# Basic Set Theory
# Based on *Elements of Set Theory* - Enderton

Alexandre Daoud
King's College London
alex.daoud@mac.com

December 18, 2015

# Chapter 1

# Introduction

## 1.1 Basic Set Theory

**Definition 1.1.** *A **set** is a collection of things referred to as its **members** or **elements**. We write $t \in A$ to say that $t$ is an element of $A$. We write $t \notin A$ to say that $t$ is not an element of $A$.*

**Notation 1.2.** *Let $A$ be a set with some elements $t_1, t_2, \dots$ (not necessarily a finite amount). We write*

$$A = \{t_1, t_2, \dots\}$$

**Axiom 1.3.** *Axiom of Extensionality*
*Let $A$ and $B$ be sets such that for every object $t$, we have*

$$t \in A \iff t \in B$$

*Then $A = B$.*

**Notation 1.4.** *If two sets $A$ and $B$ are not equal, we write $A \neq B$.*

**Example 1.5.** *Consider the set*

$$\varnothing = \{\}$$

*In other words, $\varnothing$ is the set containing no elements. By the axiom of extensionality, $\varnothing$ is unique. We call $\varnothing$ the **empty set**.*

**Remark.** *Note that $\{\varnothing\} \neq \varnothing$. The former is a set containing exactly one element (namely the empty set) while the latter is a set containing no elements.*

**Example 1.6.** *Consider the two sets $X_1 = \{x, y\}$ and $X_2 = \{y, x\}$. By the axiom of extensionality, we have that $X_1 = X_2$. We see that the ordering of elements in a set does not affect the properties of the set.*

**Notation 1.7.** *Let $A$ be a set and $t$ a prospective element of $A$. Let $P(t)$ be a logical statement - called the **entrance requirement** - that determines whether or not $t \in A$. We write*

$$A = \{\, t \mid P(t) \,\}$$

*This method of declaring sets is called **abstraction***
*We write $\vee$ for the **logical or** operator. In other words, let $A$ and $B$ be two logical statements. Then $A \vee B$ is true if $A$ is true or if $B$ is true or if both $A$ and $B$ are true.*

*We write $\wedge$ for the **logical and** operator. In other words, let $A$ and $B$ be two logical statements. Then $A \wedge B$ is true if and only if both $A$ and $B$ are true.*

**Remark.** *One must be careful when using abstraction. Consider the following set*

$$A = \{\, x \mid x \notin x \,\}$$

*We are interested in whether or not $A$ is a member of itself. If $A \notin A$ then $A$ meets the entrance requirement for $A$ and thus $A \in A$. But if $A \in A$ then $A$ fails to meet the entrace requirement and thus $A \notin A$. Obviously the given entrance requirement must be illegal. This is referred to as **Russell's Paradox**.*

**Definition 1.8.** *Let $A$ and $B$ be two sets. We define the **union** of $A$ and $B$ to be the set*

$$A \cup B = \{\, t \mid t \in A \vee t \in B \,\}$$

**Definition 1.9.** *Let $A$ and $B$ be two sets. We define the **intersection** of $A$ and $B$ to be the set*

$$A \cap B = \{\, t \mid t \in A \wedge t \in B \,\}$$

*If $A \cap B = \varnothing$, we say that $A$ and $B$ are **disjoint**.*

**Definition 1.10.** *We say that $A$ is a subset of $B$ if every element of $A$ is an element of $B$ and is denoted by $A \subseteq B$. In other words,*

$$A \subseteq B \iff (\forall\, t \in A \implies t \in B)$$

*If $A \subseteq B$, we say that $A$ is **included** in $B$ or $B$ **includes** $A$.*

**Example 1.11.** *Let $A$ be a set. Then $A \subseteq A$.*

**Example 1.12.** *Let $A$ be a set. Then $\varnothing \subseteq A$. We say that this fact is **vacuously true** since the task of verifying it requires doing nothing at all.*

**Definition 1.13.** *Let $A$ be a set. We denote the **power set** of $A$ to be*

$$\mathcal{P}A = \{\, X \mid X \subseteq A \,\}$$

*In other words, $\mathcal{P}A$ is the set of all subsets of $A$.*

# Chapter 2

# Axioms and Operations

From now on, we shall work in the **Zermelo-Fraenkel** framework which asserts that not every collection of objects (or **class**) is a set. This allows us to disregard Russell's Paradox as we can assume that such a set does not exist. We now reformulate the first chapter in terms of the axioms of set theory.

**Axiom 2.1.** *Extensionality axiom*
*If two sets have the same members, then they are equal:*

$$\forall A \forall B \left[\forall x \left(x \in A \iff x \in B\right) \implies A = B\right]$$

**Axiom 2.2.** *Empty Set Axiom*
*There is a set that contains no members:*

$$\exists B \forall x,\, x \notin B$$

**Definition 2.3.** *We define the* ***empty set*** *or* $\varnothing$ *to be the set containing no members. The existence of* $\varnothing$ *is guaranteed by the empty set axiom and its uniqueness is guaranteed by the extensionality axiom.*

**Axiom 2.4.** *Pairing Axiom*
*Let* $u$ *and* $v$ *be sets. Then there is a set that contains only* $u$ *and* $v$*:*

$$\forall u \forall v \exists B \forall x \left(x \in B \iff x = u \vee x = v\right)$$

**Definition 2.5.** *Let* $u$ *and* $v$ *be sets. The* ***pair set*** $\{u, v\}$ *is the set whose members are* $u$ *and* $v$*.*

**Axiom 2.6.** *Union Axiom*
*Let $a$ and $b$ be sets. Then there is a set whose members are those sets belonging either to $a$ or to $b$ (or both):*

$$\forall\, a \forall\, b \exists\, B \forall\, x\, (x \in B \iff x \in A \vee x \in B)$$

**Definition 2.7.** *Let $a$ and $b$ be sets. The* ***union*** *$a \cup b$ is the set whose members are those sets belonging either to $a$ or to $b$ (or both).*

**Axiom 2.8.** *Power Set Axiom*
*Let $a$ be a set. Then there is a set whose members are exactly the subsets of $a$:*

$$\forall\, a \exists\, B \forall\, x\, (x \in B \iff x \subseteq a)$$

**Definition 2.9.** *For any set $a$, the* ***power set*** *$\mathcal{P}a$ is the set whose members are exactly the subsets of $a$.*

**Definition 2.10.** *Let $x$ be a set. We define the* ***singleton*** *$\{x\}$ to be the set $\{x, x\}$, the existence of which is guaranteed by the Pairing Axiom. Given the sets $x_1, x_2, x_3$, we can define $\{x_1, x_2, x_3\} = \{x_1, x_2\} \cup \{x_3\}$. Continuing like this, we can define a set with any aribitrary number of members.*

**Axiom 2.11.** *Subset Axioms*
*Let $t_1, \ldots, t_k$ and $c$ be sets and let $P(t_1, \ldots, t_k)$ be a formula (or logical statement) not containing $B$ but mentioning $t_1, \ldots, t_k$. Then there exists a set $B$ whose members are exactly those sets $x$ in $c$ such that $P(t_1, \ldots, t_k)$ is true:*

$$\forall\, t_1 \ \ldots\ \forall\, t_k \forall\, c \exists\, B \forall\, x\, (x \in B \iff x \in c \wedge P(t_1, \ldots, t_k))$$

**Remark.** *Zermelo originally referred to these axioms as the Aussonderung axioms literally meaning the 'seperating-out' axioms. Such a collection of axioms is referred to as an* ***axiom schema****.*

**Example 2.12.** *Let $t_1 = a$ be a set and $P(a) := x \in a$ a formula. Then*

$$\forall\, a \forall\, c \exists\, B \forall\, x (x \in B \iff x \in c \wedge x \in a)$$

*is a subset axiom. This axiom asserts the existence of the* ***intersection*** *$c \cap a$ of $c$ and $a$.*

**Example 2.13.** *Let $t_1 = a$ and $P(a) := x \notin a$. Then*

$$\forall a \forall c \exists B \forall x (x \in B \iff x \in c \wedge x \notin a)$$

*is a subset axiom. This axiom asserts the existence of the* ***relative complement*** *of $a$ in $c$. This is denoted by $B = c \backslash a$*

**Theorem 2.14.** *There is no set to which every set belongs.*

*Proof.* Let $A$ be a set. We shall construct a set that is not contained in $A$. Let

$$B = \{ x \in A \mid x \notin x \}$$

We claim that $B \notin A$. We have that, by the definition of $B$,

$$B \in B \iff B \in A \wedge B \notin B$$

Now if $B \in A$

$$B \in B \iff B \notin B$$

This is impossible as one side must be true and the other side must be false. Hence $B \in A$. Therefore there cannot exist a set containing all sets. □

**Remark.** *We end this section by remarking that, in order to avoid illegal construction of sets, we require that formulas be rigorously stated in terms of logical symbols.*

## 2.1 Arbitrary Unions and Intersections

The union axiom allows us to form the union $a \cup b$ of two sets $a$ and $b$. By repeating the operation, we can form the union of finitely many sets. In order to take the union of infinitely many sets, we require the following definition:

**Definition 2.15.** *Let $A$ be a set. The* ***union*** $\bigcup A$ *of $A$ is the set defined by*

$$\bigcup A = \{ x \mid (\exists b \in A)\, x \in b \}$$

We now need an improved version of the union axiom in order to know that a set containing the members of the members of $A$ actually exists.

**Axiom 2.16.** *Union Axiom*
*Let $A$ be a set. Then there exists a set $B$ whose elements are exactly the members of the members of $A$:*

$$\forall\, x\, [x \in B \iff (\exists\, b \in A)\, x \in b]$$

**Definition 2.17.** *Let $A$ be a non-empty set. We define the* ***intersection*** $\bigcap A$ *of $A$ by*

$$\bigcap A = \{\, x \mid (\forall\, b \in A)\, x \in b \,\}$$

**Theorem 2.18.** *Let $A$ be a non-empty set. Then there exists a unique set $B$ such that for any $x$,*

$$x \in B \iff (\forall\, b \in A)\, x \in b$$

*Proof.* Let $c \in A$ (the existence of which is guaranteed by the fact that $A$ is non-empty). Then by the subset axiom, there is a set $B$ such that for any $x$,

$$\begin{aligned} x \in B &\iff (x \in c) \wedge ([\forall b \neq c \in A]\, x \in b) \\ &\iff (\forall\, b \in A)\, x \in b \end{aligned}$$

Now the uniqueness of $B$ follows from the axiom of extensionality. □

**Remark.** *Consider $A = \bigcap \varnothing$. For any $x$, it is vacuously true that $x$ belongs to any member of $A$ (since there can not exist a member of $A$ to which $x$ fails to belong). It would appear that $A$ is a set containing all sets. But by Theorem 2.14, there cannot exist such a set. This is solved by either leaving $\bigcap \varnothing$ as undefined or by defining it as some arbitrary set (usually $\varnothing$).*

**Example 2.19.** *Let $b \in A$. Then $b \subseteq \bigcup A$.*

**Example 2.20.** *Let $\{\{x\}, \{x, y\}\} \in A$. Then $\{x, y\} \in \bigcup A$, $x \in \bigcup\bigcup A$ and $y \in \bigcup\bigcup A$.*

**Example 2.21.** $\bigcap\{\{a\}, \{a, b\}\} = \{a\} \cap \{a, b\} = \{a\}$. *Therefore* $\bigcup\bigcap\{\{a\}, \{a, b\}\} = \bigcup\{a\} = a$. *On the other hand,* $\bigcap\bigcup\{\{a\}, \{a, b\}\} = \bigcap\{a, b\} = a \cap b$.

## 2.2 Algebra of Sets

**Definition 2.22.** *Let $A$ and $B$ be two sets. We define the* ***relative complement of B in A*** *$A\backslash B$ to be*

$$A\backslash B = \{\, x \in A \mid x \notin B \,\}$$

**Remark.** *Given two sets $A$ and $B$, the existence of the relative complement of $B$ in $A$ is guaranteed by the subset axioms.*

**Remark.** *Let $A$ be a set. Another complement of interest is the* ***absolute complement****. In other words, $A' = \{\, x \mid x \notin A \,\}$. Such a set cannot exist as the union axiom would imply that $A \cup A'$ exists. But $A \cup A'$ is a set that contains all sets which contradicts Theorem 2.14.*

**Proposition 2.23.** *Commutative Laws*
*Let $A$ and $B$ be sets. Then we have that*

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

*Proof.* The proof of this proposition is trivial and follows directly from the definitions of set union and intersection. □

**Proposition 2.24.** *Associative Laws*
*Let $A$ and $B$ be sets. Then we have that*

$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

*Proof.* We shall only prove the second identity.

$\subseteq$: Let $x \in A \cap (B \cap C)$. We must show that $x \in (A \cap B) \cap C$. By definition of set intersection, we must have that $x \in A$ and $x \in B \cap C$. Again by definition of the intersection, we must have that $x \in B$ and $x \in C$. Now obviously, $x \in A \cap B$. But since $x \in C$, we must have $x \in (A \cap B) \cap C$.

The opposite direction then follows by a similar argument and the two sets are equal. □

**Proposition 2.25.** *Distributive Laws*
*Let $A, B$ and $C$ be sets. Then we have that*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

*Proof.*

Part 1:

$\subseteq$: Let $x \in A \cap (B \cup C)$. We need to show that $x \in (A \cap B) \cup (A \cap C)$. By definition of set intersection, we have that $x \in A$ and $x \in B \cup C$. By definition of set union, we have that $x \in B$ or $x \in C$. Suppose first that $x \in B$. Then $x \in A$ and $x \in B$ and thus $x \in A \cap B$ whence it follows that $x \in (A \cap B) \cup (A \cap C)$. A similar argument can be applied for the case where $x \in C$.

$\supseteq$: Let $x \in (A \cap B) \cup (A \cap C)$. We must show that $x \in A \cap (B \cup C)$. By definition of set union, we have that $x \in A \cap B$ or $x \in A \cap C$. Suppose that $x \in A \cap B$. Then it follows from the definition of set intersection that $x \in A$ and $x \in B$. Obviously, $x \in B \cup C$ and thus $x \in A \cap (B \cup C)$. A similar argument can be applied for the case where $x \in A \cap C$.

Part 2:

$\subseteq$: Let $x \in A \cup (B \cap C)$. We need to show that $x \in (A \cup B) \cap (A \cup C)$. By definition of set union, we have that $x \in A$ or $x \in B \cap C$. Suppose first that $x \in A$. Then obviously $x \in A \cup B$ and $x \in A \cup C$. But then $x \in (A \cup B) \cap (A \cup C)$.
Now suppose that $x \in B \cap C$. By the definition of set intersection, $x \in B$ and $x \in C$. It then follows that $x \in A \cup B$ and $x \in A \cup C$ whence we obtain $x \in (A \cup B) \cap (A \cup C)$.

$\supseteq$: Let $x \in (A \cup B) \cap (A \cup C)$. We need to show that $x \in A \cup (B \cap C)$. By the definition of set intersection, we have that $x \in A \cup B$ and $x \in A \cup C$. By the definition of set union, we have four different possible cases. If $x \in A$ then trivially, $x \in A \cup (B \cap C)$. This leaves us with the case that $x \in B$ and $x \in C$. But then $x \in B \cap C$ whence it follows that $x \in A \cup (B \cap C)$.

□

**Proposition 2.26.** *De Morgan's Laws*
*Let $A, B$ and $C$ be sets. We have that*

$$C \backslash (A \cup B) = (C \backslash A) \cap (C \backslash B)$$
$$C \backslash (A \cap B) = (C \backslash A) \cup (C \backslash B)$$

*Proof.*

Part 1:

$\subseteq$: Let $x \in C\backslash(A \cup B)$. We must show that $x \in (C\backslash A) \cap (C\backslash B)$. By definition of the relative complement, we have that $x \in C$ but $x \notin A \cup B$. It thus follows that $x \notin A$ and $x \notin B$. Hence $x \in C\backslash A$ and $x \in C\backslash B$. Therefore, $x \in (C\backslash A) \cap (C\backslash B)$.

$\supseteq$: Let $x \in (C\backslash A) \cap (C\backslash B)$. We must show that $x \in C\backslash(A \cup B)$. By the definition of set intersection, $x \in C\backslash A$ and $x \in C\backslash B$. It follows by the definition of the relative complement that $x \in C$ but $x \notin A$ and $x \notin B$. Obviously, $x \notin A \cup B$ and therefore, $x \in C\backslash(A \cup B)$.

Part 2:

$\subseteq$: Let $x \in C\backslash(A \cap B)$. We must show that $x \in (C\backslash A) \cup (C\backslash B)$. By the definition of the relative complement, $x \in C$ but $x \notin A \cap B$. By the definition of set intersection, $x \notin A$ or $x \notin B$ or both. Suppose first that $x \notin A$. Then since $x \in C$, we have that $x \in C\backslash A$ whence it follows that $x \in (C\backslash A) \cup (C\backslash B)$. A similar argument can be applied to the other two cases.

$\supseteq$: Let $x \in (C\backslash A) \cup (C\backslash B)$. We must show that $x \in C\backslash(A \cap B)$. By the definition of set union, we have that $x \in C\backslash A$ or $x \in C\backslash B$. Suppose first that $x \in C\backslash A$. Then by the definition of the relative complement, we must have that $x \in C$ but $x \notin A$. If $x \notin A$ then obviously $x \notin A \cap B$. Therefore $x \in C\backslash(A \cap B)$. A similar argument can be applied for the case that $x \in C\backslash B$.

□

**Proposition 2.27.** *Let $A$ and $B$ be two sets. We have that*

$$A \cup \varnothing = A$$
$$A \cap \varnothing = \varnothing$$
$$A \cap (C\backslash A) = \varnothing$$

*Proof.* These identities follow directly from the relevant definitions. □

**Proposition 2.28.** *Monotone Properties*
*Let $B$ be a set and $A \subseteq B$ a subset. For any set $C$, we have the following*

$$A \cup C \subseteq B \cup C$$
$$A \cap C \subseteq B \cap C$$
$$\bigcup A \subseteq \bigcup B$$

*Proof.*

Part 1: Let $x \in A \cup C$. We want to show that $x \in B \cup C$. By the definition of set union, $x \in A$ or $x \in C$. Suppose first that $x \in A$. Then since $A \subseteq B$, we must have that $x \in B$. Then $x \in B \cup C$. Now suppose that $x \in C$. It follows that $x \in B \cup C$.

Part 2: Let $x \in A \cap C$. We need to show that $x \in B \cap C$. By definition of set intersection, we have that $x \in A$ and $x \in C$. Since $A \subseteq B$, we must have that $x \in B$. Thus $x \in B \cap C$.

Part 3: Let $x \in \bigcup A$. We must show that $x \in \bigcup B$. By the definition of the arbitrary union, we have that $(\exists\, b \in A)x \in b$. Since $A \subseteq B$, we must have that $b \in B$. But then $x \in b \in B$ and thus $x \in \bigcup B$.

□

**Proposition 2.29.** *Antimonotone Properties*
*Let $B$ be a set and $A \subseteq B$ a subset. For any set $C$ we have*

$$C \backslash B \subseteq C \backslash A$$

*and if $A \neq \varnothing$ then*

$$\bigcap B \subseteq \bigcap A$$

*Proof.*

Part 1: Let $x \in C \backslash B$. We need to show that $x \in C \backslash A$. By the definition of the relative complement, we have that $x \in C$ but $x \notin B$. Obviously, since $A \subseteq B$, we necessarily have that $x \notin A$. It hence follows that $x \in C \backslash A$.

Part 2: Let $x \in \bigcap B$. We need to show that $x \in \bigcap A$. By the definition of the arbitrary intersection, we have that $(\forall\, b \in B)x \in B$. Each such $b$ is

either a member of $A$ or is not. Choose all such sets that are members of A. Necessarily, since $A \subseteq B$, such sets must be all the members of $A$. Since all such sets contain $x$, we must have that $x \in \bigcap A$.

□

**Remark.** *The Distributive and De Morgan's Laws can easily be extended to arbitrary unions and intersections of sets (in the natural way), taking care not to allow the empty set in cases where the intersection of the empty set may arise.*

**Notation 2.30.** *Let $X$ be a set. When arbitrary intersections or unions of $X$ are involved with some other set $A$ we will employ a notation demonstrated by the following example:*

$$\bigcap_{x \in X} (A \cup X) = \bigcap \{ A \cup X \mid x \in X \}$$

# Chapter 3

# Relations and Functions

## 3.1 Ordered Pairs

**Definition 3.1.** *We define an* ***unordered pair*** *to be a structure containing two element that encodes no information about the ordering of its elements.*

**Example 3.2.** *Consider the pair set* $\{1, 2\}$*. This is an unordered pair since* $\{1, 2\} = \{2, 1\}$

**Definition 3.3.** *We define the* ***ordered pair*** $\langle x, y\rangle$ *to be the set* $\{\{x\}, \{x, y\}\}$*.*

**Theorem 3.4.** *Let* $\langle x, y\rangle$ *and* $\langle u, v\rangle$ *be ordered pairs. Then* $\langle x, y\rangle = \langle u, v\rangle$ *if and only if* $x = u$ *and* $y = v$*.*

*Proof.*

$\implies$ : Suppose that $\langle x, y\rangle = \langle u, v\rangle$. We need to show that $x = u$ and $y = v$. By the definiton of the ordered pair, we have that $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. Necessarily, $\{x\} \in \{\{u\}, \{u, v\}\}$ and $\{x, y\} \in \{\{u\}, \{u, v\}\}$. We thus have that $\{x\} = \{u\}$ or $\{x\} = \{u, v\}$ and $\{x, y\} = \{u\}$ or $\{x, y\} = \{u, v\}$. We shall check each case individually.

Suppose that $\{x\} = \{u\}$ and $\{x, y\} = \{u\}$. We thus have that $\{u\} = \{x, y\} = \{u, y\}$. It follows that $y = u$. Now looking back at the original condition, we see that $\{\{u\}\} = \{\{u\}, \{u, v\}\}$. The only option is that $v = u$ and thus $x = u = y = v$.

Now assume that $\{x\} = u$ and $\{x, y\} = \{u, v\}$. We have that $\{u, y\} = \{u, v\}$.

By the axiom of extensionality, we either have that $y = v$ or that $u = v$ and $y = u$. In the former case we are done. The latter case also implies that $y = v$.

Suppose now that $\{x\} = \{u, v\}$ and $\{x, y\} = \{u\}$. The axiom of extensionality implies that $x = u = v = y$.

Now assume that $\{x\} = \{u, v\}$ and $\{x, y\} = \{u, v\}$. Then again, the axiom of extensionality implies that $x = u = v = y$.

$\Longleftarrow$ : Suppose that $x = u$ and $y = v$. Then it follows trivially that $\langle x, y\rangle = \langle u, v\rangle$.

□

**Example 3.5.** *Consider the set $\mathbb{R}$ of all real numbers. The pair $\langle x, y\rangle$ where $x, y \in \mathbb{R}$ can be visualised as a point in the Cartesian plane. We say that $x$ and $y$ are **coordinates** of $\langle x, y\rangle$.*

**Definition 3.6.** *Let $A$ and $B$ be sets. We define their **Cartesian product** $A \times B$ to be the set*

$$A \times B = \{\, \langle x, y\rangle \mid x \in A \wedge y \in B \,\}$$

This definition does not make much sense if we do not verify that $A \times B$ is indeed a set (it could be a class). To do this, we shall find a set that contains all such pairs $\langle x, y\rangle$ and then utilise a suitable subset axiom to deduce that $A \times B$ exists. The following Lemma gives us the desired set.

**Lemma 3.7.** *Let $C$ be a set and $x, y \in C$ two elements. Then $\langle x, y\rangle \in \mathcal{PP}C$.*

*Proof.* Let $x, y \in C$. Then obviously, $\{x\} \subseteq C$ and $\{x, y\} \subseteq C$. By the definition of the power set, it follows that $\{x\} \in \mathcal{P}C$ and $\{x, y\} \in \mathcal{P}C$. By the union axiom, we know that $\{\{x\}, \{x, y\}\} \subseteq \mathcal{P}C$. Thus $\{\{x\}, \{x, y\}\} \in \mathcal{PP}C$. Now by the definition of the ordered pair, it follows that $\langle x, y\rangle \in \mathcal{PP}C$ □

**Corollary 3.8.** *Let $A$ and $B$ be sets $x \in A, y \in B$ elements. Then there exists a set whose members are exactly the ordered pairs $\langle x, y\rangle$.*

*Proof.* By a subset axiom, we can construct the set

$$\{\, w \in \mathcal{PP}(A \cup B) \mid w = \langle x, y\rangle \,\}$$

Obviously this set must only contain elements that take the form of an ordered pair. Now the previous lemma implies that such a set contains all such ordered pairs with $x \in A$ and $y \in B$. □

## 3.2 Relations

**Definition 3.9.** *A **relation** is a set of ordered pairs.*

**Notation 3.10.** *Let $R$ be a relation and $\langle x, y\rangle \in R$ an ordered pair. We write $xRy$ in the place of $\langle x, y\rangle \in R$.*

**Example 3.11.** *Consider the ordering relation $<$ on $\mathbb{R}$:*

$$< = \{\, \langle x, y\rangle \in \mathbb{R} \times \mathbb{R} \mid x < y \,\}$$

**Example 3.12.** *Let $\omega = \{\, 0, 1, 2, \dots \,\}$. We can consider the **divisibility relation***

$$\{\, \langle m, n\rangle \in \omega \times \omega \mid (\exists\, p \in \omega)\, mp = n \,\}$$

*We also have the **identity relation**:*

$$I_\omega = \{\, \langle n, n\rangle \mid n \in \omega \,\}$$

**Definition 3.13.** *Let $R$ be a relation. We define the **domain** of $R$, $dom\ R$, to be the set*

$$dom\, R = \{\, x \mid (\exists\, y)\, \langle x, y\rangle \in R \,\}$$

**Definition 3.14.** *Let $R$ be a relation. We define the **range** of $R$, $ran\ R$, to be the set*

$$ran\, R = \{\, x \mid (\exists\, t)\, \langle t, x\rangle \in R \,\}$$

**Definition 3.15.** *Let $R$ be a relation. We define the **field** of $R$, $fld\ R$, to be the set*

$$fld\, R = dom\, R \cup ran\, R$$

In order for these definitions to make sense, we need to make sure the set of first and second coordinates indeed exists. The following lemma shows the existence of a set containing such coordinates.

**Lemma 3.16.** *Let $\langle x, y\rangle$ be an ordered pair contained in some set $A$. Then $x$ and $y$ belong to $\bigcup\bigcup A$.*

*Proof.* By definition of an ordered pair, we have that $\{\{x\},\{x,y\}\} \in A$. It follows from the definition of the union that $\{x,y\} \in \bigcup A$. The definition of the union now implies that $x, y \in \bigcup\bigcup A$. □

It now suffices to apply a suitable subset axiom to the set constructed in the previous lemma to arrive at the definitions of the domain and range of a relation R:

$$dom\, R = \left\{ x \in \bigcup\bigcup R \;\middle|\; (\exists\, y)\, \langle x, y\rangle \in R \right\}$$
$$ran\, R = \left\{ x \in \bigcup\bigcup R \;\middle|\; (\exists\, t)\, \langle t, x\rangle \in R \right\}$$

## 3.3 n-ary Relations

We can generalise the idea of ordered pairs to higher dimensional concepts. For example, we can define an ordered triple as

$$\langle x, y, z\rangle = \langle \langle x, y\rangle, z\rangle$$

We can continue nesting the ordered tuples as above in order to arrive at an ordered n-tuple for any $n > 1$. For completeness, we define the 1-tuple $\langle x\rangle$ to be just $x$.

