner product space. Let  $(x_n)$  be an orthonormal sequence in  $E$ . Then  $(x_n)$  is *complete* iff, for all  $x \in E$ , we have

$$\sum_{n=1}^{\infty} \langle x, x_n \rangle x_n = x \quad .$$





## Chapter 17

# Hilbert Spaces

**Definition 17.0.1** (Hilbert Space). A *Hilbert space* is a complete inner product space.

**Proposition 17.0.2.** For  $n \in \mathbb{N}$ ,  $\mathbb{C}^n$  is a Hilbert space.

**Proposition 17.0.3.**  $l^2$  is a Hilbert space.

**Proposition 17.0.4.**  $L^2(\mathbb{R})$  is a Hilbert space.

**Proposition 17.0.5.**  $L^2([a, b])$  is a Hilbert space.

**Proposition 17.0.6.** Let  $\rho$  be a measurable function on  $[a, b]$  such that  $\rho(x) > 0$  almost everywhere. Let  $L^{2\rho}([a, b])$  be the set of all measurable functions  $f : [a, b] \rightarrow \mathbb{C}$  such that

$$\int_a^b |f(x)|^2 \rho(x) dx < \infty .$$

Define an inner product on  $L^{2\rho}([a, b])$  by

$$\langle f, g \rangle = \int_a^b f(x) \overline{g(x)} \rho(x) dx .$$

Then  $L^{2\rho}([a, b])$  is a Hilbert space.

**Proposition 17.0.7.** Let  $m$  and  $N$  be positive integers. Let  $\Omega$  be an open set in  $\mathbb{R}^N$ . Let  $\tilde{H}^m(\Omega)$  be the set of all  $f \in C^m(\Omega)$  such that, for every  $\alpha = (\alpha_1, \dots, \alpha_N) \in \mathbb{Z}_+^N$  with  $|\alpha| := \alpha_1 + \dots + \alpha_N \leq m$ , we have

$$D^\alpha f := \frac{\partial^{|\alpha|} f}{\partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \dots \partial x_N^{\alpha_N}} \in L^2(\Omega) .$$

Define an inner product on  $\tilde{H}^m(\Omega)$  by

$$\langle f, g \rangle := \int_\Omega \sum_\alpha D^\alpha f \overline{D^\alpha g} .$$

Let  $H^m(\Omega)$  be the completion of  $\tilde{H}^m(\Omega)$ . Then  $H^m(\Omega)$  is a Hilbert space.

**Theorem 17.0.8.** *Weakly convergent sequences in a Hilbert space are bounded.*

PROOF:

⟨1⟩1. LET:  $H$  be a Hilbert space.

⟨1⟩2. LET:  $(x_n)$  be a weakly convergent sequence in  $H$ .

⟨1⟩3. For  $n \in \mathbb{Z}_+$ ,

LET:  $f_n : H \rightarrow \mathbb{C}$ ,  $f_n(x) = \langle x, x_n \rangle$

⟨1⟩4. For  $n \in \mathbb{Z}_+$ ,  $f_n$  is a bounded linear functional.

⟨1⟩5. For every  $x \in H$ , the sequence  $(f_n(x))$  is bounded.

PROOF: Since it converges.

⟨1⟩6. PICK  $M > 0$  such that, for all  $n \in \mathbb{Z}_+$ , we have  $\|f_n\| \leq M$ .

PROOF: Banach-Steinhaus Theorem, ⟨1⟩4, ⟨1⟩5.

⟨1⟩7.  $\forall n \in \mathbb{Z}_+.$   $\|f_n\| = \|x_n\|$

⟨2⟩1. LET:  $n \in \mathbb{Z}_+$

⟨2⟩2.  $\|f_n\| \leq \|x_n\|$

PROOF: Since for all  $x \in H$  we have  $|f_n(x)| = |\langle x, x_n \rangle| \leq \|x\| \|x_n\|$  by Schwarz's Inequality.

⟨2⟩3.  $\|x_n\| \leq \|f_n\|$

PROOF: Since  $\|x_n\|^2 = |\langle x_n, x_n \rangle| = |f_n(x_n)| \leq \|f_n\| \|x_n\|$ .