**Definition 3.17.** *Let $A$ be a set. We define an **n-ary relation** on $A$ to be the set of ordered n-tuples with all components in $A$.*

## 3.4 Functions

**Definition 3.18.** *Let $F$ be a relation. We say that $F$ is a **function** if for each $x \in dom\, F$, there exists a unique $y$ such that $xFy$. Such a unique element is called the **value** of $F$ at $x$ and is denoted by $F(x)$.*

**Definition 3.19.** *Let $F$ be a function. We say that $F$ is a function **from A into B** or that $F$ **maps A into B**, written $F : A \to B$, if $dom\, F = A$ and $ran\, F \subseteq B$. If $ran\, F = B$ then we say that $F$ is **surjective** or **onto**.*

**Definition 3.20.** *Let $R$ be a relation. We say that $R$ is **single-rooted** if for each $y \in ran\, R$, there is only one $x$ such that $xRy$. Furthermore, if $R$ is a single-rooted function, we say that $R$ is **injective** or **one-to-one**.*

**Definition 3.21.** *Let $A, F$ and $G$ be relations. Then*

1. *The **inverse** of $F$ is the set*

$$F^{-1} = \{ \langle u, v \rangle \mid vFu \}$$

2. *The **composition** of $F$ and $G$ is the set*

$$F \circ G = \{ \langle u, v \rangle \mid \exists t(uGt \wedge tFv) \}$$

3. *The **restriction** of $F$ to $A$ is the set*

$$F|_A = \{ \langle u, v \rangle \mid uFv \wedge u \in A \}$$

4. *The **image of $A$ under $F$** is the set*

$$F[\![A]\!] = ran(F|_A)$$

**Remark.** *In the case that $F$ is a function and $A \subseteq dom\, F$, we can characterise $F[\![A]\!]$ as follows:*

$$F[\![A]\!] = \{ F(u) \mid u \in A \}$$

**Remark.** *Again these definitions only make sense if the corresponding collections are indeed sets. We have that*

1. $F^{-1} \subseteq ran\, F \times dom\, F$
2. $F \circ G \subseteq dom\, G \times ran\, F$
3. $F|_A \subseteq F$
4. $F[\![A]\!] \subseteq ran\, F$

*By the previous section we know that the right hand side of the above set inclusions are indeed sets. For each case we can therefore apply a suitable subset axiom to show that the left hand sides are sets.*

**Example 3.22.** *Consider the function $F : \mathbb{R} \to \mathbb{R}$ given by the equation $F(x) = x^2$. Let $A = [-1, 2]$. Then $F[\![A]\!] = [0, 4]$ and $F^{-1}[\![A]\!] = [-\sqrt{2}, \sqrt{2}]$*

**Example 3.23.** *Let $G : \mathbb{R} \to \mathbb{R}$ be the trigonometric sine function $G(x) = sin(x)$. Then $G^{-1}$ is not a function. Indeed, consider $1 \in dom\, G^{-1}$. Then $\left\langle 1, \frac{\pi}{2} \right\rangle$ and $\left\langle 1, \frac{5\pi}{2} \right\rangle$ are both in $G^{-1}$. However, the restriction*

$$F = G|_{\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]}$$

*is an injective function and hence its inverse is a function.*

**Theorem 3.24.** *Let $F$ be a set. Then $dom\, F^{-1} = ran\, F$ and $ran\, F^{-1} = dom\, F$. Furthermore, if $F$ is a relation then $(F^{-1})^{-1} = F$.*

**Theorem 3.25.** *Let $F$ be a set. Then $F^{-1}$ is a function if and only if $F$ is single-rooted. Furthermore, a relation $F$ is a function if and only if $F^{-1}$ is single-rooted.*

**Theorem 3.26.** *Let $F$ be an injective function. If $x \in dom\, F$ then $F^{-1}(F(x)) = x$. If $y \in ran\, F$ then $F(F^{-1}(y)) = y$.*

*Proof.* Let $x \in dom\, F$. Then by the definition of a function and its inverse, we have that $\langle x, F(x)\rangle \in F$ and $\langle F(x), x\rangle \in F^{-1}$. Hence $F(X) \in dom\, F^{-1}$. Since $F$ is injective, it follows from Theorem 3.26 that $x = F^{-1}(F(x))$.
Now let $y \in ran\, F$. We can apply the first part of the theorem to $F^{-1}$ to see that $(F^{-1})^{-1}(F^{-1}(y)) = y$. But by Theorem 3.24, we know that $(F^{-1})^{-1} = F$. Hence $F(F^{-1}(y)) = y$. □

**Theorem 3.27.** *Let $F$ and $G$ be functions. Then $F \circ G$ is a function with domain*

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

*and for any $x$ in its domain, $(F \circ G)(x) = F(G(x))$.*

*Proof.* Suppose that $x(F \circ G)y = x(F \circ G)z$. We need to show that y = z. By the definition of the composition, we have that for some a and b,

$$xGa \wedge aFy$$
$$xGb \wedge bFz$$

Since G and F are functions, we must have that $a = b$ and $y = z$.

Now let $x \in dom\, G$ and $G(x) \in dom\, F$. We need to show that $x \in$

$dom\,(F \circ G)$ and $(F \circ G)(x) = F(G(x))$. By definition, we have that $\langle x, G(x)\rangle \in G$ and $\langle G(x), F(G(x))\rangle \in F$. Therefore $\langle x, F(G(x))\rangle \in F \circ G$. Finally, suppose that $xindomF \circ G$. Then there exists some $y$ and $t$ such that $xGt$ and $tFy$. Thus, $x \in dom\, G$ and $t = G(x) \in dom\, F$. □

**Example 3.28.** *Let $G$ be an injective function. Then by Theorem 3.27, $G^{-1} \circ G$ is a function with domain*

$$\{\, x \in dom\, G \mid G(x) \in dom\, G^{-1} \,\} = dom\, G$$

*For any $x$ in its domain, Theorem 3.26 implies that*

$$\begin{aligned}(G^{-1} \circ G)(x) &= G^{-1}(G(x)) \\ &= x\end{aligned}$$

*Hence $G^{-1} \circ G = I_{dom\, G}$ or, in other words, the identity function on $dom\, G$. Similarly, we can show that $G \circ G^{-1} = I_{ran\, G}$.*

**Theorem 3.29.** *Let $F$ and $G$ be relations. Then*

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

*Proof.* We have that

$$\begin{aligned}\langle x, y\rangle \in (F \circ G)^{-1} &\iff \langle y, x\rangle \in F \circ G \\ &\iff yGt \wedge tFx && \text{for some } t \\ &\iff xF^{-1}t \wedge tG^{-1}y && \text{for some } t \\ &\iff \langle x, y\rangle \in G^{-1} \circ F^{-1}\end{aligned}$$

□

**Axiom 3.30.** *Axiom of Choice*
*Let $R$ be a relation. Then there exists a function $H \subseteq R$ such that $dom\, H = dom\, R$.*

**Theorem 3.31.** *Let $F : A \to B$ where $A$ is non-empty. Then we have the following*

1. *There exists a function $G : B \to A$, referred to as a **left-inverse**, such that $G \circ F$ is the identity function $I_A$ on $A$ if and only if $F$ is injective.*

2. *There exists a function $H : B \to A$, referred to as a **right-inverse**, such that $F \circ H$ is the identity function $I_B$ on $B$ if and only if $F$ is surjective*

*Proof.*

Part 1:

$\Longrightarrow$ : Assume that there exists a function $G$ such that $G \circ F = I_A$. Suppose that $F(x) = F(y)$. We need to show that $x = y$. Applying $G$ to both sides of the equation, we see that $G(F(x)) = G(F(y))$. But $G$ is a left inverse of $F$ so it follows that $x = y$ and thus $F$ is injective.

$\Longleftarrow$ : Now assume that $F$ is injective. Then $F^{-1}$ is a function from $ran\, F$ onto $A$. We shall extend $F^{-1}$ to a function $G$ that is defined on the whole of $B$. Choose $a \in A$, the existence of which is guaranteed by the fact that $A$ is non-empty. We can then define $G$ as follows:

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

In other words, $G$ sends any point in $B \backslash ran\, F$ to the element $a$. Obviously $G$ is a function mapping $B$ into $A$. Furthermore, $dom\,(G \circ F) = A$ and $G(F(x)) = F^{-1}(x)) = x$ for each $x \in A$. Therefore $G \circ F = I_A$.

Part 2:

$\Longrightarrow$ : Assume that there exists a function $H$ such that $F \circ H = I_B$. Let $y \in B$. We have that $y = F(H(y))$. Hence $y \in ran\, F$ and thus $F$ is surjective.

$\Longleftarrow$ : By the axiom of choice, we can choose a function $H \subseteq F^{-1}$ such that $dom\, H = dom\, F^{-1}$. Since $F$ is surjective, we have that $dom\, H = dom\, F^{-1} = ran\, F = B$. The function $H$ satisfies the results of the theorem. Indeed, $H$ is a function from $B$ into $A$. Let $y \in B$. Then $\langle y, H(y) \rangle \in F^{-1}$ and thus $F(H(y)) = y$.

□

**Theorem 3.32.** *Let $F$ be a relation and $A$ and $B$ sets. Then*

1. $F\,[\![A \cup B]\!] = F\,[\![A]\!] \cup F\,[\![B]\!]$

2. $F[\![\bigcup \mathcal{A}]\!] = \bigcup \{ F[\![A]\!] \mid A \in \mathcal{A} \}$
3. $F[\![A \cap B]\!] \subseteq F[\![A]\!] \cap F[\![B]\!]$
4. $F[\![\bigcap \mathcal{A}]\!] \subseteq \bigcap \{ F[\![A]\!] \mid A \in \mathcal{A} \}$
5. $F[\![A]\!] \setminus F[\![B]\!] \subseteq F[\![A \setminus B]\!]$

*In parts 3,4 and 5, equality holds if $F$ is single-rooted.*

*Proof.* We shall only prove parts 2, 4 and 5. Parts 1 and 3 are simply special cases of parts 2 and 4.

Part 2: Let $y \in F[\![\bigcup \mathcal{A}]\!]$. We have that

$$\begin{aligned} y \in F\left[\!\!\left[\bigcup \mathcal{A}\right]\!\!\right] &\iff \left(\exists\, x \in \bigcup \mathcal{A}\right) xFy \\ &\iff (\exists\, x \in A_1)\, xFy \vee (\exists\, x \in A_2)\, xFy \vee (\exists\, x \in A_3)\, xFy \vee \dots \\ &\iff (y \in F[\![A_1]\!]) \vee (y \in F[\![A_2]\!]) \vee (y \in F[\![A_3]\!]) \vee \dots \\ &\iff y \in \bigcup \{ F[\![A]\!] \mid A \in \mathcal{A} \} \end{aligned}$$

where $A_1, A_2, A_3, \dots$ are understood to be the elements of $\mathcal{A}$.

Part 4: Let $y \in F[\![\bigcap \mathcal{A}]\!]$. We have that

$$\begin{aligned} y \in F\left[\!\!\left[\bigcap \mathcal{A}\right]\!\!\right] &\iff \left(\exists\, x \in \bigcap \mathcal{A}\right) xFy \\ &\implies (\exists\, x \in A_1) xFy \wedge (\exists\, x \in A_2) xFy \wedge \dots \\ &\iff (y \in F[\![A_1]\!]) \wedge (y \in F[\![A_2]\!]) \wedge \dots \\ &\iff y \in \bigcap \{ F[\![A]\!] \mid A \in \mathcal{A} \} \end{aligned}$$

where $A_1, A_2, \dots$ are understood to be the elements of $\mathcal{A}$.
Now consider the second implication. It is not reversible as the individual elements chosen from each $A \in \mathcal{A}$ may be different and thus may not lie in all such $A$. However, if $F$ is single rooted than there can only be once such $x$ where $xFy$. Hence such an $x$ must lie in all $A \in \mathcal{A}$ and the implication becomes reversible.

Part 5: Let $y \in F[\![A]\!] \setminus F[\![B]\!]$. We have that

$$\begin{aligned} y \in F[\![A]\!] \setminus F[\![B]\!] &\iff (\exists\, x \in A) xFy \wedge (\nexists\, t \in B) tFy \\ &\implies (\exists\, x \in A \setminus B) xFy \\ &\iff y \in F[\![A \setminus B]\!] \end{aligned}$$

Now consider the second implication. It is not reversible as $x$ may not necessarily be the only element such that $xFy$. If $F$ is single-rooted then this condition is satisfied and we may reverse the implication.

□

**Corollary 3.33.** *Let $G$ be a function and $A, B, \mathcal{A}$ sets. Then*

1. $G^{-1}[\![\bigcup \mathcal{A}]\!] = \bigcup \{ G^{-1}[\![A]\!] \mid A \in \mathcal{A} \}$
2. $G^{-1}[\![\bigcap \mathcal{A}]\!] = \bigcap \{ G^{-1}[\![A]\!] \mid A \in \mathcal{A} \}$ *for* $\mathcal{A} \neq \varnothing$
3. $G^{-1}[\![A \backslash B]\!] = G^{-1}[\![A]\!] \backslash G^{-1}[\![B]\!]$

*Proof.* This corollary of Theorem 3.32 follows immediately from the fact that the inverse of a function is always single-rooted. □

**Definition 3.34.** *Let $I$ be an indexing set and $F$ a function such that $I \subseteq \operatorname{dom} F$. Then we define*

$$\bigcup_{i \in I} F(i) = \bigcup \{ F(i) \mid i \in I \}$$
$$\bigcap_{i \in I} F(i) = \bigcap \{ F(i) \mid i \in I \}$$

*where in the second equation, we require that $I$ be non-empty.*

**Definition 3.35.** *Let $A$ and $B$ be sets. We define the set* ***B-pre-A*** *to be*

$${}^{A}B = \{ F \mid F : A \to B \}$$

**Remark.** *If $F : A \to B$ then $F \subseteq A \times B$. Hence $F \in \mathcal{P}(A \times B)$. We can then apply a suitable subset axiom to $\mathcal{P}(A \times B)$ to construct the set ${}^{A}B$.*

**Example 3.36.** *Consider $\omega = \{ 0, 1, 2, \dots \}$. Then ${}^{\omega}\{ 0, 1 \}$ is the set of all possible functions $f : \omega \to \{ 0, 1 \}$.*

**Example 3.37.** *Let $A$ be nonempty. We have that ${}^{A}\varnothing = \varnothing$. This is because no function can map a non-empty domain into an empty range. On the other hand, ${}^{\varnothing}A = \{ \varnothing \}$ since $\varnothing$ is the only function with an empty domain.*

## 3.5 Infinite Cartesian Products

**Definition 3.38.** *Let $I$ be an indexing set and $H$ a function such that $I \subseteq dom\, H$. We define the infinite Cartesian product*

$$\prod_{i\in I} H(i) = \{\, f \mid f \text{ is a function with domain } I \text{ and } (\forall\, i \in I) f(i) \in H(i) \,\}$$

**Remark.** *The members of $\prod_{i\in I} H(i)$ are I-tuples (functions with domain $I$) for which the $i^{th}$ coordinate is in $H(i)$. In other words, the members are all the functions from $I$ into $\bigcup_{i\in I} H(i)$ and hence are members of ${}^{I}(\cup_{i\in I} H(i))$. Thus we can construct the infinite Cartesian product by applying a suitable subset axiom to ${}^{I}(\cup_{i\in I} H(i))$.*

**Example 3.39.** *Let $H$ be a function and $A$ a set such that $H(i) = A$ for all $i \in I$. Then $\prod_{i\in I} H(i) = {}^{I}A$.*

**Example 3.40.** *Consider the index set $\omega = \{\, 0, 1, 2, \dots \}$. Then $\prod_{i\in I} H(i)$ consists of $\omega$-sequences that have for their $i^{th}$ term some member of $H(i)$.*

**Remark.** *If any $H(i)$ is empty then obviously the product $\prod_{i\in I} H(i)$ must be empty. Conversely, if $H(i) \neq \varnothing$ for all $i \in I$, it does not necessarily follow that $\prod_{i\in I} \neq \varnothing$. In order to obtain a member of $f$ of the product, we need to select some members from each $H(i)$ and set $f(i)$ equal to the selected element. This requires the axiom of choice.*

**Axiom 3.41.** *Axiom of Choice (second form)*
*Let $I$ be any set and $H$ any function with domain $I$. If $H(i) \neq \varnothing$ for all $i \in I$ then $\prod_{i\in I} H(i) \neq \varnothing$.*

**Theorem 3.42.** *The first form of the Axiom of Choice (Axiom 3.30) is equivalent to the second form (Axiom 3.41).*

*Proof.*

$\Longrightarrow$ : Assume the first form of the axiom. Let $I$ be an indexing set and $H$ a function such that $dom\, H = I$ and $H(i) \neq \varnothing$. Define a relation $R \subseteq I \times \bigcup_{i\in I} H(i)$ by

$$\langle i, x\rangle \in R \iff x \in H(i)$$

We first note that $R$ is non-empty. Indeed for all $i \in I$, $i \in dom\, R$ as $H(i)$ is non-empty. By the first form of the axiom of choice, there exists a function $G \subseteq R$ such that $dom\, G = dom\, R = I$. Hence for all $\langle i, G(i)\rangle \in G$ we have that $\langle i, G(i)\rangle \in R$. By the definition of $R$, it follows that $G(i) \in H(i)$ whence we see that $G \in \prod_{i\in I} H(i)$. Hence $\prod_{i\in I} H(i)$ is non-empty.

$\Longleftarrow$ : Now assume the second form of the axiom. Let $R$ be any relation. We need to exhibit a function $G \subseteq R$ such that $dom\, G = dom\, R$. Denote $dom\, R = I$ and define the function

$$\begin{aligned} H : I &\to \mathcal{P}(ran\, R) \\ i &\mapsto \{\, x \in ran\, R \mid iRx \,\} \end{aligned}$$

It is easy to see that $H$ is a function with domain $I$. We first note that $H(i) \neq \varnothing$ for all $i \in I$. Thus by the second form of the axiom of choice, we have that $\prod_{i\in I} H(i) \neq \varnothing$. Now choose $G \in \prod_{i\in I} H(i)$. By the definition of the infinite product, $dom\, G = I$ and for all $i \in I$, $G(i) \in H(i)$. Now take $\langle i, G(i)\rangle \in G$. We have that $G(i) \in H(i) \subseteq ran\, R$ whence it follows that $\langle i, G(i)\rangle \in R$. Hence $G \subseteq R$.

□

## 3.6 Equivalence Relations

**Definition 3.43.** *Let $R$ be a relation. We say that $R$ is a binary relation on a set $A$ if $R \subseteq A \times A$.*

**Definition 3.44.** *Let $R$ be a binary relation on a set $A$. We say that $R$ is*

1. ***reflexive** on $A$ if $xRx$ for all $x \in A$*
2. ***symmetric** if whenever $xRy$ then $yRx$*
3. ***transitive** if whenever $xRy$ and $yRz$ then $xRz$*

**Definition 3.45.** *Let $R$ be a binary relation on a set $A$. We say that $R$ is an **equivalence relation** on $A$ if $R$ is reflexive on $A$, symmetric and transitive.*

**Theorem 3.46.** *Let $R$ be a symmetric and transitive relation. Then $R$ is an equivalence relation on $fld\, R$.*

*Proof.* It is trivial that a relation $R$ is a binary relation on its field. Indeed

$$R \subseteq dom\, R \times ran\, R \subseteq fld\, R \times fld\, R$$

We must now show that $R$ is reflexive on $fld\, R$. Let $x \in fld\, R$. Without loss of generality, we may assume that $x \in dom\, R$. Then

$$\begin{aligned} x \in dom\, R &\iff xRy \\ &\implies xRy \wedge yRx \\ &\implies xRx \end{aligned}$$

where in the first line we used the definition of the relation $R$. In the second line we used symmetry and in the last line we used transitivity. □

**Definition 3.47.** *We define the set* $[x]_R$ *by*

$$[x]_R = \{\, t \mid xRt \,\}$$

*If* $R$ *is an equivalence relation and* $x \in fld\, R$ *then* $[x]_R$ *is referred to as the* ***equivalence class of*** **x** ***(modulo*** **R***)***

**Remark.** *Obviously,* $[x]_R \subseteq ran\, R$ *and thus such a set can be constructed by the application of a suitable subset axiom to* $ran\, R$*. Furthermore, we can contruct a set of equivalence classes since such a set is included in* $\mathcal{P}(ran\, R)$*.*

**Lemma 3.48.** *Let* $R$ *be an equivalence relation on a set* $A$ *and let* $x, y \in A$*. Then*

$$[x]_R = [y]_R \iff xRy$$

*Proof.*

$\implies$ : Assume that $[x]_R = [y]_R$. We need to show that $xRy$. Since $R$ is reflexive, we have that $y \in [y]_R$. Hence, it follows that $y \in [x]_R$. But by the

definition of the equivalence class, we have that $xRy$.

$\Longleftarrow$ : Now assume that $xRy$. We need to show that $[x]_R = [y]_R$. Let $t \in [x]_R$. We show that $t \in [y]_R$. We have that

$$\begin{aligned} t \in [x]_R &\iff xRt && \text{(definition)} \\ &\iff xRt \wedge xRy && \text{(assumption)} \\ &\iff tRx \wedge xRy && \text{(reflexivity)} \\ &\iff tRy && \text{(transitivity)} \\ &\iff yRt && \text{(reflexvity)} \\ &\iff t \in [y]_R \end{aligned}$$

Hence $[y]_R \subseteq [x]_R$. Now since $R$ is symmetric, we have that $yRx$ and we can reverse $x$ and $y$ in the above argument to obtain $[x]_R \subseteq [y]_R$.

□

**Definition 3.49.** *Let $I$ be an index set and $\{A_i\}_{i\in I}$ a collection of subsets of $\mathcal{A}$. We say that the sets in $X$ are **exhaustive** if each element of $A$ is in some $A_i$.*

**Definition 3.50.** *Let $A$ be a set. We say that a set $\Pi$ is a **partition** of $A$ if $\Pi$ consists of non-empty subsets that are disjoint and exhaustive.*

**Theorem 3.51.** *Let $R$ be an equivalence relation on $A$. Then the set*

$$\Pi_A = \{\, [x]_R \mid x \in A \,\}$$

*is a partition of $A$.*

*Proof.* We need to show that $\Pi_A$ consists of non-empty subsets of $A$ that are disjoint and exhaustive. Since $R$ is an equivalence relation, it is reflexive. Hence given any $x \in A$, we have that $xRx$ and thus $x \in [x]_R$. Thus each equivalence class is a non-empty subset of $A$ and in particular, the collection is exhaustive.
Now let $[x]_R, [y]_R \in \Pi_A$ and suppose that they contain a common element $t$. We have that $xRt$ and $yRt$. Since $R$ is an equivalence relation, it is transitive and thus $xRy$. Now by Lemma 3.48, we must have that $[x]_R = [y]_R$. Hence the elements of $\Pi_A$ are all disjoint.