⟨1⟩8.  $\forall n \in \mathbb{Z}_+.$   $\|x_n\| \leq M$

PROOF: ⟨1⟩6, ⟨1⟩7

□

**Theorem 17.0.9.** *Let  $H$  be a Hilbert space. Let  $(x_n)$  be an orthonormal sequence in  $H$  and let  $(\alpha_n)$  be a sequence of complex numbers. Then the series  $\sum_{n=1}^{\infty} \alpha_n x_n$  converges in  $H$  if and only if  $\sum_{n=1}^{\infty} |\alpha_n|^2$  converges in  $\mathbb{R}$ , in which case*

$$\left\| \sum_{n=1}^{\infty} \alpha_n x_n \right\|^2 = \sum_{n=1}^{\infty} |\alpha_n|^2 .$$

PROOF:

⟨1⟩1. For  $m > k > 0$  we have

$$\left\| \sum_{n=k}^m \alpha_n x_n \right\|^2 = \sum_{n=k}^m |\alpha_n|^2 .$$

PROOF: Theorem 16.1.10.

⟨1⟩2. If  $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$  then  $\sum_{n=1}^{\infty} \alpha_n x_n$  converges.

⟨2⟩1. ASSUME:  $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$

⟨2⟩2.  $(\sum_{n=1}^m \alpha_n x_n)_m$  is Cauchy.

PROOF: From ⟨1⟩1.

⟨2⟩3.  $\sum_{n=1}^{\infty} \alpha_n x_n$  converges.

⟨1⟩3. If  $\sum_{n=1}^{\infty} \alpha_n x_n$  converges then  $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$ .

PROOF: From ⟨1⟩1.

⟨1⟩4. If  $\sum_{n=1}^{\infty} |\alpha_n|^2 < \infty$  then

$$\left\| \sum_{n=1}^{\infty} \alpha_n x_n \right\|^2 = \sum_{n=1}^{\infty} |\alpha_n|^2 .$$

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

□

**Proposition 17.0.10.** *Every complete orthonormal sequence in a Hilbert space is a basis.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $E$  be an inner product space.

$\langle 1 \rangle 2$ . LET:  $(e_n)$  be a complete orthonormal sequence in  $E$ .

$\langle 1 \rangle 3$ . For all  $x \in E$ , there exists a sequence  $(\alpha_n)$  in  $\mathbb{C}$  such that  $x = \sum_n \alpha_n e_n$ .

PROOF: Immediate from  $\langle 1 \rangle 2$ .

$\langle 1 \rangle 4$ . If  $\sum_n \alpha_n e_n = \sum_n \beta_n e_n$  then  $\alpha_n = \beta_n$  for all  $n$ .

$\langle 2 \rangle 1$ . LET:  $x = \sum_n \alpha_n e_n = \sum_n \beta_n e_n$

$\langle 2 \rangle 2$ .  $\sum_n |\alpha_n - \beta_n|^2 = 0$

PROOF:

$$\begin{aligned}
 0 &= \|x - x\|^2 \\
 &= \left\| \sum_{n=1}^{\infty} \alpha_n e_n - \sum_{n=1}^{\infty} \beta_n e_n \right\|^2 && (\langle 2 \rangle 1) \\
 &= \left\| \sum_{n=1}^{\infty} (\alpha_n - \beta_n) e_n \right\|^2 \\
 &= \sum_{n=1}^{\infty} |\alpha_n - \beta_n|^2 && (\text{Theorem 17.0.9})
 \end{aligned}$$

$\langle 2 \rangle 3$ .  $\alpha_n = \beta_n$  for all  $n$ .

□

**Theorem 17.0.11.** *An orthonormal sequence  $(x_n)$  in a Hilbert space  $H$  is complete if and only if, for all  $x \in H$ , if  $\forall n. \langle x, x_n \rangle = 0$  then  $x = 0$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $(x_n)$  is complete then, for all  $x \in H$ , if  $\forall n. \langle x, x_n \rangle = 0$  then  $x = 0$ .

$\langle 2 \rangle 1$ . ASSUME:  $(x_n)$  is complete.

$\langle 2 \rangle 2$ . LET:  $x \in H$

$\langle 2 \rangle 3$ . ASSUME:  $\forall n. \langle x, x_n \rangle = 0$

$\langle 2 \rangle 4$ .  $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n = 0$

$\langle 1 \rangle 2$ . If, for all  $x \in H$ , if  $\forall n. \langle x, x_n \rangle = 0$  then  $x = 0$ , then  $(x_n)$  is complete.