□

**Definition 3.52.** *Let $R$ be an equivalence relation on a set $A$. We define the* ***quotient set A modulo R*** *$A/R$ to be*

$$A/R = \{\, [x]_R \mid x \in A \,\}$$

*Furthermore, we define the* ***natural map*** *(or* ***canonical map****) $\varphi(x)$ by*

$$\begin{aligned} \varphi : A &\to A/R \\ x &\mapsto [x]_R \end{aligned}$$

**Example 3.53.** *Let $\omega = \{\, 0, 1, 2, \dots \,\}$. Consider the binary relation $\sim$ on $\omega$*

$$m \sim n \iff m - n \text{ is divisible by six}$$

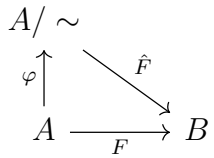
*Then $\sim$ is an equivalence relation on $\omega$. The quotient set $\omega/\sim$ consists of the following equivalence classes*

$$[0]_\sim, [1]_\sim, [2]_\sim, [3]_\sim, [4]_\sim, [5]_\sim$$

**Example 3.54.** *Let $F : A \to B$ be a function and define a binary relation $\sim$ on $A$ by*

$$x \sim y \iff F(x) = F(y)$$

*Then $\sim$ is an equivalence relation on $A$. Furthermore, there exists a unique injective function $\hat{F} : A/\sim \to B$ such that $F = \hat{F} \circ \varphi$ where $\varphi$ is understood to be the natural map from $A$ into $A/\sim$. This is demonstrated by the following diagram:*




*The value of $\hat{F}$ at a particular equivalence class is the common value of $F$ at the members of the equivalence class.*

**Definition 3.55.** *Let $F : A \to A$ be a function and $R$ a binary relation on $A$. We say that $F$ is* ***compatible*** *with $R$ if for all $x, y \in A$ we have*

$$xRy \implies F(x)RF(y)$$

**Theorem 3.56.** *Let $R$ be an equivalence relation on $A$ and $F : A \to A$ a function. If $F$ is compatible with $R$ then there exists a unique function $\hat{F} : A/R \to A/R$ such that*

$$\hat{F}([x]_R) = [F(x)]_R \quad \text{for all } x \in A \tag{3.1}$$

*If $F$ is not compatible with $R$ then no such $\hat{F}$ can exist.*

*Proof.* First suppose that $F$ is not compatible with $R$. We show that there cannot exist a function $\hat{F}$ satisfying Equation 3.1. By the definition of incompatiblity, there exists $x, y \in A$ such that $xRy$ but not $F(x)RF(y)$. Applying Lemma 3.48, we see that $[x]_R = [y]_R$ but $[F(x)]_R \neq [F(y)]_R$. Now in order for Equation 3.1 to hold, we require that $\hat{F}([x]_R) = [F(x)]_R$ and $\hat{F}([y]_R) = [F(y)]_R$. But the left hand sides of these equations coincide yet the right hand sides do not. Hence there cannot exist such a function $\hat{F}$.
Now assume that $F$ is compatible with $R$. We first observe that Equation 3.1 implies that the ordered pair $\langle [x]_R, [F(x)]_R \rangle \in \hat{F}$. Hence we shall try and define $\hat{F}$ as

$$\hat{F} = \{ \langle [x]_R, [F(x)]_R \rangle \mid x \in A \}$$

We must first show that $\hat{F}$ is a function. Consider the ordered pairs $\langle [x]_R, [F(x)]_R \rangle$, $\langle [y]_R, [F(y)]_R \rangle \in \hat{F}$. We must show that if $[x] = [y]$ then $[F(x) = [F(y)]$. We have that

$$\begin{aligned} [x] = [y] &\iff xRy \text{ (Lemma 3.48)} \\ &\implies F(x)RF(y) \text{ (compatibility)} \\ &\iff [F(x)] = [F(y)] \text{ (Lemma 3.48)} \end{aligned}$$

Now, by construction we have that $dom\, \hat{F} = A/R$ and $ran\, \hat{F} = A/R$ whence we see that $\hat{F} : A/R \to A/R$. Furthermore we can see by definition that for all $x \in A, \langle [x]_R, [F(x)]_R \rangle \in \hat{F}$ and thus Equation 3.1 is satisfied.
It suffices to show that $\hat{F}$ is the unique function satisfying Equation 3.1. Suppose $G$ is another function that satisfies such conditions. We have that $G([x]_R) = [F(x)]_R$ for all $x \in A$. Obviously, $\langle [x]_R, [F(x)]_R \rangle \in \hat{F} \iff \langle [x]_R, [F(x)]_R \rangle \in G$ and thus $G = \hat{F}$. □

## 3.7 Ordering Relations

**Definition 3.57.** *Let $A$ be a set. A **linear ordering** on $A$ (or **total ordering**) is a binary relation $R$ on $A$ that satisfies the following conditions:*

1. *transitivity*
2. ***trichotomy** on $A$. In other words, given any $x$ and $y$ in $A$ then exactly one of the following holds:*

$$xRy, \quad x = y, \quad yRx$$

**Theorem 3.58.** *Let $R$ be a linear ordering on $A$. Then there is no $x \in A$ for which $xRx$. Furthermore, for distinct $x, y \in A$, either $xRy$ or $yRx$.*

*Proof.* The theorem follows directly from the fact that $R$ satisfies trichotomy on $A$. □

**Notation 3.59.** *We shall usually write a linear ordering $R$ as $<$. For example, if $xRy$ we write $x < y$.*

# Chapter 4

# Natural Numbers

## 4.1 Inductive Sets

**Definition 4.1.** *Let $a$ be a set. We define the* ***successor*** *of $a$, $a^+$ to be*

$$a^+ = a \cup \{ a \}$$

**Definition 4.2.** *Let $A$ be a set. We say that $A$ is* ***closed under successor*** *if*

$$(\forall\, a \in A) a^+ \in A$$

**Definition 4.3.** *Let $A$ be a set. We say that $A$ is* ***inductive*** *if $\varnothing \in A$ and it is closed under successor.*

**Remark.** *In terms of the successor operation, we can define the first few natural numbers as follows:*

$$0 = \varnothing, \quad 1 = \varnothing^+, \quad 2 = \varnothing^{++}, \quad 3 = \varnothing^{+++}$$

**Axiom 4.4.** *Infinity Axiom*
*There exists an inductive set:*

$$(\exists\, A)[\varnothing \in A \wedge (\forall\, a \in A) a^+ \in A]$$

**Definition 4.5.** *A* ***natural number*** *is a set that belongs to every inductive set.*

**Theorem 4.6.** *There is a set whose members are exactly the natural numbers.*

*Proof.* Let $A$ be an inductive set, the existence of which is guaranteed by the infinity axiom. By a subset axiom , there is a set $w$ such that for any $x$,

$$\begin{aligned} x \in w &\iff x \in A \wedge \text{ x belongs to every other inductive set} \\ &\iff \text{ x belongs to every inductive set} \end{aligned}$$

□

**Notation 4.7.** *We denote the set of all natural numbers by $\omega$.*

**Theorem 4.8.** *$\omega$ is inductive and is a subset of every other inductive set.*

*Proof.* Since $\varnothing$ belongs to every inductive set, it follows that $\varnothing \in \omega$. Now,

$$\begin{aligned} a \in \omega &\implies a \text{ belongs to every inductive set} \\ &\implies a^+ \text{ belongs to every inductive set} \\ &\implies a^+ \in \omega \end{aligned}$$

Hence $\omega$ is inductive. It follows that $\omega$ is included in every other inductive set. □

**Principle 4.9.** *Inductive Principle for $\omega$*
*Any inductive subset of $\omega$ coincides with $\omega$.*

Suppose that we want to prove that, for every natural number $n$, the statement $P(n)$ holds. We form the set

$$T = \{\, n \in \omega \mid P(n) \,\}$$

of natural numbers satisfying $P(n)$. If $T$ is inductive then $P(n)$ is true for all natural numbers. Such a proof is said to be a proof by **induction**.

**Theorem 4.10.** *Every natural number except 0 is the successor of some natural number.*

*Proof.* Let $T = \{\, n \in \omega \mid n = 0 \vee (\exists\, p \in \omega) n = p^+ \,\}$. Then $0 = \varnothing \in T$. Obviously if $k \in T$ then $k^+ \in T$. Hence $T$ is inductive and thus by induction, $T = \omega$. □

## 4.2 Peano's Postulates

**Definition 4.11.** *Let $S$ be a function and $A \subseteq \operatorname{dom} S$. $A$ is said to be* ***closed*** *under $S$ if whenever $x \in A$ then $S(x) \in A$.*

**Definition 4.12.** *A* ***Peano system*** *is a triple $\langle N, s, e\rangle$ consisting of a set $N$, a function $S : N \to N$ and a member $e \in N$ such that the following three conditions hold:*

1. *$e \notin \operatorname{ran} S$*
2. *$S$ is injective*
3. *Any subset $A$ of $N$ that contains $e$ and is closed under $S$ equals $N$ itself.*

**Remark.** *The last condition in the above definition is referred to as the* ***Peano induction postulate****.*

**Definition 4.13.** *Let $A$ be a set. We say that $A$ is* ***transitive*** *if every member of a member of $A$ is itself a member of $A$:*

$$x \in a \in A \implies x \in A$$

**Remark.** *The above definition can be reformulated in any of the followng ways:*

$$\bigcup A \subseteq A$$
$$a \in A \implies a \subseteq A$$
$$A \subseteq \mathcal{P}(A)$$

**Example 4.14.** *The set $A = \{\varnothing, \{\{\varnothing\}\}\}$ is not a transitive set. Indeed, $\{\varnothing\} \in \{\{\varnothing\}\} \in A$ but $\{\varnothing\} \notin A$.*

**Example 4.15.** *The set $A = \{0, 1, 5\}$ is not transitive. Indeed, $4 \in 5 \in A$ but $4 \notin A$.*

**Theorem 4.16.** *Let $a$ be a transitive set. Then*

$$\bigcup a^+ = a$$

*Proof.* We have that

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

where in the last step we used the definition of transitivity of a set: $\bigcup a \subseteq a$. □

**Theorem 4.17.** *Every natural number is a transitive set.*

*Proof.* We shall prove the theorem by induction. We first form the set of natural numbers for which the theorem is true:

$$T = \{\, n \in \omega \mid n \text{ is a transitive set} \,\}$$

We have to show that $T$ is an inductive set. Obviously, $\varnothing = 0 \in T$. Now let $k \in T$. By definition, $k$ is transitive. We need to show that $k^+ \in T$. By the previous theorem, we see that

$$\begin{aligned}\bigcup(k^+) &= k \\ &\subseteq k^+\end{aligned}$$

whence $k^+ \in T$. Therefore $T$ is inductive and, by the inductive principle, $T = \omega$. □

**Notation 4.18.** *We denote by $\sigma$ the restriction of the successor operation to $\omega$:*

$$\sigma = \{\, \langle n, n^+ \rangle \mid n \in \omega \,\}$$

**Theorem 4.19.** *$\langle \omega, \sigma, 0 \rangle$ is a Peano system.*

*Proof.* Since $\omega$ is an inductive set, we have that $0 \in \omega$ and $\sigma : \omega \to \omega$. Now, the Peano induction postulate, as applied to $\langle \omega, \sigma, 0 \rangle$, states that any subset $A$ of $\omega$ containing 0 and closed under $\sigma$ equals $\omega$ itself. Clearly, this is just the induction principle for $\omega$. Furthermore, $0 \notin ran, \sigma$ since there does not

exist a natural number $n$ such that $n^+ = \varnothing$. It now remains to show that $\sigma$ is injective. Suppose $m^+ = n^+$. We need to show that $m = n$. We have that

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

where in the last line we have used the fact that $m$ and $n$ are transitive sets and Theorem 4.16. □

**Theorem 4.20.** *The natural numbers are a transitive set.*

*Proof.* We shall prove the theorem by induction. We need to show that $(\forall\, n \in \omega) n \subseteq \omega$. We first form the set of natural numbers for which this holds:

$$T = \{\, n \in \omega \mid n \subseteq \omega \,\}$$

We need to show that $T$ is inductive. Trivially, $0 \in T$. Let $k \in T$. We must show that $k^+ \in T$. By definition of $T$, we have that $k \subseteq \omega$ and $\{\, k \,\} \subseteq \omega$. It follows that $k^+ = k \cup \{\, k \,\} \in \omega$ and thus $T$ is inductive. Hence by the inductive principle, $T = \omega$. □

**Theorem 4.21.** *Recursion theorem on $\omega$*
*Let $A$ be a set, $a \in A$ and $F : A \to A$ a function. Then there exists a unique function $h : \omega \to A$ such that*

$$h(0) = a$$

*and for every $n \in \omega$,*

$$h(n^+) = F(h(n))$$

*Proof.* We show that $h$ is the union of many approximating functions. For the purpose of this proof, we shall call a function $v$ **acceptable** if $dom\, v \subseteq \omega, ran\, v \subseteq A$ and the following conditions hold:

1. If $0 \in dom\, v$ then $v(0) = a$
2. If $n^+ \in dom\, v$ for some natural number $n$ then also $n \in dom\, v$ and $v(n^+) = F(v(n))$

Now let $\mathcal{H}$ denote the collection of all acceptable functions and let $h \in \bigcup \mathcal{H}$. We see that

$$\langle n, y\rangle \in h \iff v(n) = y \text{ for some acceptable } v \tag{4.1}$$

We claim that $h$ satisfies the demands of the theorem. We shall prove this in four parts: we show that $h$ is a function, that $h$ is acceptable, that $dom\, h = \omega$ and that $h$ is unique.

Part 1: We must show that $h$ is a function. Let $S$ denote the set of all natural numbers at which there is no more than one value of $h(n)$:

$$S = \{\, n \in \omega \mid \text{for at most one } y, \langle n, y\rangle \in h \,\}$$

We show that $S$ is an inductive set. In order to do so, we must first show that $0 \in S$. Suppose that $\langle 0, y_1\rangle, \langle 0, y_2\rangle \in h$. Then by the definition of $h$, there must exist acceptable functions $v_1$ and $v_2$ such that $v_1(0) = y_1$ and $v_2(0) = y_2$. But by the definition of an acceptable function, we see that $y_1 = v_1(0) = a = v_2(0) = y_2$. Hence $0 \in S$.
Now let $k \in S$. We need to show that $k^+ \in S$. Suppose that $\langle k^+, y_1\rangle, \langle k^+, y_2\rangle \in h$. By the definition of $h$, there must exist acceptable functions $v_1$ and $v_2$ such that $v_1(k^+) = y_1$ and $v_2(k^+) = y_2$. Now by the definition of an acceptable function, we must have that $v_1(k^+) = F(v_1(k))$ and $v_2(k) = F(v_2(k))$. But $k \in S$ and thus $v_1(k) = v_2(k)$. It therefore follows that $y_1 = y_2$ and $S$ is inductive. By the induction principle on $\omega$, $S = \omega$ and thus $h$ is a function.

Part 2: We now show that $h$ is itself acceptable. It is clear from 4.1 that $dom\, h \subseteq \omega$ and $ran\, h \subseteq A$. We now need to show conditions 1 and 2.
Suppose that $0 \in dom\, h$. Then by the definition of $h$, there must exist some acceptable function $v$ such that $v(0) = h(0)$. Since $v(0) = a$, we have that $h(0) = a$.
Now suppose that $n^+ \in dom\, h$. There must exist some acceptable $v$ such that $v(n^+) = h(n^+)$. Hence we have that $n \in dom\, v$ and $v(n) = h(n)$. Then

$$h(n^+) = v(n^+) = F(v(n)) = F(h(n))$$

Part 3: We now have to prove that $dom\, h = \omega$. To this end, we show that $dom\, h$ is inductive. Obviously, the function $\{\, \langle 0, a\rangle \,\}$ is acceptable and thus

$0 \in dom\, h$. Now suppose that $k \in dom\, h$. We must show that $k^+ \in dom\, h$. If $k^+ \notin h$ then consider the function

$$v = h \cup \{ \langle k^+, F(h(k)) \rangle \}$$

We shall show that $v$ is acceptable. Obviously, $dom\, v \subseteq \omega$ and $ran\, v \subseteq A$. Obviously condition 1 holds as $v(0) = h(0)$ and $h$ is acceptable. It remains to check condition 2.
Suppose that $n^+ \in dom\, v$ for some $n \in \omega$ and $n^+ \neq k^+$ then $n^+ \in dom\, h$ and $v(n^+) = h(n^+) = F(h(n)) = F(v(n))$. Now suppose that $n^+ = k^+$. Since the successor operation is injective, we must have that $n = k$. Now, by assumption, $k \in dom\, h$ whence it follow that $v(k^+) = F(h(k)) = F(v(k))$. We see that $v$ is an acceptable function. But by the definition of $h, v \subseteq h$ and thus $k^+ \in dom\, h$. Hence $dom\, h$ is inductive and thus coincides with $\omega$.

Part 4: It now suffices to show that $h$ is unique. Let $h_1$ and $h_2$ both satisfy the conclusion of the theorem. Denote $S$ by the set in which both $h_1$ and $h_2$ agree:

$$S = \{ n \in \omega \mid h_1(n) = h_2(n) \}$$

We claim that $S$ is inductive. We must first show that $0 \in S$. We first note that $dom\, h_1 = dom\, h_2 = \omega$. Hence $0 \in dom\, h_1, dom\, h_2$. By the definition of an acceptable function, it follows that $h_1(0) = h_2(0) = a$ and thus $0 \in S$.
Now assume that $k \in S$. We must show that $k^+ \in S$. Since $h_1$ is acceptable, we have that $h_1(k^+) = F(h_1(k))$. But by assumption, $h_1(k) = h_2(k)$. Thus $F(h_1(k)) = F(h_2(k)) = h_2(k^+)$. It follows that $k^+ \in S$ and so $S$ is inductive. Since $S = \omega$, we have that $h_1 = h_2$. □

**Example 4.22.** *Let $\mathbb{Z}$ be the set of all integers. Then there does not exist a function $h : \mathbb{Z} \to \mathbb{Z}$ such that for all $a \in \mathbb{Z}, h(a+1) = h(a)^2 + 1$. Indeed, $h(a) > h(a-1) > h(a-2) > \cdots > 0$. Recursion on $\omega$ relies on there being a starting point 0. However, $\mathbb{Z}$ has no such starting point.*

**Example 4.23.** *Let $\mathbb{Z}$ be the set of all integers. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$:*

$$F(a) = \begin{cases} a+1 & \text{if } a < 0 \\ a & \text{if } a \geq 0 \end{cases}$$

*Then there are infinitely many functions $h : \mathbb{Z} \to \mathbb{Z}$ such that $h(0) = 0$ and for all $a \in \mathbb{Z}, h(a+1) = F(h(a))$.*

**Theorem 4.24.** *Let $\langle N, S, e\rangle$ be a Peano system. Then $\langle w, \sigma, 0\rangle$ is isomorphic to $\langle N, S, e\rangle$. In other words, there exists a function $h$ mapping $\omega$ bijectively onto $N$ in a way that preserves the successor operation*

$$h(\sigma(n)) = S(h(n))$$

*and the zero element*

$$h(0) = e$$

*Proof.* The recursion theorem implies that there exists a unique function $h : \omega \to N$ such that $h(0) = e$ and for all $n \in \omega, h(n^+) = S(h(n))$. It suffices to show that $h$ is bijective.
We first show that $h$ is surjective. We claim that $ran\, h = N$. To this end, we shall employ the Peano induction postulate for $\langle N, S, e\rangle$. Obviously, $e \in ran\, h$. Now fix $x \in ran\, h$ such that $x = h(n)$ for some $n \in \omega$. We have that $S(x) \in ran\, h$ as $S(x) = h(n^+)$. Therefore, by the Peano induction postulate applied to $ran\, h$, we have that $ran\, h = N$.
We now show that $h$ is injective. Let

$$T = \{\, n \in \omega \mid \text{ for every } m \in \omega \text{ different from n }, h(m) \neq h(n) \,\}$$

We claim that $T$ is an inductive set. We first show that $0 \in T$. By Theorem 4.10, we know that any $m \in \omega$ that does not coincide with 0 must be of the form $p^+$ for some other $p \in \omega$. Furthermore, we have that $h(p^+) = S(h(p)) \neq e$ since $e \notin ran\, S$. Hence $h(0) = e \neq h(p^+)$ and thus $0 \in T$.
Now assume that $k \in T$. We must show that $k^+ \in T$. Suppose that $h(k^+) = h(m)$. Then by the preceding result, $m \neq 0$ and so $m = p^+$ for some $p$. Thus

$$S(h(k)) = h(k^+) = h(p^+) = S(h(p))$$

But $S$ is an injective function and thus $h(k) = h(p)$. Since $k \in T$, we have that $k = p$ and hence $k^+ = p^+ = m$. It follows that $k^+ \in T$ and thus $T$ is inductive. $T$ therefore coincides with all of $\omega$ and consequently, $h$ is injective. □

**Remark.** *The equation $h(\sigma(n)) = S(h(n))$ implies that $h(1) = S(e), h(2) = S(S(e)), \ldots$ as shown in the following diagram:*

$$\begin{array}{ccccccccccc}
0 & \xrightarrow{\sigma} & 1 & \xrightarrow{\sigma} & 2 & \xrightarrow{\sigma} & 3 & \xrightarrow{\sigma} & \ldots \\
\downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h} & & \\
e & \longrightarrow & S(e) & \longrightarrow & S(S(e)) & \longrightarrow & S(S(S(e))) & \longrightarrow & \ldots
\end{array}$$

## 4.3 Arithmetic

Recursion guarantees us the existence of a function $A_m : \omega \to \omega$ for all $m \in \omega$ satisfying the following conditions:

$$A_m(0) = m$$
$$A_m(n^+) = A_m(n)^+$$

for some $n \in \omega$.

**Definition 4.25.** *We define the binary operation* ***addition*** *$(+)$ on $\omega$ such that for any $m$ and $n$ in $\omega$,*

$$m + n = A_m(n)$$

*As a relation, this is written as*

$$\{ \langle \langle m, n \rangle, p \rangle \mid m \in \omega \wedge n \in \omega \wedge p = A_m(n) \}$$

**Theorem 4.26.** *Let $m$ and $n$ be natural numbers. Then*

$$m + 0 = m \tag{A1}$$
$$m + n^+ = (m + n)^+ \tag{A2}$$

Let $n, m \in \omega$. Recursion also guarantees the existence of a function $M_m : \omega \to \omega$ such that

$$M_m(0) = 0$$
$$M_m(n^+) = M_m(n) + m$$

**Definition 4.27.** *We define the binary operation (multiplication) $(\cdot)$ on $\omega$ such that for any $m$ and $n$ in $\omega$,*

$$m \cdot n = M_m(n)$$

**Example 4.28.** *2 + 2 = 4:*

$$\begin{aligned} 2+0 &= 2 && \text{by } (A1)\\ 2+1 &= 2+0^+ \\ &= (2+0)^+ && \text{by } (A2)\\ &= 2^+ \\ &= 3 \\ 2+2 &= 2+1^+ \\ &= (2+1)^+ \\ &= 3^+ \\ &= 4 \end{aligned}$$

**Theorem 4.29.** *The following identities hold for all natural numbers:*

1. *Associative law for addition*

$$m + (n + p) = (m + n) + p$$

2. *Commutative law for addition*

$$m + n = n + m$$

3. *Distributive law*

$$m \cdot (n + p) = m \cdot n + m \cdot p$$

4. *Associative law for multiplication*

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p$$

5. *Commutative law for multiplication*

$$m \cdot n = n \cdot m$$

*Proof.* We shall prove each part of the theorem by induction.

Part 1: Consider the set

$$A = \{\, p \in \omega \mid m + (n + p) = (m + n) + p \,\}$$

We claim that $A$ is an inductive set. It is trivial to see that $0 \in A$. Now let $k \in A$. We must show that $k^+ \in A$. We have that

$$\begin{aligned} m + (n + k^+) &= m + (n + k)^+ && \text{by } (A2) \\ &= (m + (n + k))^+ && \text{by } (A2) \\ &= ((m + n) + k)^+ && \text{by assumption} \\ &= (m + n) + k^+ && \text{by } (A2) \end{aligned}$$

Thus $k^+ \in A$ and $A$ is an inductive set. It follows that $A = \omega$.

Part 2: We first show that $0 + n = n$ for all $n \in \omega$ [1]. This is equivalent to showing that the following set is inductive:

$$A = \{\, n \in \omega \mid 0 + n = n \,\}$$

Obviously, $0 \in A$ by (A1). Now suppose that $k \in A$. Then

$$\begin{aligned} 0 + k^+ &= (0 + k)^+ && \text{by } (A2) \\ &= k^+ && \text{since } k \in A \end{aligned}$$

and thus $k^+ \in A$ so $A$ is inductive.
We must now show that $m^+ + n = (m + n)^+$ for all $m, n \in \omega$. Fix $m \in \omega$ and let

$$B = \{\, n \in \omega \mid m^+ + n = (m + n)^+ \,\}$$

By (A1), $0 \in B$. Now let $k \in B$. We have that

$$\begin{aligned} m^+ + k^+ &= (m^+ + k)^+ && \text{by } (A2) \\ &= (m + k)^{++} && \text{since } k \in B \\ &= (m + k^+)^+ && \text{by } (A2) \end{aligned}$$

whence it follows that $k^+ \in B$ and $B$ is inductive.
We are now in a position to prove the commutative law. Let $n \in \omega$ and

$$\{\, m \in \omega \mid m + n = n + m \,\}$$

[1] Note that this is proving that 0 is a left additive identity. Theorem 4.26 states that 0 is a right additive identity.

We claim that $C$ is inductive. By the first result, we have that $0 + n = n = n + 0$ and thus $0 \in C$. Now suppose that $k \in C$. We wish to show that $k^+ \in C$. We have that

$$\begin{aligned} k^+ + n &= (k + n)^+ && \text{by the second result} \\ &= (n + k)^+ && \text{since } k \in C \\ &= n + k^+ \end{aligned}$$

and thus $k^+ \in C$. Thus $C$ is inductive and coincides with all of $\omega$.

Part 3: Let $m, n \in \omega$ and

$$A = \{\, p \in \omega \mid m \cdot (n + p) = m \cdot n + m \cdot p \,\}$$

We claim that $A$ is an inductive set. We must first show that $0 \in A$. We have that

$$\begin{aligned} m \cdot (n + 0) &= m \cdot n && \text{by (A1)} \\ &= m \cdot n + 0 && \text{by (A1)} \\ &= m \cdot n + m \cdot 0 && \text{by (M1)} \end{aligned}$$

Hence $0 \in A$. Now assume that $k \in A$. We want to show that $k^+ \in A$. We have that

$$\begin{aligned} m \cdot (n + k^+) &= m \cdot (n + k)^+ && \text{by (A2)} \\ &= m \cdot (n + k) + m && \text{by (M2)} \\ &= (m \cdot n + m \cdot k) + m && \text{since } k \in A \\ &= m \cdot n + (m \cdot k + m) && \text{by Part 1} \\ &= m \cdot n + m \cdot k^+ && \text{by (M2)} \end{aligned}$$

and thus $k^+ \in A$ whence $A$ is inductive.

Part 4: Let $m, n \in \omega$ and

$$A = \{\, p \in \omega \mid m \cdot (n \cdot p) = (m \cdot n) \cdot p \,\}$$

We claim that $A$ is an inductive set. We have that $m \cdot (n \cdot 0) = m \cdot 0 = 0$ by (M1) and, similarly, $(m \cdot n) \cdot 0 = 0$. Thus $0 \in A$. Now assume $k \in A$. We

need to show that $k^+ \in A$. We have that

$$\begin{aligned} m \cdot (n \cdot k^+) &= m \cdot (n \cdot k + n) && \text{by (M2)} \\ &= m \cdot (n \cdot k) + m \cdot n && \text{by Part 3} \\ &= (m \cdot n) \cdot k + m \cdot n && \text{since } k \in A \\ &= (m \cdot n) \cdot k^+ && \text{by (M2)} \end{aligned}$$

and thus $k^+ \in A$ whence $A$ is inductive.

Part 5: We first show that $0 \cdot n = 0$ for all $n \in \omega$. This is equivalent to showing that the following set is inductive:

$$A = \{\, n \in \omega \mid 0 \cdot n = 0 \,\}$$

It follows trivially from (M1) that $0 \in A$. Now let $k \in A$. We must show that $k^+ \in A$. We have that

$$\begin{aligned} 0 \cdot k^+ &= 0 \cdot k + 0 && \text{by (M2)} \\ &= 0 \cdot k && \text{by (A1)} \\ &= 0 && \text{since } k \in A \end{aligned}$$

Thus $k^+ \in A$ and $A$ is inductive.
Fix $m \in \omega$. We must now show that $m^+ \cdot n = m \cdot n + n$. It suffices to prove that the following set is inductive:

$$B = \{\, n \in \omega \mid m^+ \cdot n = m \cdot n + n \,\}$$

It follows from (A1) and (M1) that $0 \in B$. Now let $k \in B$. We have that

$$\begin{aligned} m^+ \cdot k^+ &= m^+ \cdot k + m^+ && \text{by (M2)} \\ &= m \cdot k + k + m^+ && \text{since } k \in B \\ &= m \cdot k + (k + m)^+ && \text{by (A2)} \\ &= m \cdot k + (m + k)^+ && \text{by Part 2} \\ &= m \cdot k + m + k^+ && \text{by (A2)} \\ &= m \cdot k^+ + k^+ && \text{by (M2)} \end{aligned}$$

Thus $k^+ \in B$ and $B$ is inductive.
We are now ready to show that $m \cdot n = n \cdot m$. It suffices to show that the following set is inductive:

$$C = \{\, n \in \omega \mid m \cdot n = n \cdot m \,\}$$

We must first show that $0 \in C$. By (M1), we have that $m \cdot 0 = 0$. By the first result of this section, we have that $0 \cdot m = 0$. Hence $m \cdot 0 = 0 \cdot m$ and $0 \in C$. Now assume that $k \in C$. We must show that $k^+ \in C$. We have that

$$\begin{aligned} m \cdot k^+ &= m \cdot k + m && \text{by (M2)} \\ &= k \cdot m + m && \text{since } k \in C \\ &= k^+ \cdot m && \text{by the second result} \end{aligned}$$

Therefore $k^+ \in C$ and $C$ is inductive.