$\langle 2 \rangle 1$ . ASSUME: For all  $x \in H$ , if  $\forall n. \langle x, x_n \rangle = 0$ , then  $x = 0$ .

$\langle 2 \rangle 2$ . LET:  $y = x - \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

$\langle 2 \rangle 3$ . For all  $n$ ,  $\langle y, x_n \rangle = 0$

$\langle 3 \rangle 1$ . LET:  $n \in \mathbb{Z}_+$

$\langle 3 \rangle 2$ .  $\langle y, x_n \rangle = 0$

PROOF:

$$\begin{aligned}
 \langle y, x_n \rangle &= \left\langle x - \sum_{m=1}^{\infty} \langle x, x_m \rangle x_m, x_n \right\rangle \\
 &= \langle x, x_n \rangle - \sum_{m=1}^{\infty} \langle x, x_m \rangle \langle x_m, x_n \rangle \\
 &= \langle x, x_n \rangle - \langle x, x_n \rangle \\
 &= 0
 \end{aligned}$$

$\langle 2 \rangle 4. y = 0$

$\langle 2 \rangle 5. x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

□

**Theorem 17.0.12** (Parseval's Formula). *Let  $H$  be a Hilbert space. Let  $(x_n)$  be an orthonormal sequence in  $H$ . Then  $(x_n)$  is complete if and only if, for all  $x \in H$ ,*

$$\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2.$$

PROOF:

$\langle 1 \rangle 1.$  If  $(x_n)$  is complete then for all  $x \in H$  we have  $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$ .

$\langle 2 \rangle 1.$  ASSUME:  $(x_n)$  is complete.

$\langle 2 \rangle 2.$  LET:  $x \in H$

$\langle 2 \rangle 3.$   $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$

PROOF:

$$\begin{aligned}
 \|x\|^2 &= \left\| \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n \right\|^2 && (\langle 2 \rangle 1) \\
 &= \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2 && (\text{Theorem 17.0.9})
 \end{aligned}$$

$\langle 1 \rangle 2.$  If, for all  $x \in H$ , we have  $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$ , then  $(x_n)$  is complete.

$\langle 2 \rangle 1.$  ASSUME: For all  $x \in H$ , we have  $\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n \rangle|^2$

$\langle 2 \rangle 2.$  LET:  $x \in H$

$\langle 2 \rangle 3.$   $x = \sum_{n=1}^{\infty} \langle x, x_n \rangle x_n$

□

**Proposition 17.0.13.** *For  $n \in \mathbb{Z}$ , let  $\pi_n(x) = e^{inx}/\sqrt{2\pi}$ . Then  $\{\pi_n \mid n \in \mathbb{Z}\}$  is a complete orthonormal set in  $L^2([-\pi, \pi])$ .*

TODO

**Proposition 17.0.14.**  $B = \{1/\sqrt{2\pi}\} \cup \{\cos nx/\sqrt{\pi} \mid n \in \mathbb{Z}_+\} \cup \{\sin nx/\sqrt{\pi} \mid n \in \mathbb{Z}_+\}$  is a complete orthonormal set in  $L^2([-\pi, \pi])$ .

PROOF:

$\langle 1 \rangle 1.$  For all  $f \in B$  we have  $\|f\| = 1$

$\langle 2 \rangle 1.$   $\|1/\sqrt{2\pi}\| = 1$

PROOF:

$$\begin{aligned}\|1/\sqrt{2\pi}\| &= \int_{-\pi}^{\pi} dx/2\pi \\ &= 1\end{aligned}$$

$\langle 2 \rangle 2$ . For all  $n \in \mathbb{Z}_+$  we have  $\|\cos nx/\sqrt{\pi}\| = 1$

PROOF:

$$\begin{aligned}\|\cos nx/\sqrt{\pi}\| &= 1/\pi \int_{-\pi}^{\pi} \cos^2 nx \, dx \\ &= 1/2\pi \int_{-\pi}^{\pi} (\cos 2nx + 1) \, dx \\ &= 1/2\pi [1/2n \sin 2nx + x]_{-\pi}^{\pi} \\ &= (1/2\pi)(2\pi) \\ &= 1\end{aligned}$$