□

## 4.4 Ordering on $\omega$

**Notation 4.30.** *Let $m$ and $n$ be natural numbers. We use the symbol $\subseteqq$ to mean either $\in$ or $=$. We write*

$$m < n \iff m \in n$$
$$m \leq n \iff m \subseteqq n$$

**Remark.** *We observe that $p \in k^+$ if and only if $p \subseteqq k$*

**Definition 4.31.** *We define a binary relation $\in_\omega$ on $\omega$ by*

$$\in_\omega = \{ \langle m, n \rangle \in \omega \times \omega \mid m \in n \}$$

We shall show that $\in_\omega$ is a linear ordering relation. In other words, $\in_\omega$ is a transitive relation that satisfies trichotomy on $\omega$.

**Lemma 4.32.** *$\in_\omega$ is a transitive relation on $\omega$.*

*Proof.* Let $m, n, p$ be natural numbers such that $m \in n$ and $n \in p$. It follows that since each natural number is a transitive set, we must have that $m \in p$. Hence $\in_\omega$ is a transitive relation. □

**Lemma 4.33.**

*Part 1:*

1. *Let $m, n \in \omega$. Then*

$$m \in n \iff m^+ \in n^+$$

*2. No natural number is a member of itself*

*Proof.*

$\Longrightarrow$ : First suppose that $m \in n$. Consider the set

$$T = \{\, n \in \omega \mid (\forall\, m \in n)\, m^+ \in n^+ \,\}$$

We claim that $T$ is inductive. It is vacuously true that $0 \in T$. Now assume that $k \in T$. We must show that $k^+ \in T$. In other words, whenever $m \in k^+$ then $m^+ \in k^{++}$.
Given $m \in k^+$, we have that either $m = k$ - in which case, $m^+ = k^+ \in k^{++}$ - or $m \in k$. In the latter case, we have that $m^+ \in k^+ \subseteq k^{++}$ (since $k \in T$). Hence in either case we have that $m^+ \in k^{++}$ and this $k^+ \in T$. Thus $T$ is inductive and coincides with $\omega$.

$\Longleftarrow$ : Now assume that $m^+ \in n^+$. Then $m \in m^+ \subseteqq n$. Thus, by the transitivity of $n$, we obtain $m \in n$.

Part 2: Consider the set

$$T = \{\, n \in \omega \mid n \notin n \,\}$$

We claim that $T$ is inductive. Obviously, $0 \in T$ since nothing is a member of 0. By Part 1, $k \notin k \implies k^+ \notin k^+$. This $T$ is inductive and coincides with $\omega$.

□

**Lemma 4.34.** *Let $m \in \omega$. Then $0 \subseteqq m$.*

*Proof.* Consider the set

$$T = \{\, n \in \omega \mid 0 \subseteqq n \,\}$$

We claim that $T$ is inductive. Obviously $0 \in T$ as $0 \subseteqq 0$. Now suppose $k \in T$. We have that $0 \subseteqq k \subseteq k^+$. Since $k^+$ is a transitive set, we must have that $0 \in k^+$. Hence $T$ is inductive. □

**Theorem 4.35.** *Trichotomy Law for $\omega$*
*Let $m$ and $n$ be natural numbers. Then exactly one of the following conditions holds*

$$m \in n, \qquad m = n, \qquad n \in m$$

*Proof.* We first note that at most one of the conditions can hold. If $m \in n$ and $m = n$ then $m \in m$ which contradicts Lemma 4.33. Also, if $m \in n \in m$ then, because $m$ is a transitive set, we again have that $m \in m$. It suffices to show that at least one holds. Consider the set

$$T = \{\, n \in \omega \mid (\forall\, m \in \omega)\,(m \in n \vee m = n \vee n \in m \,\}$$

We claim that $T$ is inductive. It follows from the previous lemma that $0 \in T$. Now assume that $k \in T$. We need to show that $k^+ \in T$. Consider $m \in \omega$. We have that either $m \subsetneqq k$ - in which case $m \in k^+$ or $k \in m$. In the latter case, $k^+ \in m^+$ by Lemma 4.33 and so $k^+ \subsetneqq m$. Thus in every case, either $m \in k^+, k^+ = m$ or $k^+ \in m$. Hence $k^+ \in T$ and $T$ is inductive. □

**Definition 4.36.** *Let $A$ and $B$ be sets. We say that $A$ is a **proper** subset of $B$, denoted $A \subset B$, if it is a subset of $B$ that does not coincide with $B$.*

**Corollary 4.37.** *Let $n$ and $m$ be natural numbers. We have that*

$$m \in n \iff m \subset n$$
$$m \subsetneqq n \iff m \subseteq n$$

*Proof.* Since $n$ is a transitive set, we have that $m \in n \implies m \subseteq n$. Lemma 4.33 implies that the inclusion must be proper. Conversely, assume that $m \subset n$. Then $m \neq n$ and $n \notin m$. Hence by trichotomy, $m \in n$ and we are done. □

**Theorem 4.38.** *Let $m, n$ and $p$ be natural numbers. We have that*

$$m \in n \iff m + p \in n + p$$

*If, in addition, $p \neq 0$ then*

$$m \in n \iff m \cdot p \in n \cdot p$$

*Proof.*

Part 1:

$\implies$ : Let $m \in n$ be natural numbers. Consider the set

$$A = \{\, p \in \omega \mid m + p \in n + p \,\}$$

Obviously, $0 \in A$. Let $k \in A$. We must show that $k^+ \in A$. We have that

$$\begin{aligned} k \in A &\implies m + k \in n + k && (4.2) \\ &\implies (m + k)^+ \in (n + k)^+ && \text{by Lemma 4.33} \\ &\implies m + k^+ \in n + k^+ && \text{by (A2)} \\ &\implies k^+ \in A && (4.3) \end{aligned}$$

Hence $A$ is inductive and thus $A = \omega$.

$\Longleftarrow$: Suppose that $m + p \in n + p$ for all $p \in \omega$. Then we cannot have that $m = n$ (else $n + p \in n + p$) nor $n \in m$ (else $n + p \in m + p \in n + p$). The only alternative is that $m \in n$.

Part 2:

$\Longrightarrow$: Let $m \in n$ be natural numbers. Consider the set

$$B = \{\, q \in \omega \mid m \cdot q^+ \in n \cdot q^+ \,\}^{\,2}$$

We claim that $B$ is inductive. We can easily see that $0 \in B$ since $m \cdot 0^+ = m \cdot 0 + m = m$. Now let $k \in B$. We must show that $k^+ \in B$. In other words, we must show that $m \cdot k^{++} \in n \cdot k^{++}$. We have that

$$\begin{aligned} m \cdot k^{++} &= m \cdot k^+ + m \\ &\in n \cdot k^+ + m \end{aligned}$$

where we have applied the first part of the theorem to the fact that $m \cdot k^+ \in n \cdot k^+$. Again applying the first part of the theorem, this time to the fact that $m \in n$, we see that

$$\begin{aligned} n \cdot k^+ + m &\in n \cdot k^+ + n \\ &= n \cdot k^{++} \end{aligned}$$

Therefore $k^+ \in B$ and $B$ is inductive.

Part 2: Now suppose that $m \cdot q^+ \in n \cdot q^+$ for all $q \in \omega$. Then we cannot have that $m = n$ (else $m \cdot q^+ \in m \cdot q^+$) nor can we have that $n \in m$ (else $m \cdot q^+ \in n \cdot q^+ \in m \cdot q^+$). Hence the only other option is that $m \in n$.

□

[2] Recall that for a natural number $p \neq 0$, there exists some $q \in \omega$ with $q^+ = p$

**Corollary 4.39.** *Let $m, n$ and $p$ be natural numbers. Then the following cancellation laws hold:*

$$m + p = n + p \implies m = n$$
$$m \cdot p = n \cdot p \wedge p \neq 0 \implies m = n$$

*Proof.*

Part 1: Suppose that $m + p = n + p$. We cannot have that $m \in n$ (else by the previous theorem we would have that $m + p = n + p \in m + p$) nor can we have that $n \in m$ by similar argumentation. Our only other option is that $m = n$.

Part 2: Suppose that $m \cdot p = n \cdot p$ and that $p$ is non-zero. Then we cannot have that $m \in n$ (else by the previous theorem, we would have that $m \cdot p = n \cdot p \in m \cdot p$) nor can we have that $n \in m$. Hence our only other option is that $m = n$.

□

**Theorem 4.40.** *Well Ordering of $\omega$*
*Let $A \subseteq \omega$ be a non-empty subset of the natural numbers. Then there is some $m \in A$ such that $m \subseteq n$ for all $n \in A$.*

*Proof.* Assume that $A$ is a subset of $\omega$ without a least element. We claim that $A = \varnothing$. To this end, we shall show that the following set is inductive:

$$B = \{\, m \in \omega \mid \text{ no number less than } m \text{ belongs to } A \,\}$$

It is vacuously true that $0 \in B$. Now suppose that $k \in B$. Suppose that $n$ is less than $k^+$. Then either $n$ is less than $k$ - in which case, $n \notin A$ as $k \in B$) - or $n = k$ - in which case, $n \notin A$ lest by trichotomy it be least in $A$. In both cases, $n$ is outside of $A$. Hence $k^+ \in B$ and $B$ is inductive. It clearly follows that $A = \varnothing$. □

**Corollary 4.41.** *There does not exist a function $f : \omega \to \omega$ such that $f(n^+) \in f(n)$ for every natural number $n$.*

*Proof.* If such a function were to exist, *ran* $f$ would be a non-empty subset of $\omega$ without a least element, contradicting the well ordering of $\omega$. □

**Theorem 4.42.** *Strong Induction Principle for $\omega$*
*Let $A$ be a subset of $\omega$ and assume that for every $n \in \omega$*

$$\textit{if every numbers less than } n \textit{ is in } A, \textit{ then } n \in A$$

*Then $A = \omega$*

*Proof.* Suppose that $A \neq \omega$. Then $\omega \backslash A \neq \varnothing$. By well ordering, it has a least number, say $m$. Since $m$ is least in $\omega \backslash A$, all numbers less than $m$ are in $A$. But by hypothesis, $m \in A$ which contradicts the fact that $m \in \omega \backslash A$. □

**Remark.** *The well ordering principle provides an alternative to proof by induction. When showing something is true for every natural number, instead of forming the set of numbers for which the statement is true, we can form the set for which the statement is false. We can then show that such a set has no least element meaning that it must be the empty set.*

# Chapter 5

# Construction of the Real Numbers

## 5.1 Integers

**Definition 5.1.** *Define* $\sim$ *to be the relation on* $\omega \times \omega$ *for which*

$$\langle m, n\rangle \sim \langle p, q\rangle \iff m + q = p + n$$

*Explicitly, we have that*

$$\sim = \{\, \langle \langle m, n\rangle, \langle p, q\rangle \rangle \mid m + q = p + n \,\}$$

**Theorem 5.2.** *The relation* $\sim$ *is an equivalence relation on* $\omega \times \omega$*.*

*Proof.* We must first show that $\sim$ is reflexive on $\omega \times \omega$. Consider $\langle m, n\rangle$ where $m$ and $n$ are natural numbers. Obviously by the commutativity of addition, $m + n = n + m$ and thus $\langle m, n\rangle \sim \langle m, n\rangle$. Hence $\sim$ is reflexive.
We must now show that $\sim$ is symmetric. Let $\langle m, n\rangle$ and $\langle p, q\rangle$ be such that $\langle m, n\rangle \sim \langle p, q\rangle$. We must show that $\langle p, q\rangle \sim \langle m, n\rangle$. By assumption, we have that $m + q = p + n$. It is obviously the case that $p + n = m + q$ and thus $\langle p, q\rangle \sim \langle m, n\rangle$. Therefore, $\sim$ is symmetric.
It now suffices to show that $\sim$ is transitive. Suppose that $\langle m, n\rangle \sim \langle p, q\rangle$ and $\langle p, q\rangle \sim \langle r, s\rangle$. Then by the definition of the relation, we have that $m+q = n+p$ and $p+s = r+q$. Adding these two equations together, we see that $m + q + p + s = n + p + r + q$. Now, by the cancellation law, we obtain that $m + s = r + n$ which implies that $\langle m, n\rangle \sim \langle r, s\rangle$. Thus $\sim$ is transitive whence it follows that it is also an equivalence relation. □

**Definition 5.3.** *We define the set* $\mathbb{Z} = (\omega \times \omega)/\sim$ *as the* ***integers****.*

**Example 5.4.** *The integer* $2_{\mathbb{Z}}$ *is the equivalence class*

$$[\langle 2, 0\rangle] = \{\, \langle 2, 0\rangle, \langle 3, 1\rangle, \langle 4, 2\rangle, \dots \}$$

*The integer* $-3_{\mathbb{Z}}$ *is the equivalence class*

$$[\langle 0, 3\rangle] = \{\, \langle 0, 3\rangle, \langle 1, 4\rangle, \langle 2, 5\rangle \}$$

**Lemma 5.5.** *Let* $m, n, m', n', p, q, p', q'$ *all be natural numbers. Assume that* $\langle m, n\rangle \sim \langle m', n'\rangle$ *and* $\langle p, q\rangle \sim \langle p', q'\rangle$*. Then*

$$\langle m + p, n + q\rangle \sim \langle m' + p', n' + q'\rangle$$

*Proof.* The proof follows directly from the definition of $\sim$ and then adding the two resulting equations. □

**Definition 5.6.** *Let* $a$ *and* $b$ *be integers. Then we define their addition* $a +_{\mathbb{Z}} b$ *to be*

$$a +_{\mathbb{Z}} b = [\langle m + p, n + q\rangle]$$

*where* $\langle m, n\rangle$ *is chosen from* $a$ *and* $\langle p, q\rangle$ *is chosen from* $b$*.*

**Example 5.7.** $2_{\mathbb{Z}} +_{\mathbb{Z}} (-3_{\mathbb{Z}}) = -1_{\mathbb{Z}}$*. We have that*

$$\begin{aligned} 2_{\mathbb{Z}} +_{\mathbb{Z}} (-3_{\mathbb{Z}}) &= [\langle 2, 0\rangle] +_{\mathbb{Z}} [\langle 0, 3\rangle] \\ &= [\langle 2 + 0, 0 + 3\rangle] \\ &= [\langle 2, 3\rangle] \\ &= -1_{\mathbb{Z}} \end{aligned}$$

**Theorem 5.8.** *The operation* $+_{\mathbb{Z}}$ *is commutative and associative. In other words, given any* $a, b \in \mathbb{Z}$*, we have that*

$$\begin{aligned} a +_{\mathbb{Z}} b &= b +_{\mathbb{Z}} a \\ (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c &= a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c) \end{aligned}$$

*Proof.* Let $a$ be of the form $[\langle m, n\rangle]$ for some natural numbers $m$ and $n$. Similarly, $b$ is of the form $[\langle p, q\rangle]$ and $c$ is of the form $[\langle r, s\rangle]$.

Part 1:

$$\begin{aligned} a +_{\mathbb{Z}} b &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle p, q\rangle] \\ &= [\langle m + p, n + q\rangle] && \text{by definition of } +_{\mathbb{Z}} \\ &= [\langle p + m, q + n\rangle] && \text{by commutativity of } + \text{ on } \omega \\ &= [\langle p, q\rangle] +_{\mathbb{Z}} [\langle m, n\rangle] \\ &= b +_{\mathbb{Z}} a \end{aligned}$$

Part 2:

$$\begin{aligned} (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c &= ([\langle m, n\rangle] +_{\mathbb{Z}} [\langle p, q\rangle]) +_{\mathbb{Z}} [\langle r, s\rangle] \\ &= ([\langle m + p, n + q\rangle]) +_{\mathbb{Z}} [\langle r, s\rangle] && \text{by the definition of } +_{\mathbb{Z}} \\ &= [\langle (m + p) + r, (n + q) + s\rangle] && \text{by the definition of } +_{\mathbb{Z}} \\ &= [\langle m + (p + r), n + (q + s)\rangle] && \text{by associativity of } + \text{ on } \omega \\ &= [\langle m, n\rangle] +_{\mathbb{Z}} ([\langle p + r, q + s\rangle]) \\ &= [\langle m, n\rangle] +_{\mathbb{Z}} ([\langle p, q\rangle] +_{\mathbb{Z}} [\langle r, s\rangle]) \\ &= a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c) \end{aligned}$$

□

**Theorem 5.9.**

1. *$0_{\mathbb{Z}}$ is an identity element for $+_{\mathbb{Z}}$:*

$$a +_{\mathbb{Z}} 0_{\mathbb{Z}} = a$$

   *for all $a \in \mathbb{Z}$.*

2. *For any integer $a$, there exists a unique integer (called an **inverse** and denoted $-a$) $b$ such that*

$$a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$$

*Proof.*

Part 1: Suppose that $a = [\langle m, n\rangle]$ where $m$ and $n$ are some natural numbers.

$$\begin{aligned} a +_{\mathbb{Z}} 0_{\mathbb{Z}} &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle 0, 0\rangle] \\ &= [\langle m + 0, n + 0\rangle] && \text{by the definition of } +_{\mathbb{Z}} \\ &= [\langle m, n\rangle] && \text{by (A1)} \\ &= a \end{aligned}$$

Part 2: Given an integer $a$, it must be of the form $[\langle m, n\rangle]$ where $m$ and $n$ are some natural numbers. Take $b = [\langle n, m\rangle]$. Then

$$\begin{aligned} a +_{\mathbb{Z}} b &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle n, m\rangle] \\ &= [\langle m + n, n + m\rangle] && \text{by the definition of } +_{\mathbb{Z}} \\ &= [\langle m + n, m + n\rangle] && \text{by the commutativity of } + \text{ on } \omega \\ &= [\langle 0, 0\rangle] \\ &= 0_{\mathbb{Z}} \end{aligned}$$

To show that additive inverses are unique, suppose that $b$ and $b'$ are both additive inverses of $a$. Then we have that $b = b+_{\mathbb{Z}}(a+_{\mathbb{Z}}b') = (b+_{\mathbb{Z}}a)+_{\mathbb{Z}}b' = b'$ where we have used the associativity of $+_{\mathbb{Z}}$.

□

**Remark.** *The two previous theorems show that $\mathbb{Z}$ with the operation $+_{\mathbb{Z}}$ and the identity element $0_{\mathbb{Z}}$ form an* ***Abelian group***

**Definition 5.10.** *Let $a$ and $b$ be two integers. We define the operation of* ***subtraction*** *(denoted -) on $a$ and $b$ by the following:*

$$b - a = b +_{\mathbb{Z}} (-a)$$

**Lemma 5.11.** *Let $m, n, m', n', p, q, p', q'$ all be natural numbers. Assume that $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$. Then*

$$\langle mp + nq, mq + np\rangle \sim \langle m'p' + n'q', m'q' + n'p'\rangle$$

*Proof.* By the definition of $\sim$, we have the following two equations:

$$m + n' = m' + n \tag{5.1}$$
$$p + q' = p' + q \tag{5.2}$$

We first multiply Equation (5.1) by $p$ which gives us

$$mp + n'p = m'p + np \tag{5.3}$$

Next we multiply the reverse of Equation (5.1) by $q$ which gives us

$$m'q + nq = mq + n'q \tag{5.4}$$

We now multiply Equation (5.2) by $m'$ giving us

$$pm' + q'm' = p'm' + qm' \tag{5.5}$$

Finally we multiply the reverse of Equation (5.2) by $n'$ which gives us

$$p'n' + qn' = pn' + q'n' \tag{5.6}$$

Adding up these four equations, we have

$$\begin{aligned} mp + n'p + m'q + nq + pm' + q'm' + p'n' + qn' =& m'p + np + mq \\ &+ n'q + p'm' + qm' + pn' + q'n' \end{aligned}$$

We can now apply the cancellation law (and the commutativity of addition on the natural numbers) to this equation to arrive at

$$mp + nq + m'q' + n'p' = m'p' + n'q' + mq + np$$

Now applying the definition of $\sim$, we arrive at the conclusion of the lemma. □

**Definition 5.12.** *Let $a$ and $b$ be two integers. We define their multiplication $\cdot_{\mathbb{Z}}$ to be*

$$a \cdot_{\mathbb{Z}} b = [\langle mp + nq, mq + np \rangle]$$

*where $\langle m, n \rangle$ is chosen from $a$ and $\langle p, q \rangle$ is chosen from $b$.*

**Theorem 5.13.** *Let $a, b$ and $c$ be integers. Then the following properties hold:*

1. *Commutatvity of $\cdot_{\mathbb{Z}}$:*

$$a \cdot_{\mathbb{Z}} b = b \cdot_{\mathbb{Z}} a$$

2. *Associativity of* $\cdot_{\mathbb{Z}}$*:*

$$(a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c = a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c)$$

3. *Distributivity of* $\cdot_{\mathbb{Z}}$ *over* $+_{\mathbb{Z}}$*:*

$$a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) = (a \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} c)$$

*Proof.* Assume that $a = [\langle m, n\rangle], b = [\langle p, q\rangle]$ and $c = [\langle r, s\rangle]$.

Part 1:

$$\begin{aligned}
a \cdot_{\mathbb{Z}} b &= [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] \\
&= [\langle mp + nq, mq + np\rangle] && \text{by the definition of } \cdot_{\mathbb{Z}} \\
&= [\langle pm + qn, qm + pn\rangle] && \text{by the commutativity of } \cdot \text{ over } \omega \\
&= [\langle pm + qn, pn + qm\rangle] && \text{by the commutativity of } + \text{ over } \omega \\
&= [\langle p, q\rangle] \cdot_{\mathbb{Z}} [\langle m, n\rangle] && \text{by the definition of } \cdot_{\mathbb{Z}} \\
&= b \cdot_{\mathbb{Z}} a && (5.7)
\end{aligned}$$

Part 2:

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

Part 3:

$$\begin{aligned}
a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) &= [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p + r, q + s\rangle] \\
&= [\langle m(p + r) + n(q + s), m(q + s) + n(p + r)\rangle] \\
&= [\langle mp + mr + nq + ns, mq + ms + np + nr\rangle] \\
&= [\langle (mp + nq) + (mr + ns), (mq + np) + (ms + nr)\rangle] \\
&= [\langle mp + nq, mq + np\rangle] +_{\mathbb{Z}} [\langle mr + ns, ms + nr\rangle] \\
&= ([\langle m, n]\rangle \cdot_{\mathbb{Z}} [\langle p, q\rangle]) +_{\mathbb{Z}} ([\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle r, s\rangle]) \\
&= a \cdot_{\mathbb{Z}} b +_{\mathbb{Z}} a \cdot_{\mathbb{Z}} c
\end{aligned}$$

□

**Theorem 5.14.** *Let $a$ and $b$ be integers.*

1. *The integer $1_{\mathbb{Z}}$ is a multiplicative identity element:*

$$a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$$

2. $0_{\mathbb{Z}}/neq1_{\mathbb{Z}}$

3. *If $a \cdot_{\mathbb{Z}} b = 0_{\mathbb{Z}}$ then either $a = 0_{\mathbb{Z}}$ or $b = 0_{\mathbb{Z}}$*

*Proof.* Let $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$.

Part 1:

$$\begin{aligned} a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} &= [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle 1, 0\rangle] \\ &= [\langle m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1\rangle] \\ &= [\langle m, n\rangle] \\ &= a \end{aligned}$$

Part 2: Obviously, $0 \neq 1$ in $\omega$ and thus $\langle 0, 0\rangle \not\sim \langle 1, 0\rangle$.

Part 3: Assume that $a \neq 0_{\mathbb{Z}}$ and $b \neq 0_{\mathbb{Z}}$. It suffices to show that $a \cdot_{\mathbb{Z}} b \neq 0_{\mathbb{Z}}$. We have that $a \cdot_{\mathbb{Z}} b = [\langle mp + nq, mq + np\rangle]$. Now since $a \neq [\langle 0, 0\rangle]$, we must have that $m \neq n$ and thus, by trichotomy, either $m \in n$ or $n \in m$. Similarly, either $p \in q$ or $q \in p$. It thus follows, again by trichotomy, that we cannot have that $mp + nq = mq + np$. Thus $a \cdot_{\mathbb{Z}} b \neq 0_{\mathbb{Z}}$.

□

**Lemma 5.15.** *Let $m, n, m', n', p, q, p', q'$ all be natural numbers. Assume that $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$. Then*

$$m + q \in p + n \iff m' + q' \in p' + n'$$

*Proof.* By assumption, we have the following two equations:

$$\begin{aligned} m + n' &= m' + n \\ p + q' &= p' + q \end{aligned}$$

We then have

$$\begin{aligned} m+q \in p+n &\iff m+q+n'+q' \in p+n+n'+q' \\ &\qquad\qquad \text{by the cancellation law} \\ &\iff m'+n+q+q' \in p'+q+n+n' \\ &\qquad\qquad \text{by the two equations above} \\ &\iff m'+q' \in p'+n' \qquad \text{by the cancellation law} \end{aligned}$$

□

**Definition 5.16.** *Let $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$ be integers (where $m, n, p$ and $q$ are natural numbers). We define an ordering relation $<_{\mathbb{Z}}$ by the following:*

$$a <_{\mathbb{Z}} b \iff m+q \in p+n$$

**Theorem 5.17.** *The relation $<_{\mathbb{Z}}$ is a linear ordering on the set of integers.*

*Proof.* We must first show that $<_{\mathbb{Z}}$ is a transitive relation on $\mathbb{Z}$. Let $a = [\langle m, n\rangle], b = [\langle p, q\rangle]$ and $c = [\langle r, s\rangle]$ be integers. Then

$$\begin{aligned} a <_{\mathbb{Z}} b \wedge b <_{\mathbb{Z}} c &\implies m+q \in p+n \wedge p+s \in r+q \\ &\implies m+q+s \in p+n+s \wedge p+s+n \in r+q+n \\ &\implies m+q+s \in r+q+n \\ &\implies m+s \in r+n \\ &\implies a <_{\mathbb{Z}} c \end{aligned}$$

We must now show that $<_{\mathbb{Z}}$ satisfies trichotomy on $\mathbb{Z}$. To say that exactly one of the following holds:

$$a <_{\mathbb{Z}} b, \qquad a = b, \qquad b <_{\mathbb{Z}} a$$

is the same as saying that exactly one of the following holds:

$$m+q \in p+n, \qquad m+q = p+n, \qquad p+n \in m+q$$

This follows directly from trichotomy of ¡ on $\omega$. □

**Definition 5.18.** *An integer $b$ is called **positive** if $0_{\mathbb{Z}} <_{\mathbb{Z}} b$.*

**Remark.** *It is easy to see that*

$$b <_{\mathbb{Z}} 0_{\mathbb{Z}} \iff 0_{\mathbb{Z}} <_{\mathbb{Z}} -b$$

*Hence a consequence of trichotomy is that exactly one of the three following alternatives holds:*

$$b \text{ is positive}, \qquad b \text{ is zero}, \qquad -b \text{ is positive}$$

**Theorem 5.19.** *Let $a = [\langle m, n\rangle], b = [\langle p, q\rangle]$ and $c = [\langle r, s\rangle]$ be integers.*

1. $a <_{\mathbb{Z}} b \iff a +_{\mathbb{Z}} c <_{\mathbb{Z}} b +_{\mathbb{Z}} c$
2. *If $0_{\mathbb{Z}} <_{\mathbb{Z}} c$ then*

$$a <_{\mathbb{Z}} b \iff a \cdot_{\mathbb{Z}} c <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c$$

*Proof.*

Part 1: By definition of $<_{\mathbb{Z}}$ we want to show that

$$m + q \in p + n \iff m + r + q + s \in p + r + n + s$$

But this follows directly from the cancellation law for natural numbers.