$\langle 2 \rangle 3$ . For all  $n \in \mathbb{Z}_+$  we have  $\|\sin nx/\sqrt{\pi}\| = 1$

PROOF:

$$\begin{aligned}\|\sin nx/\sqrt{\pi}\| &= 1/\pi \int_{-\pi}^{\pi} \sin^2 nx \, dx \\ &= -1/2\pi \int_{-\pi}^{\pi} (\cos 2nx - 1) \, dx \\ &= -1/2\pi [1/2n \sin 2nx - x]_{-\pi}^{\pi} \\ &= (-1/2\pi)(-2\pi) \\ &= 1\end{aligned}$$

$\langle 1 \rangle 2$ . For all  $f, g \in B$  with  $f \neq g$  we have  $\langle f, g \rangle = 0$

$\langle 2 \rangle 1$ .  $\langle 1, \cos nx \rangle = 0$

PROOF:

$$\begin{aligned}\int_{-\pi}^{\pi} \cos nx \, dx &= [1/n \sin nx]_{-\pi}^{\pi} \\ &= 0\end{aligned}$$

$\langle 2 \rangle 2$ .  $\langle 1, \sin nx \rangle = 0$

PROOF:

$$\begin{aligned}\int_{-\pi}^{\pi} \sin nx \, dx &= [-1/n \cos nx]_{-\pi}^{\pi} \\ &= -1/n \cos n\pi + 1/n \cos n\pi \\ &= 0\end{aligned}$$

$\langle 2 \rangle 3$ . If  $m \neq n$  then  $\langle \cos mx, \cos nx \rangle = 0$

PROOF:

$$\begin{aligned}\int_{-\pi}^{\pi} \cos mx \cos nx \, dx &= 1/2 \int_{-\pi}^{\pi} (\cos(n+m)x - \cos(n-m)x) \, dx \\ &= 1/2 \left[ \frac{1}{n+m} \sin(n+m)x - \frac{1}{n-m} \sin(n-m)x \right]_{-\pi}^{\pi} \\ &= 0\end{aligned}$$

$\langle 2 \rangle 4$ .  $\langle \cos mx, \sin nx \rangle = 0$

PROOF:

$$\begin{aligned} \int_{-\pi}^{\pi} \cos mx \sin nx \, dx &= 1/2 \int_{-\pi}^{\pi} (\sin(n+m)x - \sin(n-m)x) \, dx \\ &= 1/2 \left[ -\frac{1}{n+m} \cos(n+m)x + \frac{1}{n-m} \cos(n-m)x \right]_{-\pi}^{\pi} \\ &= 0 \end{aligned} \quad (\cos \text{ is odd})$$

$\langle 2 \rangle 5$ . If  $m \neq n$  then  $\langle \sin mx, \sin nx \rangle = 0$

PROOF:

$$\begin{aligned} \int_{-\pi}^{\pi} \sin mx \sin nx \, dx &= 1/2 \int_{-\pi}^{\pi} (\cos(n-m)x - \cos(n+m)x) \, dx \\ &= 1/2 \left[ \frac{1}{n-m} \sin(n-m)x - \frac{1}{n+m} \sin(n+m)x \right]_{-\pi}^{\pi} \\ &= 0 \end{aligned}$$

$\langle 1 \rangle 3$ . For all  $f \in L^2([-\pi, \pi])$ , if  $\forall g \in B. \langle f, g \rangle = 0$  then  $f = 0$

$\langle 2 \rangle 1$ . LET:  $f \in L^2([-\pi, \pi])$

$\langle 2 \rangle 2$ . ASSUME:  $\forall g \in B. \langle f, g \rangle = 0$

$\langle 2 \rangle 3$ . For all  $n \in \mathbb{Z}$ ,  $\langle f, e^{inx} \rangle = 0$

PROOF: Since  $e^{inx} = \cos nx + i \sin nx$ .

$\langle 2 \rangle 4$ .  $f = 0$

PROOF: From Proposition 17.0.13.