Part 2: The proof is left as an exercise to the reader.

□

**Corollary 5.20.** *Let $a, b$ and $c$ be integers. Then the cancellation law holds:*

$$a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c \implies a = b$$
$$a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c \wedge c \neq 0_{\mathbb{Z}} \implies a = b$$

*Proof.* This corollary follows immediately from the previous theorem and the same argumentation between Theorem 4.38 and Corollary 4.39. □

**Theorem 5.21.** *Consider the function $E : \omega \to \mathbb{Z}$ given by*

$$E(n) = [\langle n, 0\rangle]$$

*Then $E$ is an injective mapping between $\omega$ and $\mathbb{Z}$ and, given any $n, m \in \omega$, satisfies the following properties:*

1. $E(m+n) = E(m) +_{\mathbb{Z}} E(n)$
2. $E(mn) = E(m) \cdot_{\mathbb{Z}} E(n)$
3. $m \in n \iff E(m) <_{\mathbb{Z}} E(n)$

*Proof.* We first show that $E$ is injective. We have that

$$\begin{aligned} E(m) = E(n) &\iff [\langle m, 0\rangle] = [\langle n, 0\rangle] \\ &\iff \langle m, 0\rangle \sim \langle n, 0\rangle \\ &\iff m + 0 = n + 0 \\ &\iff m = n \end{aligned}$$

Part 1:

$$\begin{aligned} E(m+n) &= [\langle m+n, 0\rangle] \\ &= [\langle m, 0\rangle] + [\langle n, 0\rangle] \\ &= E(m) + E(n) \end{aligned}$$

Part 2:

$$\begin{aligned} E(mn) &= [\langle mn, 0\rangle] \\ &= [\langle m, 0\rangle] \cdot_{\mathbb{Z}} [\langle n, 0\rangle] \\ &= E(m) \cdot_{\mathbb{Z}} E(n) \end{aligned}$$

Part 3:

$$\begin{aligned} m \in n &\iff m + 0 \in n + 0 \\ &\iff [\langle m, 0\rangle] <_{\mathbb{Z}} [\langle n, 0\rangle] \\ &\iff E(m) <_{\mathbb{Z}} E(n) \end{aligned}$$

□

**Remark.** *From now on, we shall streamline our notation by omitting the $\mathbb{Z}$ subscript on $+_{\mathbb{Z}}, \cdot_{\mathbb{Z}}$ etc.*

## 5.2 Rational Numbers

**Definition 5.22.** *Let $a$ and $b$ be integers with $b$ non-zero. We say that the ordered pair $\langle a, b\rangle$ is a **fraction**. The first component is the **numerator** and the second component is the **denominator**. Let $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$. Then $\mathbb{Z} \times \mathbb{Z}'$ is the set of all fractions.*

**Definition 5.23.** *We define $\sim$ to be the binary relation on $\mathbb{Z} \times \mathbb{Z}'$ satisfying the following:*

$$\langle a, b\rangle \sim \langle c, d\rangle \iff a \cdot d = c \cdot b$$

*where $a, b, c$ and $d$ are integers.*

**Theorem 5.24.** *The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$.*

*Proof.* We first show that $\sim$ is reflexive on $\mathbb{Z} \times \mathbb{Z}'$. Let $x = \langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}'$. We must show that $x \sim x$. Indeed, $a \cdot b = b \cdot a$ by commutativity of the multiplication of integers. Thus $\sim$ is reflexive on $\mathbb{Z} \times \mathbb{Z}'$.
We must now show that $\sim$ is symmetric. Let $x = \langle a, b\rangle$ and $y = \langle c, d\rangle$. We must show that $x \sim y \iff y \sim x$. We have that

$$\begin{aligned} \langle a, b\rangle \sim \langle c, d\rangle &\iff a \cdot d = c \cdot b \\ &\iff c \cdot b = a \cdot d \\ &\iff \langle c, d\rangle \sim \langle a, b\rangle \end{aligned}$$

Finally, we show that $\sim$ is transitive. Let $x = \langle a, b\rangle, y = \langle c, d\rangle$ and $z = \langle e, f\rangle$. We must show that if $x \sim y$ and $y \sim z$ then $x \sim z$. We have that

$$\begin{aligned} (\langle a, b\rangle \sim \langle c, d\rangle) \wedge (\langle c, d\rangle \sim \langle e, f\rangle) &\iff (ad = cb) \wedge (cf = ed) \\ &\iff (adf = cbf) \wedge (cfb = edb) \\ &\iff (adf = cfb) \wedge (cfb = edb) \\ &\iff adf = edb \\ &\iff af = eb \\ &\iff \langle a, b\rangle \sim \langle e, f\rangle \end{aligned}$$

□

**Remark.** *Knowing that $\sim$ is indeed an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$, we now define the **rational numbers** $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}')/\sim$ to be the set of equivalence classes of fractions.*

**Lemma 5.25.** *Let $a, b, a', b', c, d, c', d'$ all be integers. Assume that $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$. Then*

$$\langle ad + cb, bd\rangle \sim \langle a'd' + c'b', b'd'\rangle$$

*Proof.* By the definition of $\sim$, we have the following two equations:

$$ab' = a'b$$
$$cd' = c'd$$

Multiplying the first equation by $dd'$ we get

$$ab'dd' = a'bdd'$$

Now multiplying the second equation by bb' we get

$$cd'bb' = c'dbb'$$

Adding these two equations we get

$$ab'dd' + cd'bb' = a'bdd' + c'dbb'$$

Now using the commutativity and distributivity laws of multiplication of integers, we have

$$(ad + cb)b'd' = (a'd' + c'b')bd$$

And by the definition of $\sim$, we arrive at

$$\langle ad + cb, bd\rangle \sim \langle a'd' + c'b', b'd'\rangle$$

□

**Definition 5.26.** *Let $[\langle a, b\rangle]$ and $[\langle c, d\rangle]$ be two rational numbers (where $a, b, c$ and $d$ are integers). Then we define their* ***addition*** *$[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle]$ by the following:*

$$[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ad + cb, bd\rangle]$$

**Example 5.27.** *We shall check $2 + 2 = 4$ in $\mathbb{Q}$. Let $2_{\mathbb{Q}} = [\langle 2, 1\rangle]$ and $4_{\mathbb{Q}} = [\langle 4, 1\rangle]$. Then we have that*

$$\begin{aligned} 2_{\mathbb{Q}} +_{\mathbb{Q}} 2_{\mathbb{Q}} &= [\langle 2, 1\rangle] +_{\mathbb{Q}} +[\langle 2, 1\rangle] \\ &= [\langle 2 + 2, 1\rangle] \\ &= [\langle 4, 1\rangle] \\ &= 4_{\mathbb{Q}} \end{aligned}$$

**Theorem 5.28.** *Let $q = [\langle a, b\rangle], r = [\langle c, d\rangle]$ and $s = [\langle e, f\rangle]$ be rational numbers. Then the following properties hold:*

1. *Associativity of $+_{\mathbb{Q}}$:*

$$(q +_{\mathbb{Q}} r) +_{\mathbb{Q}} s = q +_{\mathbb{Q}} (r +_{\mathbb{Q}} s)$$

2. *Commutativity of $+_{\mathbb{Q}}$:*

$$r +_{\mathbb{Q}} s = s +_{\mathbb{Q}} r$$

3. *There exists an additive identity $0_{\mathbb{Q}}$:*

$$r +_{\mathbb{Q}} 0_{\mathbb{Q}} = r$$

4. *For any $r \in \mathbb{Q}$, there exists an inverse $s \in \mathbb{Q}$ (denoted -r) such that $r +_{\mathbb{Q}} s = 0_{\mathbb{Q}}$*

*Proof.*

Part 1:

$$\begin{aligned}
(q +_{\mathbb{Q}} r) +_{\mathbb{Q}} s &= ([\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle]) +_{\mathbb{Q}} [\langle e, f\rangle] \\
&= [\langle ad + cb, bd\rangle] +_{\mathbb{Q}} [\langle e, f\rangle] \\
&= [\langle (ad + cb)f + ebd, bdf\rangle] \\
&= [\langle adf + cbf + ebd, bdf\rangle] \\
&= [\langle adf + b(cf + ed), bdf\rangle] \\
&= [\langle a, b\rangle] +_{\mathbb{Q}} [\langle cf + ed, df\rangle] \\
&= [\langle a, b\rangle] +_{\mathbb{Q}} ([\langle c, d\rangle] +_{\mathbb{Q}} [\langle e, f\rangle])
\end{aligned}$$

Part 2:

$$\begin{aligned}
r +_{\mathbb{Q}} s &= [\langle c, d\rangle] +_{\mathbb{Q}} [\langle e, f\rangle] \\
&= [\langle cf + ed, df\rangle] \\
&= [\langle ed + cf, fd\rangle] \\
&= [\langle e, f\rangle] + [\langle c, d\rangle]
\end{aligned}$$

Part 3:

$$\begin{aligned} r +_{\mathbb{Q}} 0_{\mathbb{Q}} &= [\langle c, d\rangle] +_{\mathbb{Q}} [\langle 0, 1\rangle] \\ &= [\langle c \cdot 1 + 0 \cdot d, d \cdot 1\rangle] \\ &= [\langle c, d\rangle] \\ &= r \end{aligned}$$

Part 4: Given $r = [\langle c, d\rangle]$, take $s = [\langle -c, d\rangle]$. Then we have that

$$\begin{aligned} r +_{\mathbb{Q}} s &= [\langle c, d\rangle] +_{\mathbb{Q}} [\langle -c, d\rangle] \\ &= [\langle cd - cd, dd\rangle] \\ &= [\langle 0, dd\rangle] \\ &= 0_{\mathbb{Q}} \end{aligned}$$

□

**Lemma 5.29.** *Let $a, b, a'b, b', c, d, c', d'$ be integers. Assume that $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$. Then*

$$\langle ac, bd\rangle \sim \langle a'c', b'd'\rangle$$

*Proof.* The proof follows the same argumentation as Lemma 5.25. □

**Definition 5.30.** *Let $[\langle a, b\rangle]$ and $[\langle c, d\rangle]$ be two rational numbers (where $a, b, c$ and $d$ are integers). Then we define their **multiplication** $[\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle c, d\rangle]$ by the following:*

$$[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ac, bd\rangle]$$

**Theorem 5.31.** *Let $p = [\langle a, b\rangle], q = [\langle c, d\rangle]$ and $r = [\langle e, f\rangle]$ be rational numbers. Then the following properties hold:*

1. *Associativity of $\cdot_{\mathbb{Q}}$:*

$$(p \cdot_{\mathbb{Q}} q) \cdot_{\mathbb{Q}} r = p \cdot_{\mathbb{Q}} (q \cdot_{\mathbb{Q}} r)$$

2. *Commutativity of $\cdot_{\mathbb{Q}}$:*

$$q \cdot_{\mathbb{Q}} r = r \cdot_{\mathbb{Q}} q$$

*3. Distributivity of $\cdot_{\mathbb{Q}}$ over $+_{\mathbb{Q}}$:*

$$p \cdot_{\mathbb{Q}} (q +_{\mathbb{Q}} r) = (p \cdot_{\mathbb{Q}} q) +_{\mathbb{Q}} (p \cdot_{\mathbb{Q}} r)$$

*Proof.* The proofs of Part 1 and Part 2 follow the same argumentation as the proofs for the same properties for $+_{\mathbb{Q}}$.

Part 3:

$$\begin{aligned} p \cdot_{\mathbb{Q}} (q +_{\mathbb{Q}} r) &= [\langle a, b\rangle] \cdot_{\mathbb{Q}} ([\langle c, d\rangle] + [\langle e, f\rangle] \\ &= [\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle cf + ed, df\rangle] \\ &= [\langle a(cf + ed), bdf\rangle] \\ &= [\langle bacf + baed, bbdf\rangle] \\ &= [\langle acbf + aebd, bdbf\rangle] \\ &= [\langle ac, bd\rangle] +_{\mathbb{Q}} [\langle ae, bf\rangle] \\ &= [\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle c, d\rangle] +_{\mathbb{Q}} [\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle e, f\rangle] \end{aligned}$$

where we have used the fact that $\langle i, j\rangle \sim \langle bi, bj\rangle$.

□

**Theorem 5.32.** *Let $r \in \mathbb{Q}$ be non-zero. Then there exists a non-zero $q \in \mathbb{Q}$ (called the **multiplicative inverse** of $r$ and denoted $r^{-1}$) such that $r \cdot_{\mathbb{Q}} q = 1_{\mathbb{Q}}$.*

*Proof.* Given an $r \in \mathbb{Q}$ of the form $r = [\langle a, b\rangle]$ (where $a$ is a non-zero integer), take $q = [\langle b, a\rangle]$. Then obviously, $q \neq 0_{\mathbb{Q}}$ and $r \cdot_{\mathbb{Q}} q = [\langle ab, ab\rangle] = 1_{\mathbb{Q}}$. □

**Corollary 5.33.** *Let $r$ and $s$ be non-zero rational numbers. Then $r \cdot_{\mathbb{Q}} q$ is also non-zero.*

*Proof.* Assume that $r \cdot_{\mathbb{Q}} q = 0_{\mathbb{Q}}$. The previous theorem provides guarantees the existence of rational numbers $r^{-1}$ and $s^{-1}$ such that $r \cdot_{\mathbb{Q}} r^{-1} = 1_{\mathbb{Q}}$ and $s \cdot_{\mathbb{Q}} s^{-1} = 1_{\mathbb{Q}}$. Therefore, by the laws of commutativity and associativity of multiplication of rational numbers, we have that

$$\begin{aligned} 1_{\mathbb{Q}} &= (r \cdot_{\mathbb{Q}} s) \cdot_{\mathbb{Q}} (r^{-1} \cdot_{\mathbb{Q}} s^{-1}) \\ &= 0_{\mathbb{Q}} \cdot_{\mathbb{Q}} (r^{-1} \cdot_{\mathbb{Q}} s^{-1}) \\ &= 0_{\mathbb{Q}} \end{aligned}$$

which is a contradiction as the multiplicative and additive identities must be distinct. □

**Definition 5.34.** *Given any two rational numbers $s$ and $r$, we define the operation of* ***division*** $\div$ *as follows:*

$$r \div s = r \cdot_{\mathbb{Q}} s^{-1}$$

**Definition 5.35.** *Let $p = [\langle a, b\rangle]$ and $q = [\langle c, d\rangle]$ be rational numbers (where $a, b, c$ and $d$ are integers). We define the ordering relation $<_{\mathbb{Q}}$ by the following:*

$$p <_{\mathbb{Q}} q \iff ad < cb$$

*where $a, b, c$ and $d$ are chosen such that the denominators $b$ and $d$ are positive.*

**Remark.** *The reason for the above definition is motivated by the following intuition:*

$$\frac{a}{b} < \frac{c}{d} \iff ad < cb$$

*However this is only true if both $b$ and $d$ are positive. However, in the context of set theory, we have that $[\langle a, b\rangle] = \langle -a, -b\rangle$ and thus we can always choose representative rational numbers whose denominators are positive.*

**Lemma 5.36.** *Let $a, b, a', b', c, d, c', d'$ all be integers. Assume that $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$. Furthermore, assume that $b, b', d, d'$ are all positive. Then*

$$ad < cb \iff a'd' < c'b'$$

*Proof.* The proof follows the same reasoning as the one for Lemma 5.15. □

**Remark.** *The previous lemma guarantees that when we test whether or not $r <_{\mathbb{Q}} s$, it does not matter which fractions with positive denominators we choose from $r$ and $s$.*

**Theorem 5.37.** *The relation $<_{\mathbb{Q}}$ is a linear ordering on $\mathbb{Q}$.*

*Proof.* We first show that $<_{\mathbb{Q}}$ is a transitive relation. Let $p = [\langle a, b\rangle], q = [\langle c, d\rangle]$ and $r = [\langle e, f\rangle]$ be rational numbers (with $b, d$ and $f$ all positive).

Suppose that $p <_{\mathbb{Q}} q$ and $q <_{\mathbb{Q}} r$. We need to show that $p <_{\mathbb{Q}} r$. We have that

$$\begin{aligned}
(p <_{\mathbb{Q}} q) \wedge (q <_{\mathbb{Q}} r) &\iff ([\langle a, b\rangle] <_{\mathbb{Q}} [\langle c, d\rangle]) \wedge ([\langle c, d\rangle] <_{\mathbb{Q}} [\langle e, f\rangle]) \\
&\iff (ad < cb) \wedge (cf < ed) \\
&\iff (fad < fcb) \wedge (bcf < bed) \\
&\iff (afd < bcf) \wedge (bcf < ebd) \\
&\iff afd < ebd \\
&\iff af < eb \\
&\iff [\langle a, b\rangle] <_{\mathbb{Q}} [\langle e, f\rangle] \\
&\iff p <_{\mathbb{Q}} r
\end{aligned}$$

we must now show that $<_{\mathbb{Q}}$ satisfies trichotomy on $\mathbb{Q}$. Consider the rational numbers $p = [\langle a, b\rangle]$ and $q = [\langle c, d\rangle]$ (with $b$ and $d$ positive integers). Then trichotomy on $\mathbb{Z}$ implies that exactly one of the following holds:

$$ad < cb, \qquad ad = cb, \qquad cb < ad$$

But this is equivalent to exactly one of the following holding:

$$p <_{\mathbb{Q}} r, \qquad p = r, r <_{\mathbb{Q}} p$$

□

**Definition 5.38.** *Let $q$ be a rational number. We say that $q$ is **positive** if $0_{\mathbb{Q}} <_{\mathbb{Q}} q$.*

**Remark.** *It is easy to see that $r <_{\mathbb{Q}} 0_{\mathbb{Q}} \iff 0_{\mathbb{Q}} <_{\mathbb{Q}} -r$. Thus, as a consequence of trichotomy, we have that exactly one of the three alternatives holds:*

$$r \text{ is positive}, \qquad r \text{ is zero}, \qquad -r \text{ is positive}$$

**Theorem 5.39.** *Let $r, s$ and $t$ be rational numbers. Then*

1. *$r <_{\mathbb{Q}} s \iff r +_{\mathbb{Q}} t <_{\mathbb{Q}} s +_{\mathbb{Q}} t$*
2. *If $t$ is positive then*

$$r <_{\mathbb{Q}} s \iff r \cdot_{\mathbb{Q}} t <_{\mathbb{Q}} s \cdot_{\mathbb{Q}} t$$

*Proof.* Assume that $r = [\langle a, b\rangle], s = [\langle c, d\rangle]$ and $t = [\langle e, f\rangle]$ where $b, d$ and $f$ are all positive integers.

Part 1:

$$\begin{aligned}
r +_{\mathbb{Q}} t <_{\mathbb{Q}} s +_{\mathbb{Q}} t &\iff [\langle a, b\rangle] +_{\mathbb{Q}} [\langle e, f\rangle] <_{\mathbb{Q}} [\langle c, d\rangle] +_{\mathbb{Q}} [\langle e, f\rangle] \\
&\iff [\langle af + eb, bf\rangle] <_{\mathbb{Q}} [\langle cf + ed, df\rangle] \\
&\iff (af + eb)df < (cf + ed)bf \\
&\iff afdf + ebdf < cfbf + edbf \\
&\iff adff < cbff \\
&\iff ad < cb \\
&\iff [\langle a, b\rangle] <_{\mathbb{Q}} [\langle c, d\rangle] \\
&\iff r <_{\mathbb{Q}} s
\end{aligned}$$

Part 2:

$$\begin{aligned}
r \cdot_{\mathbb{Q}} t <_{\mathbb{Q}} s \cdot_{\mathbb{Q}} t &\iff [\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle e, f\rangle] <_{\mathbb{Q}} [\langle c, d\rangle] \cdot_{\mathbb{Q}} [\langle e, f\rangle] \\
&\iff \langle ae, bf\rangle <_{\mathbb{Q}} \langle ce, df\rangle \\
&\iff aedf < cebf \\
&\iff ad < cb \\
&\iff [\langle a, b\rangle] <_{\mathbb{Q}} [\langle c, d\rangle] \\
&\iff r <_{\mathbb{Q}} s
\end{aligned}$$

□

**Theorem 5.40.** *Let $r, s$ and $t$ be rational numbers. Then the following cancellation laws hold:*

1. $(r +_{\mathbb{Q}} t = s +_{\mathbb{Q}} t) \implies r = s$
2. $(r \cdot_{\mathbb{Q}} t = s \cdot_{\mathbb{Q}} t) \wedge t \neq 0_{\mathbb{Q}} \implies r = s$

*Proof.* The proof follows directly by adding $-t$ to both sides of the equation in Part 1 and multiplying by $t^{-1}$ on both sides of the equation in Part 2. □

**Theorem 5.41.** *Consider the embedding $E : \mathbb{Z} \to \mathbb{Q}$ defined by*

$$E(a) = [\langle a, 1\rangle]$$

*Then the following properties are satisfied:*

1. *$E$ is an injective function*
2. *$E(a+b) = E(a) +_{\mathbb{Q}} E(b)$*
3. *$E(ab) = E(a) \cdot_{\mathbb{Q}} E(b)$*
4. *$a < b \iff E(a) <_{\mathbb{Q}} E(b)$*

*Proof.*

Part 1:

$$\begin{aligned} E(a) = E(b) &\implies [\langle a, 1\rangle] = [\langle b, 1\rangle] \\ &\implies \langle a, 1\rangle \sim \langle b, 1\rangle \\ &\implies a = b \end{aligned}$$

Part 2:

$$\begin{aligned} E(a+b) &= [\langle a+b, 1\rangle] \\ &= [\langle a, 1\rangle] +_{\mathbb{Q}} [\langle b, 1\rangle] \\ &= E(a) +_{\mathbb{Q}} E(b) \end{aligned}$$

Part 3:

$$\begin{aligned} E(ab) &= [\langle ab, 1\rangle] \\ &= [\langle a, 1\rangle] \cdot_{\mathbb{Q}} [\langle b, 1\rangle] \\ &= E(a) \cdot_{\mathbb{Q}} E(b) \end{aligned}$$

Part 4:

$$\begin{aligned} a < b &\iff a \cdot 1 < b \cdot 1 \\ &\iff [\langle a, 1\rangle] <_{\mathbb{Q}} [\langle b, 1\rangle] \\ &\iff E(a) <_{\mathbb{Q}} E(b) \end{aligned}$$

□

**Remark.** *From now on, we shall omit the $\mathbb{Q}$ subscript on all operations and assume them to be implicit.*

## 5.3 Real Numbers

**Definition 5.42.** *A **Dedekind cut** is a subset $x$ of $\mathbb{Q}$ satisfying the following properties:*

1. $\varnothing \neq x \neq \mathbb{Q}$
2. *$x$ is **closed downward**. In other words:*

$$q \in x \wedge r < q \implies r \in x$$

3. *$x$ has no largest member*

**Definition 5.43.** *We define the set of **real numbers** $\mathbb{R}$ to be the set of all Dedekind cuts.*

**Definition 5.44.** *Let $x$ and $y$ be real numbers. We define the ordering relation $<_{\mathbb{R}}$ on the real numbers by the following:*

$$x <_{\mathbb{R}} y \iff x \subset y$$

**Theorem 5.45.** *The relation $<_{\mathbb{R}}$ is a linear ordering on $\mathbb{R}$.*

*Proof.* We first show that $<_{\mathbb{R}}$ is transitive on $\mathbb{R}$. Let $x, y$ and $z$ be real numbers such that $x <_{\mathbb{R}} y$ and $y <_{\mathbb{R}} z$. Then we have that

$$\begin{aligned}(x <_{\mathbb{R}} y) \wedge (y <_{\mathbb{R}} z) &\iff (x \subset y) \wedge (y \subset z) \\ &\iff x \subset z \\ &\iff x <_{\mathbb{R}} z\end{aligned}$$

We now show that $<_{\mathbb{R}}$ satisfies trichotomy on the real numbers. Let $x, y \in \mathbb{R}$. We need to show that at most one of the following holds:

$$x \subset y, \qquad x = y, \qquad y \subset x$$

Suppose that $x \not\subseteq y$. We must show that $y \subset x$. Since $x \not\subseteq y$, we may choose a rational number $r \in x \backslash y$. Let $q \in y$, we need to show that $q \in x$. If $r \leq q$ then, since $y$ is closed downward, we have that $r \in y$. But this contradicts that $r \in x \backslash y$. Hence we must have that $q < r$. But $x$ is closed downward and $r \in x$ thus $q \in x$. □

**Definition 5.46.** *Let $A \subseteq \mathbb{R}$ be a subset. We say that a real number $x$ (not necessarily a member of $A$) is an **upper bound** for $A$ if $y \leq_{\mathbb{R}} x$ for all $y \in A$. In this case, $A$ is said to be **bounded**. A **least upper bound** of $A$ is an upper bound that is less than any other upper bound.*

**Theorem 5.47.** *Any bounded non-empty subset of $\mathbb{R}$ has a least upper bound in $\mathbb{R}$.*

*Proof.* Let $A$ be a subset satisfying the conditions of the theorem. We show that the least upper bound is $\bigcup A$.
By the definition of $\bigcup A$, we have that $x \subseteq \bigcup A$ for all $x \in A$. Now let $z$ be any upper bound for $A$ so that $x \subseteq z$ for all $x \in A$. It thus follows that $\bigcup A \subseteq z$.
It remains to show that $\bigcup A$ is in fact a real number. Since $A$ is non-empty, it is obvious that $\bigcup A \neq \varnothing$. Furthermore since $\bigcup \subseteq z$ (where $z$ is an upper bound for $A$), we must have that $\bigcup A \neq \mathbb{Q}$.
To show that $\bigcup A$ is closed downward, suppose $q \in \bigcup A$ and that $r \leq q$ for some rational numbers $q$ and $r$. Since $q \in \bigcup A$, there must exist some real number $a \in A$ such that $q \in a$. But $a$ is a real number and is thus closed downward, hence $r \in a$. It thus follows that $r \in a \subseteq \bigcup A$ and hence $\bigcup A$ is closed downward.
It remains to show that $\bigcup A$ has no largest element. Suppose the contrary and that there exists an $x \in \bigcup A$ such that for all $y \in \bigcup A, y \leq_{\mathbb{R}} x$. Since $x \in \bigcup A$, there must exist some real number $a \in A$ such that $x \in a$. Since $a$ is a real number, it does not have a largest element. Choose an element $x_2 \in a$ that is bigger than $x$. We have that $x_2 \in a \subseteq \bigcup A$ and thus $x_2 \in \bigcup A$. But then $x_2$ is an element of $\bigcup A$ which is larger than $x$, contradicting the assumption that $x$ is the largest element of $\bigcup A$. Hence $\bigcup A$ cannot have a largest element. □

**Definition 5.48.** *Let $x$ and $y$ be two real numbers. We define the operation of **addition** $+_{\mathbb{R}}$ on the real numbers by the following:*

$$x +_{\mathbb{R}} y = \{\, q + r \mid q \in x \wedge r \in y \,\}$$

**Lemma 5.49.** *Let $x$ and $y$ be real numbers. Then their sum $z = x +_{\mathbb{R}} y$ is also a real number.*

*Proof.* It is obvious that $z$ is a non-empty subset of $\mathbb{Q}$. We now show that

their sum cannot equal all of $\mathbb{Q}$. Choose $q' \in \mathbb{Q}\backslash x$ and $r' \in \mathbb{Q}\backslash y$. Then

$$\begin{aligned} q \in x \wedge r \in y &\implies q < q' \wedge r < r' \\ &\implies q + r < q' + r' \end{aligned}$$

Hence any member $q + r$ of $z$ is strictly less than $q' + r'$ and thus $q' + r' \notin z$. We next show that $z$ is closed downward. Let $q + r \in z$ and consider a rational number $p$ such that $p < q + r$. Adding $-q$ to both sides, we have that $p + (-q) < r$. Since $y$ is closed downward, we have that $p + (-q) \in y$. Obviously, we can rewrite $p = q + (p + (-q))$ where $q \in x$ and $p + (-q) \in y$. Hence, by definition of $z$, we must have that $p \in z$.
It remains to show that $z$ has no largest element. Suppose that $q + r$ is the largest element of $z$. Since $x$ is a real number, there must exist some rational number $s$ such that $q < s$ and $s \in x$. By definition of $z$, we then have that $s + r \in z$. We see that

$$q < s \implies q + r < s + r$$

which contradicts that $q + r$ is the largest element of $z$. □

**Theorem 5.50.** *Let $x, y$ and $z$ be real numbers. Then the following properties hold:*

1. *Associativity of $+_{\mathbb{R}}$:*

$$(x +_{\mathbb{R}} y) +_{\mathbb{R}} z = x +_{\mathbb{R}} (y +_{\mathbb{R}} z)$$

2. *Commutativity of $+_{\mathbb{R}}$:*

$$x +_{\mathbb{R}} y = y +_{\mathbb{R}} x$$

*Proof.*

Part 1:

$$\begin{aligned} (x +_{\mathbb{R}} y) +_{\mathbb{R}} z &= \{\, s + r \mid s \in\ +_{\mathbb{R}} y \wedge r \in z \,\} \\ &= \{\, (p + q) + r \mid p \in x \wedge q \in y \wedge r \in z \,\} \\ &= \{\, p + (q + r) \mid p \in x \wedge q \in y \wedge r \in z \,\} \\ &= \{\, p + s \mid p \in x \wedge s \in y +_{\mathbb{R}} z \,\} \\ &= x +_{\mathbb{R}} (y +_{\mathbb{R}} z) \end{aligned}$$

Part 2:

$$\begin{aligned} x +_{\mathbb{R}} y &= \{\, p + q \mid p \in x \wedge q \in y \,\} \\ &= \{\, q + p \mid q \in y \wedge p \in x \,\} \\ &= y +_{\mathbb{R}} x \end{aligned}$$

□

**Definition 5.51.** *We define the zero element* $0_{\mathbb{R}}$ *as follows:*

$$0_{\mathbb{R}} = \{\, r \in \mathbb{Q} \mid r < 0 \,\}$$

**Remark.** *It is quite easy to see that* $0_{\mathbb{R}}$ *is a real number. It is indeed non-empty and does not coincide with* $\mathbb{Q}$*. It is obviously closed downward and it has no maximal element as between any two rational numbers, there is always another rational number.*

**Theorem 5.52.** *Let* $x \in \mathbb{R}$*. Then* $x +_{\mathbb{R}} 0_{\mathbb{R}} = x$

*Proof.* We need to show that

$$\{\, r + s \mid r \in x \wedge s < 0 \,\} = x$$

$\subseteq$: Let $p \in \{\, r + s \mid r \in x \wedge s < 0 \,\}$. We must show that $p \in x$. By definition, we have that $p = r + s$ where $r \in x$ and $s < 0$. Obviously $r + s < r$ and, since $x$ is closed downward, we must have that $p = r + s \in x$.

$\supseteq$: Let $p \in x$. We must show that $p \in \{\, r + s \mid r \in x \wedge s < 0 \,\}$. Since $x$ has no largest member, there must exist some rational number $r$ such that $p < r \in x$. Let $s = p + (-r)$. Then obviously, $s < 0$ and $p = r + s$ and thus $p \in \{\, r + s \mid r \in x \wedge s < 0 \,\}$.

□

**Definition 5.53.** *Let* $x$ *be a real number. We define the* ***additive inverse*** *of* $x$ *by the following:*

$$-x = \{\, r \in \mathbb{Q} \mid (\exists\, s > r) - s \in x \,\}$$

**Theorem 5.54.** *Let $x \in \mathbb{R}$. Then the following hold:*

1. $-x \in \mathbb{R}$
2. $x +_{\mathbb{R}} (-x) = 0_{\mathbb{R}}$

*Proof.*

Part 1: We first show that $\varnothing \neq -x \neq \mathbb{Q}$. Let $t$ be a rational number such that $t \notin x$. Let $r = -t - 1$. Then $r \in x$ since $r < -t$ and $-(-t) \notin x$. Hence $-x \neq \varnothing$. Now take any $p \in x$. We claim that $-p \notin -x$. If $s > -p$ then $-s < p \in x$ whence it follows that $-s \in x$ (as $x$ is closed downward). Hence $-p \notin -x$ and thus $-x \neq \mathbb{Q}$.
we next show that $-x$ is closed downward. Let $r \in -x$ and let $q$ be a rational number such that $q < r$. Then there must exist an $s > r$ such that $-s \in x$. Consequently, there exists an $s > q$ such that $-s \in x$ and this $q \in -x$.
It remains to show that $-x$ has no largest element. Let $r \in -x$. By definition of $-x$, we know that there exists an $s > r$ such that $-s \notin x$. We can always choose another rational $p$ such that $s > p > r$. Then $p \in -x$ and $p$ is larger then $r$.

Part 2: By definition, we have that

$$x +_{\mathbb{R}} (-x) = \{\, q + r \mid q \in x \wedge (\exists\, s > r) - s \notin x \,\}$$

We need to show that

$$\{\, q \in \mathbb{Q} \mid q < 0 \,\} = \{\, q + r \mid q \in x \wedge (\exists\, s > r) - s \notin x \,\}$$

$\subseteq$: Let $p \in 0_{\mathbb{R}}$. We need to show that $p \in \{\, q + r \mid q \in x \wedge (\exists\, s > r) - s \notin x \,\}$. By definition, we have that $p < 0$ and thus $-p$ is a positive rational number. We can of course find some $q \in x$ such that $q + (-p \div 2) \notin x$. Let $s = (p/div2) - q$. Then $-s$ $\not\in nx$. We thus have that $p = q + (p - q)$ where $q \in x$ and $p - q \in -x$ ($p - q < s$ where $s \notin x$). Hence $p \in x +_{\mathbb{R}} (-x)$.

$\supseteq$: Let $q + r \in \{\, q + r \mid q \in x \wedge (\exists\, s > r) - s \notin x \,\}$. We have that $r < s$ and $q < -s$. Hence

$$q + r < (-s) + s = 0$$

Hence $q + r \in 0_{\mathbb{R}}$.

□

**Corollary 5.55.** *Let $x, y$ and $z$ be real numbers. Then*

$$x +_{\mathbb{R}} z = y +_{\mathbb{R}} z \implies x + y$$

*Proof.* This follows directly by adding $-z$ to both sides of the equation. □

**Theorem 5.56.** *Let $x, y$ and $z$ be real numbers. Then*

$$x <_{\mathbb{R}} y \iff x +_{\mathbb{R}} z < y +_{\mathbb{R}} z$$

*Proof.*

$\implies$ : It is easy to see that

$$x \leq_{\mathbb{R}} y \implies x +_{\mathbb{R}} z < y +_{\mathbb{R}} z$$

since this is equivalent to the statement that if $x \subseteq y$ then

$$\{\, q + s \mid q \in x \wedge s \in z \,\} \subseteq \{\, r + s \mid r \in y \wedge s \in z \,\}$$

By the previous corollary, we have that

$$x \neq y \implies x +_{\mathbb{R}} z \neq y +_{\mathbb{R}} z$$

$\impliedby$ : This part follows directly from the trichotomy of $+_{\mathbb{R}}$

□

**Definition 5.57.** *Let $x$ be a real number. We define its **absolute value** $|x|$ as follows:*

$$|x| = x \cup -x$$

*In other words, the absolute value is the larger of $x$ and $-x$.*

**Remark.** *It is clear that $|x|$ is always non-negative.*

**Definition 5.58.** *Let $x$ and $y$ be real numbers. We define the operation of **multiplication** $\cdot_{\mathbb{R}}$ as follows:*

- *If $x$ and $y$ are non-negative real numbers then*

$$x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}} \cup \{\, rs \mid 0 \leq r \in x \wedge 0 \leq s \in y \,\}$$

- *If $x$ and $y$ are both negative real numbers, then*

$$x \cdot_{\mathbb{R}} y = |x| \cdot_{\mathbb{R}} |y|$$

- *If one of $x$ and $y$ is negative and the other is non-negative, then*

$$x \cdot_{\mathbb{R}} y = -(|x| \cdot_{\mathbb{R}} |y|)$$

**Theorem 5.59.** *Let $x, y$ and $z$ be real numbers. Then the following hold:*

1. *$x \cdot_{\mathbb{R}} y$ is a real number*
2. *Multiplication is associative, commutative and distributive over addition*
3. *$0_{\mathbb{R}} \neq 1_{\mathbb{R}}$ and $x \cdot_{\mathbb{R}} 1_{\mathbb{R}} = x$*
4. *For non-zero $x$, there is a non-zero real number $y$ such that $x \cdot_{\mathbb{R}} y = 1_{\mathbb{R}}$*
5. *Multiplication by a positive number preserves order: If $0_{\mathbb{R}} <_{\mathbb{R}} z$ then*

$$x <_{\mathbb{R}} y \iff x \cdot_{\mathbb{R}} z <_{\mathbb{R}} y \cdot_{\mathbb{R}} z$$

**Theorem 5.60.** *Consider the embedding $E : \mathbb{Q} \to \mathbb{R}$ given by*

$$E(r) = \{\, q \in \mathbb{Q} \mid q < r \,\}$$

*In other words, every rational number $r$ can be realised as a real number by constructing the set of all rational numbers less than $r$. Such an embedding function satisfies the following properties:*

1. *$E$ is a real number*
2. *$E$ is an injective function*
3. *$E(r + s) = E(r) +_{\mathbb{R}} E(s)$*
4. *$E(rs) = E(r) \cdot_{\mathbb{R}} E(s)$*
5. *$r < s \iff E(r) <_{\mathbb{R}} E(s)$*

*Proof.*

Part 1: Fix $r \in \mathbb{Q}$. By definition, $E(r)$ is closed downward. Obviously, $\varnothing \neq E(r) \neq \mathbb{Q}$ as $r - 1 \in E(r)$ and $r \notin E(r)$. $E(r)$ has no largest element as if $q \in E(r)$ then there is a larger rational $p$ such that $q < p < r$. Therefore $E(r)$ is a real number.

Part 2: Suppose that $r \neq s$. We must show that $E(r) \neq E(s)$. If $r \neq s$ then by trichotomy, one is less than the other. Without loss of generality, we may assume that $r < s$. Then $r \in E(s)$ whereas $r \notin E(r)$ hence $E(r) \neq E(s)$.

Part 3: We have that

$$\begin{aligned} E(r) +_{\mathbb{R}} E(s) &= \{\, p + q \mid p \in E(r) \wedge q \in E(s) \,\} \\ &= \{\, p + q \mid p < r \wedge q < s \,\} \end{aligned}$$

We need to show that this is equivalent to the following set:

$$\{\, t \mid t < r + s \,\}$$

$\subseteq$: By Theorem 5.39, we have that

$$p + q < r + q < r + s$$

and thus $\{\, p + q \mid p < r \wedge q < s \,\} \subseteq \{\, t \mid t < r + s \,\}$

$\supseteq$: Suppose that $t < r + s$. Define $\varepsilon = (r + s - t) \div 2$. Then $\varepsilon > 0$. Now let $p = r - \varepsilon$ and $q = s - \varepsilon$. Then $p < r$ and $q < s$ and $p + q = t$. Hence $t \in \{\, p + q \mid p < r \wedge q < s \,\}$.

Part 4: The proof of this part is omitted .

Part 5: If $r < s$ then clearly $E(r) \subseteq E(s)$. Since $E$ is injective, the inclusion must be proper. The converse follows from trichotomy. If $E(r) \subset E(s)$ then we cannot have $r = s$ nor $s < r$ (lest $E(s) < E(r)$) so we must have that $r < s$.

□

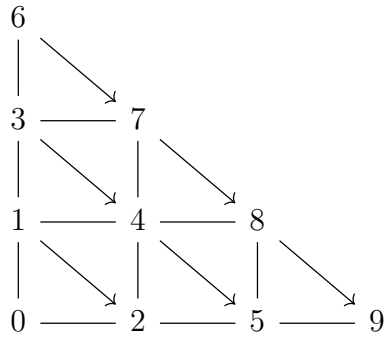
# Chapter 6

# Cardinal Numbers and the Axiom of Choice

## 6.1 Equinumerosity

**Definition 6.1.** *Let $A$ and $B$ be sets. We say that $A$ is* ***equinumerous*** *to $B$, denoted $A \approx B$ if there exists a bijection from $A$ onto $B$.*

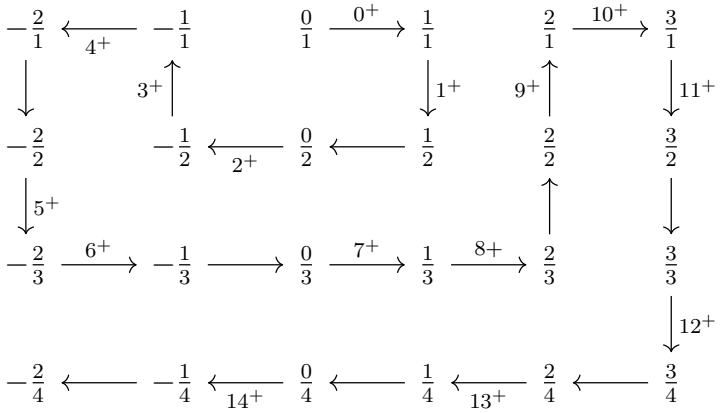
**Example 6.2.** *$\omega \times \omega$ is equinumerous to $\omega$ as the following diagram demonstrates:*




*where the arrows indicate the progression of the natural numbers. This can also be written as the following function:*

$$J(m,n) = \frac{1}{2}\left[(m+n)^2 + 3m + n\right]$$

**Example 6.3.** *$\mathbb{Q} \approx \omega$. The bijection is demonstrated in the diagram below. In order to ensure that the function is injective, we skip fractions that would be in the same equivalence class as fractions that have been covered before.*




**Example 6.4.** *The open unit interval*

$$(0,1) = \{\, x \in \mathbb{R} \mid 0 < x < 1 \,\}$$

*is equinumerous to* $\mathbb{R}$*. A bijection* $f : (0,1) \to \mathbb{R}$ *is given by*

$$f(x) = \tan \frac{\pi(2x-1)}{2}$$

**Example 6.5.** *For any set* $A$*, we have that* $\mathcal{P}A \approx^A 2$*. We define a bijection* $H : \mathcal{P}A \to^A 2$ *as follows: Let* $B$ *be a subset of* $A$*. Then* $H(B)$ *is the characteristic function of* $B$*. In other words, the function* $f_B$ *from* $A$ *into 2 for which*

$$f_B(x) = \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{if } x \in A \backslash B \end{cases}$$

*Then any function* $g \in^A 2$ *is in* $\operatorname{ran} H$ *since*

$$g = H(\{\, x \in A \mid g(x) = 1 \,\})$$

**Theorem 6.6.** *Let* $A$*,* $B$ *and* $C$ *be sets. Then we have that*

1. $A \approx A$
2. $A \approx B \implies B \approx A$
3. $A \approx B \wedge B \approx C \implies A \approx C$

*Proof.*

Part 1: This part is trivial as we can just take the identity function (which is clearly bijective):

$$\begin{aligned} f : A &\to A \\ x &\mapsto x \end{aligned}$$

Part 2: We have that $A \approx B$ and thus, by definition, there must exist some bijection $f : A \to B$. By results from Chapter 3, we can always find a bijective inverse $f^{-1} : B \to A$ of $f$ and thus $B \approx A$.

Part 3: We have that $A \approx B$ and $B \approx C$. By definition, there must exist bijections $f : A \to B$ and $g : B \to C$. Consider the composition function $h = g \circ f$. Then by results from Chapter 3, $h$ is a bijection from $A$ into $C$ whence $A \approx C$.

□

**Remark.** *Despite the fact that $\approx$ satisfies the conditions for an equivalence relation, we cannot label it as such. The reason for this is that it concerns all sets and, as we know, we cannot form the set of all sets.*

**Theorem 6.7.**

1. *The set $\omega$ is not equinumerous to the set $\mathbb{R}$ of all real numbers.*

2. *No set is equinumerous to its power set.*

*Proof.* Part 1: Fix a function $f : \omega \to \mathbb{R}$. We claim that there exists a real number $z \in \mathbb{R}$ such that $z \notin ran\, f$. We can write the values $f$ takes in the following array:

$$\begin{aligned} f(0) &= k_0.d_{01}d_{02}d_{03}\dots \\ f(1) &= k_1.d_{11}d_{12}d_{13}\dots \\ f(2) &= k_2.d_{21}d_{22}d_{23}\dots \\ &\vdots \\ f(n) &= k_n.d_{n1}d_{n2}d_{n3}\dots d_{nn+1}\dots \end{aligned}$$

where $k_n$ is the integer part of $f(n)$ and the $d_{ni}$ are the decimals of $f(n)$ with $i \geq 1$.
We now define the real number $z$ as follows:

$$z = 0.d_1 d_2 d_3 \dots d_{n+1}$$

where $d_{n+1} = 1$ if $d_{nn+1} \neq 1$ else $d_{n+1} = 2$. By this definition, we can see that

$$d_{n+1} \neq d_{nn+1}$$

for all $n \geq 0$. It thus follows that $z$ cannot be in the array above whence $z \notin ran\, f$

Part 2: Fix $g : A \to \mathcal{P}A$. we claim that there exists a subset $B$ of $A$ such that $B \notin ran\, g$. Let

$$B = \{\, x \in A \mid x \notin g(x) \,\}$$

Then, obviously, $B \subseteq A$ but given $x \in A$,

$$x \in B \iff x \notin g(x)$$

Hence $B \neq g(x)$.

□

## 6.2 Finite Sets

**Definition 6.8.** *Let $A$ be a set. We say that $A$ is **finite** if $A \approx n$ for some $n \in \omega$. If not then we say that $A$ is **infinite**.*

**Example 6.9.** *It follows trivially from the definition that any natural number is itself finite.*

**Theorem 6.10.** *(Pigeonhole Principle)*
*No natural number is equinumerous to a proper subset of itself.*

*Proof.* Fix a natural number $n \in \omega$ and let $f$ be an injective function from $n$ into $n$. We show that $ran\, f$ necessarily coincides with $n$ (and not a proper subset of $n$). Define

$$T = \{\, n \in \omega \mid \text{any injective function from } n \text{ into } n \text{ has range } n \,\}$$

We claim that $T$ is inductive. Obviously $0 \in T$ as the only function from 0 into 0 is $\varnothing$ and its range is 0. Now suppose that $k \in T$. We must show that $k^+ \in T$. Suppose $f$ is an injective function from $k^+$ into $k^+$. It suffices to show that $ran\, f = k^+$. Now consider $f|_k$. This restriction maps the set $k$ injectively into $k^+$. We have the following two cases:

Case 1: We have the case where the set $k$ is closed under $f$. In that case $f|_k$ is an injective map between $k$ and $k$. Now since $k \in T$, we can conclude that $ran(f|_k) = k$. Now since $f$ is injective, the only possible value for $f(k)$ is $k$ itself. Hence $ran\, f = k \cup \{\, k \,\} = k^+$.

Case 2: We have the case where $f(p) = k$ for some $p < k$. If this is the case then we interchange two values of the function. Define the function $\hat{f}$ by the following:

$$\hat{f}(x) = \begin{cases} f(k) & \text{if } x = p \\ f(p) & \text{if } x = k \\ f(x) & \text{if } otherwise \end{cases}$$

Then $\hat{f}$ maps $k^+$ injectively into $k^+$ and the set $k$ is closed under $\hat{f}$. Then by the first case, $ran\, \hat{f} = k^+$. But $ran\, \hat{f} = ran\, f$. Hence in either case, $ran\, f = k^+$. It follows that $T$ is inductive whence $T = \omega$.

□

**Remark.** *The previous theorem essentially implies that if n objects are placed into fewer than n pigeonholes then there most be some pigeonhole that receives more than one object.*

**Corollary 6.11.** *No finite set is equinumerous to a proper subset of itself.*

*Proof.* Fix a finite set $A$ and let $g$ be the bijection between $A$ and some natural number $n$. Suppose that there exists a bijection $g$ between $A$ and some proper subset of $A$. Now consider the composition map $g \circ f \circ g^{-1}$. This composition maps $n$ into $n$ and is bijective. Furthermore, its range is $C$ where $C$ is some proper subset of $n$. Then $n$ is equinumerous to $C$, contradicting the pigeonhole principle. □

**Corollary 6.12.**

1. *Any set that is equinumerous to a proper subset of itself is infinite.*
2. *The set $\omega$ is infinite.*

*Proof.*

Part 1: The proof of this part follows directly from the contrapositive of the previous corollary.

Part 2: Consider the function $\sigma$ whose value at each number $n$ is $n^+$. Then $\sigma$ maps $\omega$ bijectively into $\omega \setminus \{ 0 \}$. Hence by Part 1, $\omega$ is infinite.

□

**Corollary 6.13.** *Any finite set is necessarily equinumerous to a unique natural number.*

*Proof.* Fix a finite set $A$. Suppose that $A \approx m$ and $A \approx n$ for distinct natural numbers $m$ and $n$. By trichotomy, we must either have that $m = n$ or that one is a proper subset of the other. But the latter case is impossible since $m \approx n$. Hence $m = n$. □

**Definition 6.14.** *Let $A$ be a finite set where $A \approx n$ for some natural number $n$ (where the uniqueness of $n$ is guaranteed by the previous corollary). Then $n$ is said to be the* ***cardinal number*** *of $A$, denoted $A$.*

**Example 6.15.** *Let $n$ be a natural number. Then $|n| = n$.*

**Example 6.16.** *Suppose $a, b, c$ and $d$ are all distinct objects. Then $|\{ a, b, c, d \}| = 4$.*

**Remark.** *We leave a rigorous definition of $|A|$ to Chapter 7. For now, we shall assume the following properties:*

- *Let $A$ and $B$ be sets. Then*

$$|A| = |B| \iff A \approx B$$

- *For a finite set $A$, $|A|$ is the natural number $n$ for which $A \approx n$.*

*The cardinality for infinite sets is not yet defined. For now, we shall define the cardinality of $\omega$ by*

$$|\omega| = \aleph_0$$

**Lemma 6.17.** *Let $C$ be a proper subset of a natural number $n$. Then $C \approx m$ for some $m$ less than $n$.*

*Proof.* Consider the set

$$T = \{\, n \in \omega \mid \text{any proper subset of } n \text{ is equinumerous to a member of } n \,\}$$

We claim that $T$ is inductive. $0 \in T$ vacuously as it has no proper subsets. Suppose that $k \in T$. We must show that $k^+ \in T$. Consider a proper subset $C$ of $k^+$. We have three cases.

Case 1: $C = k$. In this case, $C \approx k \in k^+$.

Case 2: $C \subset k$. Then since $k \in T$, we have that $C \approx m$ where $m \in k \in k^+$.

Case 3: Otherwise, $k \in C$. Then $C = (C \cap k) \cup \{\, k \,\}$ and $C \cap k$ is a proper subset of $k$. Since $k \in T$, there is a an $m \in k$ such that $C \cap k \approx m$. Let $f$ be the bijection between them. Then $f \cup \{\, \langle k, m \rangle \,\}$ is a bijection between $C$ and $m^+$. Since $m \in k$, we have that $m^+ \in k^+$. Hence, $C \approx m^+ \in k^+$ and $k^+ \in T$.

Hence $T$ is inductive and coincides with $\omega$. □

**Corollary 6.18.** *Any subset of a finite set is finite.*

*Proof.* Consider $A \subseteq B$ where $B$ is a finite set. Let $f$ be a bijection between $B$ and $n$ where $n$ is a natural number. Then $A \approx f[\![A]\!] \subseteq n$ and, by the previous lemma, $f[\![A]\!] \approx m$ for some $m \subseteq n$. Hence $A \approx m \in \omega$. □

## 6.3 Cardinal Arithmetic

**Definition 6.19.** *Let $\kappa$ and $\lambda$ be cardinal numbers. Then*

- $\kappa + \lambda = |K \cup L|$ *where $K$ and $L$ are disjoint sets of cardinality $\kappa$ and $\lambda$ respectively.*
- $\kappa \cdot \lambda = |K \times L|$ *where $K$ and $L$ are any sets of cardinality $\kappa$ and $\lambda$ respectively*
- $\kappa^\lambda = \left|{}^L K\right|$ *where $K$ and $L$ are any sets of cardinality $\kappa$ and $\lambda$*

**Theorem 6.20.** *Assume that $K_1 \approx K_2$ and $L_1 \approx L_2$. Then*

1. *If $K_1 \cap L_1 = K_2 \cap L_2 = \varnothing$ then $K_1 \cup K_2 \approx K_2 \cup L_2$*
2. *$K_1 \times L_1 \approx K_2 \times L_2$*
3. *${}^{(L_1)}K_1 \approx {}^{(L_2)}K_2$*

*Proof.*

Part 1: Since $K_1 \approx K_2$ there exists a bijection $f$ between $K_1$ and $K_2$. Since $L_1 \approx L_2$, there exists a bijection $g$ between $L_1$ and $L_2$. Now consider the surjective relation

$$h(x) = \begin{cases} f(x) & \text{if } x \in K_1 \\ g(x) & \text{if } x \in L_1 \end{cases}$$

which maps $K_1 \cup L_1$ onto $K_2 \cup L_2$. Now since $K_1 \cap L_1 = \varnothing$, $h$ is guaranteed to be a function. Since $K_2 \cap L_2 = \varnothing$, $h$ is guaranteed to be injective. Hence $h$ is a bijection between $K_1 \cup L_1$ and $K_2 \cup L_2$ whence $K_1 \cup L_1 \approx K_2 \cup L_2$.