□

**Proposition 17.0.15.**  $\{\frac{1}{\sqrt{\pi}}\} \cup \{\sqrt{\frac{2}{\pi}} \cos nx \mid n \in \mathbb{Z}_+\}$  is a complete orthonormal set in  $L^2([0, \pi])$ .

**Proposition 17.0.16.**  $\{\sqrt{\frac{2}{\pi}} \sin nx \mid n \in \mathbb{Z}_+\}$  is a complete orthonormal set in  $L^2([0, \pi])$ .

**Definition 17.0.17** (Signum). The *signum* function  $\text{sgn} : \mathbb{R} \rightarrow \mathbb{R}$  is defined by

$$\text{sgn } x = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

**Definition 17.0.18** (Rademacher Functions). The *Rademacher functions*  $R : \mathbb{N} \times [0, 1] \rightarrow \{-1, 0, 1\}$  are defined by

$$R(m, x) = \text{sgn}(\sin(2^m \pi x)) \quad .$$

**Proposition 17.0.19.** The Rademacher functions  $\{R(m, -) \mid m \in \mathbb{N}\}$  are orthonormal in  $L^2([0, 1])$ .

PROOF:

$\langle 1 \rangle 1$ .  $\forall m \in \mathbb{N}. \|R(m, -)\| = 1$

PROOF:  $\int_0^1 \text{sgn}(\sin(2^m \pi x))^2 \, dx = 1$  since the integrand is 1 except for finitely many points in  $[0, 1]$ .

$\langle 1 \rangle 2$ . Given natural numbers  $m \neq n$ , we have  $\langle R(m, -), R(n, -) \rangle = 0$

$\langle 2 \rangle 1$ . Given reals  $a, b$  and a natural number  $m$ , we have  $\int_a^b R(m, x) dx = 0$  whenever  $2^m(b - a)$  is an even integer.

PROOF: If  $m > 0$ , or if  $m = 0$  and  $b - a$  is an even integer, then the regions where  $R(m, x) = 1$  are isometric with the regions where  $R(m, x) = -1$ .

$\langle 2 \rangle 2$ . LET:  $m$  and  $n$  be natural numbers with  $n < m$ .

$\langle 2 \rangle 3$ .  $\langle R(m, -), R(n, -) \rangle = 0$

PROOF:

$$\begin{aligned} \int_0^1 R(m, x) R(n, x) dx &= \sum_{k=1}^{2^n} \int_{\frac{k-1}{2^n}}^{\frac{k}{2^n}} R(m, x) R(n, x) dx \\ &= \sum_{k=1}^{2^n} (-i)^{k+1} \int_{\frac{k-1}{2^n}}^{\frac{k}{2^n}} R(m, x) dx \end{aligned}$$

$$= 0$$

$$(\langle 2 \rangle 1, 2^m \left( \frac{k}{2^n} - \frac{k-1}{2^n} \right) = 2^{m-n} \text{ is an even integer})$$

□

**Proposition 17.0.20.** *The set of Rademacher functions is not complete.*

PROOF:

$\langle 1 \rangle 1$ . Define  $f : [0, 1] \rightarrow \mathbb{C}$  by  $f(x) = 0$  if  $0 \leq x < 1/4$ ,  $f(x) = 1$  if  $1/4 \leq x \leq 3/4$ ,  $f(x) = 0$  if  $3/4 < x \leq 1$ .

$\langle 1 \rangle 2$ .  $f \in L^2([0, 1])$

$\langle 1 \rangle 3$ .  $\langle R(0, -), f \rangle = 1/2$

$\langle 1 \rangle 4$ .  $\langle R(m, -), f \rangle = 0$  for  $m \geq 1$

$\langle 1 \rangle 5$ .  $f \neq 1/2 R(0, -)$

□

**Definition 17.0.21** (Walsh Functions). Define the *Walsh functions*  $W : \mathbb{N} \times [0, 1] \rightarrow \{-1, 0, 1\}$  as follows. Given  $m \in \mathbb{N}$ , let  $m = \sum_{k=1}^n 2^{k-1} a_k$  where each  $a_k$  is either 0 or 1. Then

$$W(m, x) = \prod_{k=1}^n R(k, x)^{a_k} .$$

**Proposition 17.0.22.** *The set of Walsh functions  $\{W(m, -) \mid m \in \mathbb{N}\}$  is a complete orthonormal set.*

TODO