Part 2: Let $x \in K_1$ and $y \in L_1$. Consider the function

$$h(\langle x, y\rangle) = \langle f(x), g(y)\rangle$$

Then $h$ is a bijection between $K_1 \times L_1$ and $K_2 \times L_2$.

Part 3: First consider the following diagram:

$$\begin{array}{ccc} L_2 & \xrightarrow{H(j)} & K_2 \\ {\scriptstyle g^{-1}}\downarrow & & \uparrow{\scriptstyle f} \\ L_1 & \xrightarrow[j]{} & K_1 \end{array}$$

It is easy to see that $H(j)$ is a function from $L_2$ to $K_2$ (independent of the choice of $j$). Consider $j$ and $j'$ such that $j \neq j'$. In other words, there exists some $t \in L_1$ such that $j(t) \neq j'(t)$. Then we have that

$$H(j)(g(t)) = f(j(g^{-1}(g(t)))) = f(j(t)) \neq f(j'(t)) = f(j'(g^{-1}(g(t)))) = H(j')(g(t))$$

where we have used the fact that $f$ is an injective function. Hence we see that $H(j) \neq H(j')$ (as is evidenced by their differing action on $g(t)$) and thus $H(j)$ is injective.
We now show that $H(j)$ is a surjective function. Consider any function $d \in {}^{L_2}K_2$. Then $d = H(j)$ where $j = f^{-1} \circ d \circ g$. □

**Example 6.21.**

1. *Let $m$ and $n$ be natural numbers. Then*

$$m \cdot n = |m \times n| \qquad \text{and} \qquad m^n = |{}^n m|$$

2. *Let $n$ be a natural number. Then*

   - $n + \aleph_0 = \aleph_0$
   - $n \cdot \aleph_0 = \aleph_0$ *unless* $n = 0$
   - $\aleph_0 + \aleph_0 = \aleph_0$
   - $\aleph_0 \cdot \aleph_0$

3. *Let $\kappa$ be a cardinal number. Then*

   - $\kappa + 0 = \kappa$
   - $\kappa \cdot 0 = 0$
   - $\kappa \cdot 1 = \kappa$
   - $\kappa^0 = 1$
   - $0^\kappa = 0$ *for non-zero* $\kappa$

4. *Let $A$ be a set. Then $|\mathcal{P}A| = 2^{|A|}$*

5. *By Cantor's Theorem and the preceeding example, $\aleph_0 \neq 2^{\aleph_0}$*

**Theorem 6.22.** *Let $\kappa, \lambda$ and $\mu$ be cardinal numbers. Then*

1. $\kappa + \lambda = \lambda + \kappa$
2. $\kappa \cdot \lambda = \lambda \cdot \kappa$
3. $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$
4. $\kappa \cdot (\lambda + \mu) = (\kappa \cdot \lambda) \cdot \mu$
5. $\kappa(\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$
6. $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$
7. $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$

8. $(\kappa^\lambda)^\mu = \kappa^{\lambda \cot \mu}$

*Proof.* Consider sets $K, L$ and $M$ with $|K| = \kappa, |L| = \lambda$ and $|M| = \mu$. For convenience, we choose them in such a way that any two are disjoint. Then each of the equations reduces to a corresponding statement about equinumerous sets:

Part 1: We have that $\kappa + \lambda = |K \cup L|$ and $\lambda + \kappa = |L \cup K|$. Hence we must show that $K \cup L \approx L \cup K$. Consider the function $f : K \cup L \to L \cup K$ given by $f : x \mapsto x$ (in other words, the identity function). Then $f$ is a bijection between the two sets.

Part 2: We have that $\kappa \cdot \lambda = |K \times L|$ and $\lambda \cdot \kappa = |L \times K|$. We must therefore show that $K \times L \approx L \times K$. Consider the function

$$\begin{aligned} f : K \times L &\to L \times K \\ \langle x, y \rangle &\mapsto \langle y, x \rangle \end{aligned}$$

Then $f$ is a bijection.

Part 3: The proof of this part follows directly from the associativity of set union and the use of the identity bijection.

Part 4: The proof of this part follows similar argumentation as that of Part 2.

Part 5: We have that $\kappa(\lambda + \mu) = |K \times (L \cup M)|$ and $\kappa \cdot \lambda + \kappa \cdot \mu = |(K \times L) \cup (K \times M)|$. Hence we must show that $K \times (L \cup M) \approx (K \times L) \cup (K \times M)$. Consider the function

$$\begin{aligned} f : K \times (L \cup M) &\to (K \times L) \cup (K \times M) \\ \langle x, y \rangle &\mapsto \langle x, y \rangle \end{aligned}$$

Then $f$ is a bijection.

Part 6: We have that $\kappa^{\lambda+\mu} = \left|{}^{(L \cup M)}K\right|$ and $\kappa^\lambda \cdot \kappa^\mu = \left|{}^L K \times {}^M K\right|$. Hence we must show that ${}^{(L \cup M)}K \approx {}^L K \times {}^M K$. Consider the following function

$$\begin{aligned} h : {}^{(L \cup M)}K &\to {}^L K \times {}^M K \\ g &\mapsto \langle g|_L, g|_M \rangle \end{aligned}$$

We claim that $h$ is a bijection. We first show that $h$ is injective. Let $h(g) = h(g')$. Then $\langle g|_L, g|_M \rangle = \langle g'|_L, g'|_M \rangle$. We know that ordered pairs are equal

if and only if their coordinates are equal. Thus we have that $g|_L = g'|_L$ and $g|_M = g'|_M$. Since $L$ and $M$ are disjoint, the restrictions of any function on $L \cup M$ are disjoint on $L$ and $M$. It thus follows that $g = g'$.
We now show that $h$ is surjective. Let $\langle a, b\rangle \in {}^{L}K \times {}^{M}K$ where $a$ is a function on $L$ and $b$ is a function on $m$. We must exhibit a function $c \in {}^{(L\cup M)}K$ such that $h(c) = \langle a, b\rangle$. Consider $c = a \cup b$. Then $h(c) = \langle c|_L, c|_M\rangle = \langle a, b\rangle$ as required.

Part 7: We have that $(\kappa\cdot\lambda)^\mu = \left|{}^{M}(K \times L)\right|$ and $\kappa^\mu\cdot\lambda^\mu = \left|{}^{M}K \times {}^{M}L\right|$. Hence we must show that ${}^{M}(K \times L) \approx {}^{M}K \times {}^{M}L$. Let $f \in {}^{M}(K \times L)$. Consider the ordered pair $\langle f, g\rangle \in {}^{M}K \times {}^{M}L$. Suppose that for any $m \in M$, $f(m) = k$ and $g(m) = l$ for some $k \in K$ and $l \in L$. Define $H(\langle f, g\rangle)$ to be the function whose value at $m$ is $\langle k, l\rangle$. We claim that $H$ is a bijection between $A = {}^{M}K \times {}^{M}L$ and $B = {}^{M}(K \times L)$.
We first show that $H$ is injective. Let $\langle f, g\rangle$ and $\langle f', g'\rangle$ be ordered pairs in $A$. Choose $m \in M$ such that $f(m) \neq f'(m)$ and $g(m) \neq g'(m)$. Then we have that

$$H(\langle f, g\rangle)(m) = \langle m, \langle f(m), g(m)\rangle\rangle \neq \langle m, \langle f'(m), g'(m)\rangle\rangle = H(\langle f', g'\rangle)(m)$$

In other words, $\langle f, g\rangle \neq \langle f', g'\rangle$ and thus $H$ is injective.
We now show that $H$ is surjective. Let $b \in B$. We need to exhibit an ordered pair $a \in A$ such that $H(a) = b$. We know that $b$ is a function that maps an element $m \in M$ to an ordered pair $\langle k, l\rangle \in K \times L$. With this information, we can define the ordered pair $a = \langle f, g\rangle$ such that $f(m) = k$ and $g(m) = l$. We can see that $a \in A$. Indeed, $f \in {}^{M}K$ and $g \in {}^{L}K$ and thus $a = \langle f, g\rangle \in A$. Hence $H$ is surjective.

Part 8: We have that $(\kappa^\lambda)^\mu = \left|{}^{M}({}^{L}k)\right|$ and $\kappa^{\lambda\cdot\mu} = \left|{}^{(L\times M)}K\right|$. Hence we must show that ${}^{M}({}^{L}k) \approx {}^{(L\times M)}K$. Let $f \in {}^{M}({}^{L}k)$. Consider the function $H(f)$ whose value at $\langle l, m\rangle$ equals to the value of the function $f(m)$ at $l$. We claim that $H$ is a bijection between $A = {}^{M}({}^{L}k)$ and $B = {}^{(L\times M)}K$.
We first show that $H$ is a bijection. Let $f \neq g$ be functions in $A$. Then for some $m$, the functions $f(m) \neq g(m)$. Therefore, for some $l, f(m)(l) \neq g(m)(l)$. Hence

$$H(f)(l, m) = f(m)(l) \neq g(m)(l) = H(g)(l, m)$$

whence $H(f) \neq H(g)$.
We now show that $H$ is surjective. Consider any $j \in B$. Then $j = H(f)$

where, for some $m \in M$, $f(m)$ is the function whose value at $l \in L$ is $j(l, m)$. □

**Theorem 6.23.** *Let $m$ and $n$ be finite cardinal numbers. Then*

1. $m + n = m +_\omega n$
2. $m \cdot n = m \cdot_\omega n$
3. $m^n = m^n$

*where the operations on the right hand side is understood to be the operations introduced on the natural numbers in Chapter 4 and the operations on the left hand side are the operations of cardinal arithmetic.*

*Proof.* We first claim that the following identities hold (for any finite cardinals $\kappa$ and $\lambda$): (they are either trivial or follow directly from the previous theorem)

$$\kappa + 0 = \kappa \tag{a1}$$
$$\kappa + (\lambda + 1) = (\kappa + \lambda) + 1 \tag{a2}$$
$$\kappa \cdot 0 = 0 \tag{m1}$$
$$\kappa \cdot (\lambda + 1) = \kappa \cdot \lambda + \kappa \tag{a2}$$
$$\kappa^0 = 1 \tag{e1}$$
$$\kappa^{\lambda+1} = \kappa^\lambda \cdot \kappa \tag{e2}$$

Now let $n$ be a finite cardinal. We claim that $n + 1 = n^+$. We have that

$$n + 1 = |n \cup \{ n \}| = \left|n^+\right| = n^+$$

as required. We now define the set

$$T = \{ n \in \omega \mid m + n = m +_\omega n \}$$

for some fixed $m \in \omega$. We claim that $T$ is inductive. Then $0 \in T$ since $n + 0 = n = n +_\omega 0$ by (a1) and (A1). Now let $k \in T$. We have that

$$\begin{aligned} m + k^+ &= m + (k + 1) \\ &= (m + k) + 1 && \text{by (a2)} \\ &= (m +_\omega k) + 1 && \text{since } k \in T \\ &= (m +_\omega k)^+ \\ &= (m +_\omega k^+) && \text{by (A2)} \end{aligned}$$

and thus $k^+ \in T$ whence $T$ is inductive and $T = \omega$. The argumentation is exactly the same for multiplication and exponentiation. □

**Corollary 6.24.** *Let $A$ and $B$ be finite sets. Then $A \cup B, A \times B$ and ${}^B A$ are also finite.*

*Proof.* This follows directly by converting cardinal arithmetic to that of the natural numbers. □

## 6.4 Ordering Cardinal Numbers

**Definition 6.25.** *Let $A$ and $B$ be sets. We say that $A$ is **dominated** by $B$, denoted $A \preceq B$, if there exists an injective function from $A$ into $B$.*

**Example 6.26.** *Let $A$ be a set. Then it follows trivially that $A \preceq A$ by considering the bijective identity map betweeen $A$ and itself.*

**Example 6.27.** *Let $B$ be a set and $A \subset B$ be a subset. Then $A \preceq B$ since the identity function maps $A$ bijectively into $B$. More generally, We have that $A \preceq B$ if $A$ is equinumerous to some subset of $B$.*

**Definition 6.28.** *Let $A$ and $B$ be sets. Then we define the ordering relation $\leq$ on their cardinalities as follows:*

$$|A| \leq |B| \iff A \preceq B$$

**Lemma 6.29.** *Let $K, K', L, L'$ be sets. Suppose that $\kappa = |K| = |K'|$ and $\lambda = |L| = |L'|$. Then*

$$K \preceq L \iff K' \preceq L'$$

*Proof.* We first note that $K \approx K'$ and $L \approx L'$ since their cardinalities are equal. Hence there exist bijections between $K$ and $K'$ and between $L$ and $L'$. Since $K \preceq L$, there is an injective map from $K$ into $L$. Composing these three functions, we get an injective map from $K'$ into $L'$. □

**Definition 6.30.** *Let $\kappa$ and $\lambda$ be cardinals. We define the relation $<$ on these numbers as follows:*

$$\kappa < \lambda \iff \kappa \leq \lambda \wedge \kappa \neq \lambda$$

*In terms of sets, this is equivalent to*

$$|K| < |L| \iff K \preceq L \wedge K \neq L$$

**Example 6.31.** *1. Let $A \subseteq B$. Then $|A| \leq |B|$. Conversely, whenever $\kappa < \lambda$, then there exists sets $K \subseteq L$ with $|K| = \kappa$ and $|L| = \lambda$.*

*2. Let $K$ be a cardinal. We have that $0 \leq \kappa$.*

*3. Let $n$ be a finite cardinal. We have that $n < \aleph_0$. For any two finite cardinals $m$ and $n$, we have that*

$$m \in n \implies m \subseteq n \implies m \leq n$$

*In addition, the converse also holds. Indeed if $m \leq n$ then $m \preceq n$ and there is an injective function $f : m \to n$. By the pigeonhole principle, it is impossible to have $n$ less than $m$ so by trichotomy, $m \in n$. Hence the ordering on finite cardinals agrees with the ordering we defined in Chapter 4.*

*4. Let $\kappa$ be a cardinal. Then $\kappa < 2^\kappa$. Indeed if $A$ is any set of cardinality $\kappa$ then $\mathcal{P}A$ has cardinality $2^\kappa$. Then $A \preceq \mathcal{P}A$ by the map $x \mapsto \{ x \}$. But by Cantor's theorem, $A \not\approx \mathcal{P}A$ and thus $\kappa < 2^\kappa$. This shows that there is no largest cardinal number.*

**Theorem 6.32.** *Scröder-Bernstein Theorem*
*Let $A$ and $B$ be sets and $\kappa$ and $\lambda$ cardinals. We have that*

*1. If $A \preceq B$ and $B \preceq A$ then $A \approx B$*

*2. If $\kappa \leq \lambda$ and $\lambda \leq \kappa$ then $\kappa = \lambda$*

*Proof.* By the definition of domination, we have injective functions $f : A \to B$ and $g : B \to A$. Consider the set $C_0 = A \backslash ran\, g$. If $C_0 = \varnothing$ then $g$ is surjective and hence a bijection and we are done. Therefore we may assume $C_0$ is non-empty. We now define recursively the following sets:

$$C_{n^+} = g\, [\![ f\, [\![ C_n ]\!] ]\!]$$

We claim that

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

is a bijection from $A$ to $B$. Note that in the second case, $x \notin C_0$ and thus $x \in ran\, g$ so $g^{-1}$ makes sense.

We first show that $h$ is injective. Define $D_n = f[\![C_n]\!]$ so that $C_{n^+} = g[\![D_n]\!]$. Consider $x \neq x'$ in $A$. Since both $f$ and $g^{-1}$ are injective, the only possible problem arises when $x \in C_m$ and $x' \notin \bigcup_{n\in\omega} C_n$. In this case, we have that

$$h(x) = f(x) \in D_m$$

whereas

$$h(x') = g^{-1}(x) \notin D_m$$

lest $x' \in C_{m+}$. Hence $h(x) \neq h(x')$.
We now show that $h$ is surjective. Obviously, each $D_n \subseteq ran\, h$ since $D_n = h[\![C_n]\!]$. Now consider a point $y \in B \setminus \bigcup_{n\in\omega} D_n$. We can see that $g \not\in C_0$ by definition. Furthermore, $g(y) \notin C_{n^+}$ since $C_{n^+} = g[\![D_n]\!], y \notin D_n$ and $g$ is injective. Hence $g(y) \notin C_n$ for any $n$. Hence $h(g(y)) = g^{-1}(g(y)) = y$. □

**Example 6.33.**

1. *If $A \subseteq B \subseteq C$ and $A \approx C$ then all three sets are equinumerous.*
2. *The set of real numbers is equinumerous to the closed interval $[0, 1]$ since*

$$(0, 1) \subseteq [0, 1] \subseteq \mathbb{R}$$

3.

$$\kappa \leq \lambda < \mu \implies \kappa < \mu$$
$$\kappa < \lambda \leq \mu \implies \kappa < \mu$$

**Theorem 6.34.** *The set of real numbers is equinumerous to ${}^{\omega}2$ and thus equinumerous to $\mathcal{P}\omega$.*

*Proof.* We shall show that $\mathbb{R} \preceq {}^{\omega}2$ and ${}^{\omega}2 \preceq \mathbb{R}$ and then apply the Scröder-Bernstein Theorem.

$\preceq$: We shall construct an injective function from the open interval $(0, 1)$ into ${}^{\omega}2$. The existence of such a function together with the fact that $\mathbb{R} \approx (0, 1)$ will lead to $\mathbb{R} \preceq {}^{\omega}2$. We shall make use of the binary digit expansions of real numbers. We define a function such that the real number whose binary expansion is $0.1100010\ldots$ is mapped to the function in ${}^{\omega}2$ whose successive

values are $1, 1, 0, 0, 0, 1, 0, \ldots$. In general, for a real number $z \in (0, 1)$, let $H(z)$ be the function $H(z) : \omega \to 2$ whose value at $n$ equals the $(n+1)st$ binary digit in the binary expansion of $z$. Clearly $H$ is injective.

$\succeq$: We follow a similar argumentation for the converse. The function in ${}^{\omega}2$ whose successive values are $1, 1, 0, 0, 0, 1, 0, \ldots$ is mapped to the real number with decimal expansion $0.1100010\ldots$. This maps ${}^{\omega}2$ injectively into the closed interval $[0, \frac{1}{9}$.

□

**Remark.** *The previous theorem shows us that* $|\mathbb{R}| = 2^{\aleph_0}$. *Consequently, the plane* $\mathbb{R}^2$ *has cardinality*

$$2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$$

**Theorem 6.35.** *Let* $\kappa, \lambda$ *and* $\mu$ *be cardinal numbers. Then*

1. $\kappa \leq \lambda \implies \kappa + \mu \leq \lambda + \mu$
2. $\kappa \leq \lambda \implies \kappa \cdot \mu \leq \lambda \cdot \mu$
3. $\kappa \leq \lambda \implies \kappa^{\mu} \leq \lambda^{\mu}$
4. $\kappa \leq \lambda \implies \mu^{\kappa} \leq \mu^{\lambda}$ *if not both* $\kappa$ *and* $\mu$ *equal zero*

*Proof.* Let $K, L$ and $M$ be sets of cardinality $\kappa, \lambda$ and $\mu$ respectively and assume that $\kappa < \mu$. We may thus choose $K$ and $L$ such that $K \subseteq L$ and $M$ such that $L \cap M = \varnothing$. Parts 1,2 and 3 follow immediately since

$$K \cup M \subseteq L \cup M, \qquad K \times M \subseteq L \times M, \qquad {}^{M}K \subseteq {}^{M}L$$

For Part 4, first consider the case when $\mu = 0$. Then by assumption, $\kappa \neq 0$ and $\mu^{\kappa} = 0 \leq \mu^{\lambda}$. Now suppose $\mu \neq 0$. Fix $a \in M$. We need to exhibit an injective function $G$ from ${}^{K}M$ into ${}^{L}M$. Let $f \in {}^{K}M$ and define $G(f)$ to be the function with domain $L$ such that

$$G(f)(x) = \begin{cases} f(x) & \text{if } x \in K \\ a & \text{if } x \in L \backslash K \end{cases}$$

Then $G : {}^{K}M \to {}^{L}M$ and is indeed injective. □

**Example 6.36.** *We can calculate the product* $\aleph_0 \cdot 2^{\aleph_0}$ *as follows:*

$$2^{\aleph_0} \leq \aleph_0 \cdot 2^{\aleph_0} \leq 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$$

*whence equality holds throughout.*

## 6.5 Axiom of Choice

**Definition 6.37.** *Let $\mathcal{A}$ be a set. We say that $\mathcal{A}$ is a chain if for any $B, C \in \mathcal{A}$ then either $B \subseteq C$ or $C \subseteq B$.*

**Theorem 6.38.** *The following statements are equivalent:*

1. *Axiom of Choice I: For any relation $R$, there exists a function $F \subseteq R$ with $\operatorname{dom} F = \operatorname{dom} R$*

2. *Axiom of Choice II: The Cartesian product of nonempty sets is always nonempty. In other words, if $H$ is a function with domain $I$ and if $(\forall\, i \in I) H(i) \neq \varnothing$ then there is a function $f$ with domain $I$ such that $(\forall\, i \in I) f(i) \in H(i)$*

3. *Axiom of Choice III: For any set $A$ there exists a function $F$ (a **choice function** for $A$) such that the domain of $F$ is the set of nonempty subsets of $A$ and such that $F(B) \in B$ for every nonempty $B \subseteq A$.*

4. *Axiom of Choice IV: Let $\mathcal{A}$ be a such such that*

   - *each member of $\mathcal{A}$ is a nonempty set*
   - *any two distinct members of $\mathcal{A}$ are disjoint*

   *Then there exists a set $C$ containing exactly one element from each member of $\mathcal{A}$*

5. *Cardinal Comparability: For any sets $C$ and $D$, either $C \preceq D$ or $D \preceq C$. For any two cardinal numbers $\kappa$ and $\lambda$, either $\kappa \leq \lambda$ or $\lambda \leq \kappa$.*

6. *Zorn's Lemma: Let $\mathcal{A}$ be a set such that for every chain $\mathcal{B} \subseteq \mathcal{A}$, we have that $\bigcup \mathcal{B} \in \mathcal{A}$. Then $\mathcal{A}$ contains an element $M$ (a **maximal** element) such that $M$ is not a subset of any other set in $\mathcal{A}$*

*Proof.*

$1 \implies 2$: Assume that $H$ is a function with domain $I$ such that $H(i) \neq \varnothing$ for all $i \in I$. Define the relation

$$R = \{\, \langle i, x \rangle \mid i \in I \wedge x \in H(i) \,\}$$

Then Statement 1 guarantees the existence of a function $F \subseteq R$ such that $dom\, F = dom\, R$. Since $\langle i, F(i)\rangle \in F \subseteq R$, we must have that $F(i) \in H(i)$. Hence Statement 2 holds.

2 $\implies$ 4: Let $\mathcal{A}$ be a set meeting the two conditions in Statement 4. Define $H$ to be the identity function on $\mathcal{A}$. Then for all $B \subseteq \mathcal{A}$ we have that $H(B) \neq \varnothing$. By Statement 2, there exists a function $f$ with domain $\mathcal{A}$ such that for all $B \in \mathcal{A}, f(B) \in H(B) = B$. Let $C = ran\, f$. Then for $B \in \mathcal{A}$, we have that $B \cap C = \{\, f(B)\,\}$ (nothing else could be in this set by the second condition).

4 $\implies$ 3: Fix a set $A$. Define

$$\mathcal{A} = \{\, \{\, B\,\} \times B \mid B \text{ is a nonempty subset of } A\,\}$$

Then each member of $\mathcal{A}$is nonempty and any two distinct members are disjoint. Indeed if $\langle x, y\rangle \in (\{\, B\,\} \times B) \cap (\{\, B'\,\} \times B)$ then $x = B = B'$. Now let $C$ be a set (whose existence is guaranteed by Statement 4) whose intersection with each member of $\mathcal{A}$ is a singleton:

$$C \cap (\{\, B\,\} \times B) = \{\, \langle B, x\rangle\,\}$$

where $x \in B$. It is possible that $C$ contains extraneous elemebts that do not belong to any member of $\mathcal{A}$. We discard them by letting $F = C \cap (\bigcup \mathcal{A})$. We claim that $F$ is a choice function for $A$. Any member of $F$ belongs to some $\{\, B\,\} \times B$ and hence is of the form $\langle B, x\rangle$ for $x \in B$. For any nonempty subset $B \subseteq A$, there is a unique $x$ such that $\langle B, x\rangle \in F$ since $F \cap (\{\, B\,\} \times B)$ is a singleton. This $x$ is just $F(B)$ and is a member of $B$ and thus Statement 3 holds.

3 $\implies$ 1: Let $R$ be a relation.Then Statement 3 guarantees the existence of a choice function $G$ for $ran\, R$. Hence $G(B) \in B$ for any nonempty subset $B$ of $ran\, R$. Define a function $F$ with $dom\, F = dom\, R$ by

$$F(x) = G(\{\, y \mid xRy\,\})$$

Then $F(x) \in \{\, y \mid xRy\,\}$ whence $\langle x, F(x)\rangle \in R$. Thus $F \subseteq R$.

6 $\implies$ 1: Fix a relation $R$. We need to exhibit a function $F \subseteq R$ such that $dom\, F = dom\, R$. Consider the set

$$\mathcal{A} = \{\, f \subseteq R \mid f \text{ is a function}\,\}$$

We shall apply Zorn's Lemma to $A$ in order to find such a function $F$. We must first check that $\mathcal{A}$ is closed under unions of chains. Let $\mathcal{B} \subseteq \mathcal{A}$ be a chain. Since every member of $\mathcal{B}$ is a subset of $R$,$\bigcup \mathcal{B}$ is a subset of $R$. We must show that $\bigcup \mathcal{B}$ is a function. Suppose $\langle x, y\rangle, \langle x, z\rangle \in \bigcup \mathcal{B}$. Then we have that $\langle x, y\rangle \in G \in \mathcal{B}$ and $\langle x, z\rangle \in H \in \mathcal{B}$ for some functions $G$ and $H$ in $\mathcal{B}$. Since $\mathcal{B}$ is a chain, we must have that either $G \subseteq H$ or $H \subseteq G$. In either event, both $\langle x, y\rangle$ and $\langle x, z\rangle$ belong to the same function and thus $y = z$. Thus $\bigcup \mathcal{B} \in \mathcal{A}$.
Now, Zorn's Lemma guarantees us the existence of a maximal function $F$ in $\mathcal{A}$. We claim that $dom\, F = dom\, R$. Suppose that $x \in dom\, R \backslash dom\, F$. Since $x \in dom\, R$, by definition there is some $y$ such that $xRy$. Define

$$F' = F \cup \{ \langle x, y\rangle \}$$

Then $F' \in \mathcal{A}$, contradicting the maximality of $F$. Hence $dom\, F = dom\, R$.

6 $\implies$ 5: Let $C$ and $D$ be any sets. We shall show that either $C \preceq D$ or $D \preceq C$. Define

$$\mathcal{A} = \{ f \mid f \text{ is an injective function } \wedge dom\, f \subseteq C \wedge ran\, f \subseteq D \}$$

Let $\mathcal{B} \subseteq \mathcal{A}$ be a chain. We know from the previous proof that $\bigcup \mathcal{B}$ is a function. We must now show that it is injective. Let $\langle x, y\rangle, \langle x', y\rangle \in \bigcup \mathcal{B}$ (where $x$ and $x'$ are understood to be distinct elements of $C$). We have that there exist injective functions $G$ and $H$ such that $\langle x, y\rangle \in G \in \mathcal{B}$ and $\langle x', y\rangle \in H \in \mathcal{B}$. Since $\mathcal{B}$ is a chain, we must have that either $G \subseteq H$ or $H \subseteq G$. Suppose, without loss of generality, that the first case holds. Then $\langle x, y\rangle, \langle x', y\rangle \in H$. But $H$ is an injective function so $x = x'$. Finally, consider $\langle x, y\rangle \in \bigcup \mathcal{B}$. Then $\langle x, y\rangle \in f \in \mathcal{A}$ whence $x \in C$ and $y \in D$. It therefore follows that $dom \bigcup \mathcal{B} \subseteq C$ and $ran \bigcup \mathcal{B} \subseteq D$. Hence we may, and do, apply Zorn's Lemma to $\mathcal{A}$.
Let $\hat{f}$ be the maximal function in $\mathcal{A}$ whose existence is guaranteed by Zorn's Lemma. We claim that either $dom\, \hat{f} = C$ (in which case, $C \preceq D$) or $ran\, \hat{f} = D$ (in which case $D \preceq C$ since $f^{-1}$ is an injective function from $D$ into $C$). Suppose, for a contradiction, that neither condition holds. Then there exists elements $c \in C \backslash dom\, \hat{f}$ and $d \in D \backslash ran\, \hat{f}$. It then follows that

$$f' = \hat{f} \cup \{ \langle c, d\rangle \}$$

is in $\mathcal{A}$, contradicting the maximality of $\hat{f}$.

The proof of this theorem is completed in Chapter 7. $\square$

**Theorem 6.39.** *Let $A$ be an infinite set. Then $\omega \preceq A$. In other words, $\aleph_0 \leq \kappa$ for any infinite cardinal $\kappa$.*

*Proof.* Fix an infinite set $A$. The idea of the proof is to select $\aleph_0$ elements from $A$. Let $F$ be the choice function for $A$ whose existence is guaranteed by the Axiom of Choice III. Define, by recursion, the function $h$ such that

$$\begin{aligned} h(0) &= \varnothing \\ h(n^+) &= h(n) \cup \{ F(A \backslash h(n)) \} \end{aligned}$$

We thus start with $\varnothing$ and successively add chosen new elements from $A$. $A \backslash h(n)$is nonempty since $A$ is finite and $h(n)$ is a finite subset. We may then define the following function

$$g(n) = F(A \backslash h(n))$$

where $g$ is a function from $\omega$ to $A$. We must show that $g$ is injective.
Suppose that $m \neq n$. By trichotomy, we must have that one number is less than the other, say $m \in n$. Then $m^+ \subseteq n$ and so

$$g(m) \in h(m^+) \subseteq h(n)$$

But $g(n) \notin h(n)$ since

$$g(n) = F(A \backslash h(n)) \in A \backslash h(n)$$

hence $g(m) \neq g(n)$. □

**Corollary 6.40.** *A set is infinite if and only if it is equinumerous to a proper subset of itself.*

*Proof.* One implication in this theorem was proven in Corollary 6.12 where we showed that if a set is equinumerous to a proper subset of itself, then it is infinite.
Conversely, consider an infinite set $A$. Then by the previous theorem, there exists an injective function $f$ from $\omega$ into $A$. Define a function $g$ from $A$ into $A$ by

$$\begin{aligned} g(f(n)) &= f(n^+) && \text{for } n \in \omega \\ g(x) &= x && \text{for } x \notin ran\, f \end{aligned}$$

then $g$ is a bijection between $A$ and $A \backslash \{ f(0) \}$. □

## 6.6 Countable Sets

**Definition 6.41.** *Let $A$ be a set. We say that $A$ is **countable** if $A \preceq \omega$. In other words, $|A| \leq \aleph_0$.*

**Example 6.42.** *$\omega, \mathbb{Z}, \mathbb{Q}$ are all countable sets. However, $\mathbb{R}$ is uncountable.*

**Example 6.43.** *Let $A$ and $B$ be countable sets. Then $C = A \cup B$ is countable as its cardinality $|C| \leq \aleph_0 + \aleph_0 = \aleph_0$. $D = A \times B$ is also countable as $|D| = \leq \aleph_0 \cdot \aleph_0 = \aleph_0$.*

**Theorem 6.44.** *The countable union of countable sets is necessarily countable. In other words, if $\mathcal{A}$ is countable and every member of $\mathcal{A}$ is countable then $\bigcup \mathcal{A}$ is countable.*

*Proof.* We may first suppose that $\varnothing \notin \mathcal{A}$ since its presence does not affect set union. We may further suppose that $\mathcal{A} \neq \varnothing$ since $\bigcup \varnothing$ is indeed countable. Thus $\mathcal{A}$ is a countable collection of non-empty sets. We shall construct a function from $\omega \times \omega$ onto $\bigcup \mathcal{A}$. Since we know that there exists functions from $\omega$ onto $\omega \times \omega$, the composition will map $\omega$ onto $\bigcup \mathcal{A}$ whence $\bigcup \mathcal{A}$ is countable.
Since $\mathcal{A}$ is countable but non-empty, there exists a function $G$ from $\omega$ onto $\mathcal{A}$:

$$\mathcal{A} = \{\, G(0), G(1), \dots \}$$

By assumption, each set $G(m)$ is countable and non-empty. Hence for each $m$, there is a function from $\omega$ onto $G(m)$. We shall use the axiom of choice to select a suitable function for each $m$. Consider the function $H : \omega \to {}^{\omega}(\bigcup \mathcal{A})$ defined by

$$H(m) = \{\, g \mid g \text{ is a function from } \omega \text{ onto } G(m) \,\}$$

Obviously, $H(m)$ is non-empty for each $m \in \omega$. By the axiom of choice, there exists a function $F$ with domain $\omega$ such that for each $m \in \omega$, $F(m)$ is a function from $\omega$ onto $G(m)$. We can now define $f(m, n) = F(m)(n)$ which is a function from $\omega \times \omega$ onto $\bigcup \mathcal{A}$. □

**Example 6.45.** *Let $A$ be a set. We define a **sequence** in $A$ to be a function from some natural number into $A$. Let $Sq(A)$ be the set of all sequences in $A$:*

$$\begin{aligned} Sq(A) &= \{\, f \mid (\exists\, n \in \omega) f \text{ maps } n \text{ into } A \,\} \\ &= {}^0A \cup {}^1A \cup {}^2A \cup \dots \end{aligned}$$

We define the **length** of a sequence to be its domain.
$Sq(A)$ is indeed a valid set as if $f : n \to A$ then

$$f \subseteq n \times A \subseteq \omega \times A$$

whence $f \in \mathcal{P}(\omega \times A)$. Hence $Sq(A) \subseteq \mathcal{P}(\omega \times A)$.
We now have the following:

1. $Sq(\omega)$ has cardinality $\aleph_0$. Indeed, consider any $f \in Sq(\omega)$ and let $n$ be its length. Then define

   $$H(f) = 2^{f(0)+1} \cdot 3^{f(1)+1} \dots p_{n-1}^{f(n-1)+1}$$

   where $p_i$ is the $(i+1)st$ prime (if the length of $f$ is 0 then $H(f) = 1$). Hence $H : Sq(\omega) \to \omega$ and, by the fundamental theorem of arithmetic, $H$ is injective. Hence $Sq(\omega) \leq \aleph_0$. The opposite inequality follows trivially.

2. $Sq(A)$ is countable for any countable set $A$. Since $A$ is countable, there exists an injective function $g$ from $A$ into $\omega$. This function naturally induces an injective mapping from $Sq(A)$ into $Sq(\omega)$. Hence $|Sq(A)| \leq |Sq(\omega)| = \aleph_0$.

3. There are $\aleph_0$ algebraic numbers. We first note that the set $\mathbb{Z}$ of integers has cardinality $\aleph_0 + \aleph_0 = \aleph_0$. We next calculate the cardinality of the set of polynomials $P$ with integer coeffcients. To each polynomial (of degree n), we may assign a sequence (of length $n + 1$) consisting of its coefficients. This defines an injective mapping from $P$ into $Sq(\mathbb{Z})$ which is a countable set. Hence $P$ is countable. Since each polynomial in $P$ has only finitely many roots, the set of algebraic numbers is a countable union of finite sets. Therefore, the algebraic numbers are countable. Since the set of algebraic numbers is infinite, it must have cardinality $\aleph_0$.

4. There are uncountably many transcendental numbers. Since the set of algebraic numbers is countable, the set of transcendental numbers cannot be countable, lest the set $\mathbb{R}$ is countable.

## 6.7 Arithmetic of Infinite Cardinals

**Lemma 6.46.** *Let $\kappa$ be an infinite cardinal. Then $\kappa \cdot \kappa = \kappa$.*

*Proof.* Let $B$ be a set of cardinality $\kappa$. It suffices to show that $B \times B \approx B$. Define

$$\mathcal{H} = \{\, f \mid f = \varnothing \text{ or for some infinite } A \subseteq B, f \text{ is a bijection between } A \times A \text{ and } A \,\}$$

We shall use Zorn's Lemma to obtain a maximal function $f_0$ in $\mathcal{H}$.
We must first check that $\mathcal{H}$ is closed under unions of chains. Let $\mathcal{C}$ be a chain in $\mathcal{H}$. We may assume that $\mathcal{C}$ contains some non-empty function else $\bigcup \mathcal{C} = \varnothing \in \mathcal{H}$. From previous results, we know that $\bigcup \mathcal{C}$ is an injective function. Define the set

$$A = \bigcup \{\, ran\, f \mid f \in \mathcal{C} \,\} = ran \bigcup \mathcal{C}$$

$A$ is infinite since $\mathcal{C}$ contains some non-empty function. We claim that $\bigcup \mathcal{C}$ is a bijection between $A \times A$ and $A$. It hence suffices to show that $dom\, \mathcal{C} = A \times A$. Let $\langle a_1, a_2 \rangle \in A \times A$. Then $a_1 \in ran\, f_1$ and $a_2 \in ran\, f_2$ for some $f_1, f_2 \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, we have that $f_1 \subseteq f_2$ or $f_2 \subseteq f_1$. Without loss of generality, we may assume that $f_1 \subseteq f_2$. Then

$$\langle a_1, a_2 \rangle \in ran\, f_2 \times ran\, f_2 = dom\, f_2 \subseteq \bigcup \{\, dom\, f \mid f \in \mathcal{C} \,\} = dom \bigcup \mathcal{C}$$

Conversely, any member of $dom \bigcup \mathcal{C}$ belongs to $dom\, f$ for some $f \in \mathcal{C}$. But $dom\, f = ran\, f \times ran\, f \subseteq A \times A$. Hence $dom \bigcup \mathcal{C} = A \times A$ whence $\bigcup \mathcal{C}$ is a bijection between $A \times A$ and $A$.
Zorn's Lemma now guarantees the existence of a maximal $f_0 \in \mathcal{H}$. We must first check that $f_0 \neq \varnothing$. Since $B$ is infinite, it has a subset $A$ of cardinality $\aleph_0$. Since $\aleph_0 \times \aleph_0 = \aleph_0$, there is a bijection $g$ between $A \times A$ and $A$. Hence $g \in \mathcal{H}$. Since $g$ has more elements than $\varnothing$, it follows that $\varnothing$ can not be a maximal element of $\mathcal{H}$. Hence, by the definition of $\mathcal{H}$, $f_0$ is a bijection between $A_0 \times A_0$ and $A_0$ where $A_0$ is some infinite subset of $B$.
Now let $\lambda = |A_0|$. Then $\lambda$ is infinite and $\lambda \times \lambda = \lambda$. We shall now show that $\lambda = \kappa$ and that $B \backslash A_0$ necessarily has smaller cardinality.
Suppose that $\lambda \leq |B \backslash A_0|$. Then $B \backslash A_0$ has a subset $D$ of cardinality $\lambda$. We shall show that this contradicts the maximality of $f_0$ by extending $f_0$ to a bijection between the sets $(A_0 \cup D) \times (A_0 \cup D)$ and $A_0 \cup D$. We have that

$$(A_0 \cup D) \times (A_0 \cup D) = (A_0 \times A_0) \cup (A_0 \times D) \cup (D \times A_0) \cup (D \times D)$$

$A_0 \times A_0$ is already in bijection with $A_0$ by $f_0$. The remainder

$$(A_0 \times D) \cup (D \times A_0) \cup (D \times D) \tag{6.1}$$

has cardinality

$$\begin{aligned} \lambda \cdot \lambda + \lambda \cdot \lambda + \lambda \times \lambda &= \lambda + \lambda + \lambda \\ &= 3 \cdot \lambda \\ &\leq \lambda \times \lambda \\ &= \lambda \end{aligned}$$

Hence there exists a bijection between (6.1) and $D$. It follows that $f_0 \cup g \in \mathcal{H}$ and properly extends $f_0$, contradicting the maximality of $f_0$. Thus $|B \backslash A_0| < \lambda$.
Now

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

whence $\lambda = \kappa$. Hence $\kappa \cdot \kappa = \kappa$. □

**Theorem 6.47.** *Absorption Law of Cardinal Arithmetic*
*Let $\kappa$ and $\lambda$ be cardinal numbers, the larger of which is infinite and the smaller of which is nonzero. Then*

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

*Proof.* Without loss of generality, we may assume that $\lambda \leq \kappa$. Then

$$\kappa \leq \kappa + \lambda \leq \kappa + \kappa = 2 \cdot \kappa \leq \kappa \times \kappa = \kappa$$

and

$$\kappa \leq \kappa \times \lambda \leq \kappa \times \kappa = \kappa$$

Hence equality holds throughout. □

**Example 6.48.** *The operation of subtraction for infinite cardinal numbers is not well defined. If one starts with $\aleph_0$ objects and removes $\aleph_0$ objects then the number of remaining objects can be anywhere from 0 to $\aleph_0$. However, if one starts with $\kappa$ (where $\kappa$ is infinite) objects and removes $\lambda$ objects (where $\lambda$ is strictly less than $\kappa$) then exactly $\kappa$ objects remain. To see this, let $\mu$ be the cardinality of the remaining objects. Then $\kappa = \lambda + \mu = \max(\lambda, \mu)$ whence $\kappa = \mu$*

**Example 6.49.** *There are $2^{\aleph_0}$ transcendental numbers. This follows from the previous example. If from $2^{\aleph_0}$ real numbers one removes $\aleph_0$ algebraic numbers, then $2^{\aleph_0}$ numbers remain.*

**Example 6.50.** *For any infinite cardinal $\kappa$, we have that $\kappa^\kappa = 2^\kappa$. Indeed*

$$\kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa\cdot\kappa} = 2^\kappa \leq \kappa^\kappa$$

*whence equality holds throughout.*

**Example 6.51.** *The cardinality of ${}^{\mathbb{R}}\mathbb{R}$ is $2^{2^{\aleph_0}}$. Indeed, the cardinal number of the set is*

$$(2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0\cdot 2^{\aleph_0}} = 2^{2^{\aleph_0}}$$

*We now want to consider the cardinality of the real valued continuous functions. Denote the continuous functions in ${}^{\mathbb{R}}\mathbb{R}$ by $C(\mathbb{R})$. It is easy to see that*

$$2^{\aleph_0} \leq |C(\mathbb{R})| \leq 2^{2^{\aleph_0}}$$

*We claim that $|C(\mathbb{R})| = 2^{\aleph_0}$. First consider the map*

$$\begin{aligned} h : C(\mathbb{R}) &\to {}^{\mathbb{Q}}\mathbb{R} \\ f &\mapsto f|_{\mathbb{Q}} \end{aligned}$$

*We claim that $h$ is an injective mapping. Let $f, g \in C(\mathbb{R})$ be distinct functions. Then $f - g$ is not identically zero. It follows that, since $f$ and $g$ are continuous, there exists an open interval upon which $f - g$ is nonzero. Such an interval must contain a rational number and hence*

$$h(f) = f|_{\mathbb{Q}} \neq g|_{\mathbb{Q}} = h(g)$$

*and hence $h$ is injective. It follows that $C(\mathbb{R}) \preceq {}^{\mathbb{Q}}\mathbb{R}$ whence*

$$|C(\mathbb{R})| \leq \left|{}^{\mathbb{Q}}\mathbb{R}\right| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$$

*Therefore $|C(\mathbb{R})| = 2^{\aleph_0}$.*

## 6.8 Continuum Hypothesis

The continuum hypothesis asserts that there does not exist sets of cardinality $\kappa$ such that $\aleph_0 < \kappa < 2^{\aleph_0}$. It was proved by Gödel in 1939 that the hypothesis could not be disproved. In 1963, Cohen showed that the hypothesis can not be proved from the Zermelo-Fraenkel axioms either. It is therefore undecidable.

The generalised continuum hypothesis asserts that for any infinite cardinal $\kappa$, there does not exist a cardinal number $\lambda$ such that $\kappa < \lambda < 2^{\kappa}$.

# Chapter 7

# Orderings and Ordinals

## 7.1 Partial Orderings

**Definition 7.1.** *Let $R$ be a relation. We say that $R$ is a* ***partial ordering*** *if the following two conditions are met:*

- *$R$ is a transitive relation:*

$$xRy \wedge yRz \implies xRz$$

- *$R$ is irreflexive:*

$$\textit{It is never the case that } xRx$$

**Example 7.2.** *Let $S$ be a set. Define $\subset_S$ to be the relation of strict inclusion on subsets of $S$:*

$$\subset_S = \{\, \langle A, B\rangle \mid A \subseteq B \subseteq S \wedge A \neq B \,\}$$

*Then $\subset_S$ is a partial ordering.*

**Example 7.3.** *Let $P$ be the set of positive integers. The strict divisibility relation on $P$ is*

$$\{\, \langle a, b\rangle \in P \times P \mid a \cdot q = b \textit{ for some } q \neq 1 \,\}$$

**Theorem 7.4.** *Let $<$ be a partial ordering. Then, given any $x, y$ and $z$, we have that*

1. *At most one of the three following alternatives can hold:*

$$x < y, \qquad x = y, \qquad y < x$$

2. $x \leq y \leq x \implies x = y$

*Proof.*

Part 1: Suppose we had both $x < y$ and $x = y$. Then we would have that $x < x$, contradicting irreflexivity. If both $x < y$ and $y < x$ then, by transitivity, we conclude that $x < x$, again contradicting reflexivity.

Part 2: Suppose that $x \neq y$. Then we would have that $x < y < x$, contradicting Part 1.

□

**Definition 7.5.** *A **structure** is a pair $\langle A, R \rangle$ consisting of a set $A$ and a binary relation $R$ on $A$.*

**Remark.** *In particular, we can speak of a **partially ordered structure** (or **linearly**) if $R$ is a partial (or linear) ordering relation on $A$. These are sometimes referred to as **posets** (or **losets**).*

**Definition 7.6.** *Let $<$ be a partial ordering and $D$ a set. An element $m$ of $D$ is said to be a **minimal** element of $D$ if for all $x \in D, x \not< m$. $m$ is a **least** element of $D$ if $m \leq x$ for all $x \in D$. A least element is necessarily minimal.*
*Similar definitions apply to **maximal** and **greatest** elements.*

**Remark.** *For a linear ordering on a set that includes $D$, the two concepts coincide since*

$$x \not< m \implies m \leq x$$

*In the nonlinear case, minimality is weaker than leastness.*

**Example 7.7.** *Consider the strict divisibility relation on the set $P$ of positive integers. Then $1$ is the least element of $P$. But let $D = \{\, a \in P \mid a \neq 1 \,\}$. Then every prime is a minimal element of $D$ and $D$ has no least element.*

**Definition 7.8.** *Let $<$ be a partial ordering on a set $A$ and consider a subset $C \subseteq A$. An **upper bound** of $C$ is an element $b \in A$ such that $x \leq b$ for all $x \in C$. If $b \in C$ then $b$ is the greatest element of $C$.*
*If $b$ is the least element of the set of all upper bounds for $C$ then $b$ is the **least upper bound** (or **supremum**) of $C$. Similar definitions apply to **lower bounds** and **greatest lower bounds** (or **infimums**)*

**Example 7.9.** *Consider a set $S$ and the partial ordering $\subset_S$ on $\mathcal{P}(S)$. For $A$ and $B$ in $\mathcal{P}(S)$, the set $\{ A, B \}$ has the least upper bound $A \cup B$. Similarly, $A \cap B$ is the greatest lower bound. If $\mathcal{A} \subseteq \mathcal{P}(S)$ then $\bigcup \mathcal{A}$ is the least upper bound of $\mathcal{A}$ and $\bigcap \mathcal{A}$ is the greatest lower bound.*

**Example 7.10.** *Consider the set $\{ x \in \mathbb{Q} \mid x^2 < 2 \}$. This set has upper bounds in $\mathbb{Q}$ but it has no least upper bound in $\mathbb{Q}$.*

## 7.2 Well Orderings

**Definition 7.11.** *A **well ordering** on a set $A$ is a linear ordering on $A$ such that every nonempty subset of $A$ has a least element.*

**Example 7.12.** *The usual ordering on $\omega$ is a well ordering.*

**Theorem 7.13.** *Let $<$ be a linear ordering on $A$. Then $A$ is a well ordering if and only if there does not exist a function $f : \omega \to A$ such that $f(n^+) < f(n)$ for all $n \in \omega$.*

*Proof.* We shall refer to a function satisfying the conditions of the theorem as a **descending chain**.

$\Longrightarrow$ : Let $f$ be a descending chain. Then $ran\, f$ is a nonempty subset of $A$. Clearly, $ran\, f$ has no least element. Indeed, for each element $f(n)$, there is a smaller element $f(n^+)$. Hence $<$ cannot be a well ordering.

$\Longleftarrow$ : Assume that $<$ is not a well ordering on $A$. By definition, some nonempty subset $B \subseteq A$ lacks a least element. Then $(\forall\, x \in B)(\exists\, y \in B) y < x$. Fix $x \in B$ and define a function $f : \omega \to B$ recursively as follows:

$$f(0) = x$$
$$f(n^+) = y$$

where $y \in B$ is chosen such that $y < f(n)$ (the existence of which is always guaranteed by the fact that $B$ lacks a least element). Then $f$ is a descending chain with $f(n^+) < f(n)$ for all $n \in \omega$.

□

**Definition 7.14.** *Let $A$ be a set and $<$ any kind of ordering on $A$. Then the set*

$$\operatorname{seg} t = \{\, x \mid x < t \,\}$$

*is called the* ***initial segment up to t****.*

**Example 7.15.** *Let $n \in \omega$ (with the usual $\in$ ordering). Then*

$$\operatorname{seg} n = \{\, x \mid x \in n \,\} = n$$

**Theorem 7.16.** *Transfinite Induction Principle*
*Let $<$ be a well ordering on $A$. Let $B \subseteq A$ be a subset and assume that for every $t \in A$,*

$$\operatorname{seg} t \subseteq B \implies t \in B$$

*Then $B$ coincides with $A$.*

*Proof.* Suppose that $B$ is a proper subset of $A$. Then $A \backslash B$ has a least element $m$. By leastness, $y \in B$ for any $y < m$. But this is equivalent to $\operatorname{seg} m \subseteq B$ and thus $m \in B$. □

**Definition 7.17.** *Let $A$ be a set and $B \subseteq A$ a subset. We say that $B$ is a $<$-inductive subset of $A$ if and only if it has the property that for every $t \in A$,*

$$\operatorname{seg} t \subseteq B \implies t \in B$$

**Remark.** *We can now reformulate the transfinite induction principle as follows: If $<$ is a well ordering on $A$ then any $<$-inductive subset of $A$ must coincide with $A$.*

**Theorem 7.18.** *Let $<$ be a linear ordering on $A$. Assume that the only $<$-inductive subset of $A$ is $A$ itself. In other words, assume that for any $B \subseteq A$ satisfying the condition*

$$(\forall\, t \in A)(\operatorname{seg} t \subseteq B \implies t \in B) \tag{7.1}$$

*we have that $B = A$. Then $<$ is a well ordering on $A$.*

*Proof.* Let $C$ be a subset of $A$. We claim that either $C$ has a least element or $C$ is empty. Consider the following set of strict lower bounds of $C$:

$$B = \{\, t \in A \mid t < x \forall\, x \in C \,\}$$

First note that $B \cap C = \varnothing$, lest $t < t$. We now have two cases:

Condition (7.1) does not hold for $B$: In this case, there exists some $t \in A$ such that $\operatorname{seg} t \subseteq B$ but $t \notin B$. We claim that $t$ is a least element of $C$. Since $t \notin B$, there exists some $x \in c$ with $x \leq t$. But $x$ cannot belong to $\operatorname{seg} t$ which is disjoint from $C$. Thus $x = t$ is a least element of $C$.

Condition (7.1) holds for $B$: By hypothesis, $A = B$ whence $C = \varnothing$.

□

**Definition 7.19.** *Let $A$ be a well ordered set and $G$ a function on $A$ whose value at $t \in A$ is dependent on all values $G(x)$ for $x < t$. We say that a function $F$ is* ***G-constructed*** *if, given $t \in A$, the following holds:*

$$F(t) = G(F|_{\operatorname{seg} t})$$

**Remark.** *For the right hand side of the above equation to be valid, the domain of the function $G$ must contain all functions of the form $F|_{\operatorname{seg} t}$.*

**Definition 7.20.** *We define the set ${}^{<A}B$ to be the set of all functions from initial segments of $<$ into $B$:*

$${}^{<A}B = \{\, f \mid \text{ for some } t \in A, f \text{ is a function from } \operatorname{seg} t \text{ into } B \,\}$$

**Remark.** *Note that if $f : \operatorname{seg} t \to B$ then $f \subseteq A \times B$. Hence ${}^{<A}B$ is obtainable by applying applying a suitable subset axiom to $\mathcal{P}(A \times B)$.*

**Theorem 7.21.** *Transfinite Recursion Theorem, Preliminary Form*
*Let $<$ be a well ordering on a set $A$. Furthermore, let $G : {}^{<A}B \to B$. Then there exists a unique function $F : A \to B$ such that, given any $t \in A$,*

$$F(t) = G(F|_{\operatorname{seg} t})$$

**Example 7.22.** *Consider the well ordered natural numbers $\omega$. We have for each $n \in \omega$ the equation $\operatorname{seg} n = n$. Hence the transfinite recursion theorem asserts the existence of a unique $F : \omega \to B$ such that, for all $n \in \omega$,*

$$F(n) = G(F|_n)$$

*In particular:*

$$F(0) = G(F|_0) = G(\varnothing)$$
$$F(1) = G(F|_1) = G(\{\, \langle 0, F(0)\rangle \,\})$$
$$F(2) = G(F|_2) = G(\{\, \langle 0, F(0)\rangle \,, \langle 1, F(1)\rangle \,\})$$