Introduction to Set Theory

A Solution Manual for Hrbacek and Jech (1999)

Jianfei Shen

School of Economics, The University of New South Wales

Sydney, Australia

The Lord by wisdom founded the earth, by understanding he established the heavens.

— Proverbs 3:19

Contents

Preface

Sydney, *Jianfei Shen*
Date

Acknowledgements

1

SETS

1.1 Introduction to Sets

No exercises.

1.2 Properties

No exercises.

1.3 The Axioms

► Exercise 1 (1.3.1). *Show that the set of all x such that $x \in A$ and $x \notin B$ exists.*

Proof. Notice that

$$\{x : x \in A \text{ and } x \notin B\} = \{x \in A : x \notin B\} .$$

Then by the Axiom Schema of Comprehension, we know that such a set does exist. □

► Exercise 2 (1.3.2). *Replace The Axiom of Existence by the following weaker postulate:*

Weak Axiom of Existence*: Some set exists.*

Prove the Axiom of Existence using the Weak Axiom of Existence and the Comprehension Schema.

Proof. Let A be a set known to exist. By the Axiom Schema of Comprehension, there is a set X such that

$$X = \{x \in A : x \neq x\} .$$

There is no subjects x satisfying $x \neq x$, so there is no elements in X, which proves the Axiom of Existence. □

► EXERCISE 3 (1.3.3). a. *Prove that a "set of all sets" does not exist.*

b. *Prove that for any set A there is some $x \notin A$.*

PROOF. **(a)** Suppose that there exists a *universe* set (a set of all sets) $\mathcal{V}$. Then by the Axiom Schema of Comprehension, there is a *set* $B = \{x \in \mathcal{V} : x \notin x\}$; that is

$$x \in B \iff x \in \mathcal{V} \text{ and } x \notin x. \tag{1.1}$$

Now we show that $B \notin \mathcal{V}$, that is, B is not a set. Indeed, if $B \in \mathcal{V}$, then either $B \in B$, or $B \notin B$. If $B \in B$, then, by the "$\Longrightarrow$" direction of (1.1), $B \in V$ and $B \notin B$. A contradiction; if $B \notin B$, then, by the "$\Longleftarrow$" direction of (1.1), the assumption $B \in \mathcal{V}$ and $B \notin B$ yield $B \in B$. A contradiction again. This completes the proof that $B \notin \mathcal{V}$.

(b) If there were a set A such that $x \in A$ for all x, then A is "a set of all sets", which, as we have proven, does not exist. □

► EXERCISE 4 (1.3.4). *Let A and B be sets. Show that there exists a unique set C such that $x \in C$ if and only if either $x \in A$ and $x \notin B$ or $x \in B$ and $x \notin A$.*

PROOF. Let A and B be sets. The following two sets exist:

$$C_1 = \left\{x : x \in A \text{ and } x \notin B\right\} = \left\{x \in A : x \notin B\right\},$$
$$C_2 = \left\{x : x \notin A \text{ and } x \in B\right\} = \left\{x \in B : x \notin A\right\}.$$

Then $C = C_1 \cup C_2$ exists by the Axiom of Union. The uniques of C follows from the Axiom of Extensionality. □

► EXERCISE 5 (1.3.5). a. *Given A, B, and C, there is a set P such that $x \in P$ iff $x = A$ or $x = B$ or $x = C$.*

b. *Generalize to four elements.*

PROOF. **(a)** By the Axiom of Pair, there exist two sets: $\{A, B\}$ and $\{C, C\} = \{C\}$. By the Axiom of Union, there exists set P satisfying $P = \{A, B\} \cup \{C\} = \{A, B, C\}$.

(b) Suppose there are four sets A, B, C, and D. Then the Axiom of Pair implies that there exist $\{A, B\}$ and $\{C, D\}$, and the Axiom of Union implies that there exists

$$P = \{A, B\} \cup \{C, D\} = \{A, B, C, D\}.$$ □

► EXERCISE 6 (1.3.6). *Show that $\mathcal{P}(X) \subseteq X$ is false for any X. In particular, $\mathcal{P}(X) \neq X$ for any X. This proves again that a "set of all sets" does not exist.*

PROOF. Let X be an arbitrary set; then there exists a set $Y = \{u \in X : u \notin u\}$. Obviously, $Y \subseteq X$, so $Y \in \mathcal{P}(X)$ by the Axiom of Power Set. If $Y \in X$, then we have $Y \in Y$ if and only if $Y \notin Y$ [See Exercise 3(a)]. This proves that $\mathcal{P}(X) \nsubseteq X$, and $\mathcal{P}(X) \neq X$ by the Axiom of Extensionality. □

► EXERCISE 7 (1.3.7). *The Axiom of Pair, the Axiom of Union, and the Axiom of Power Set can be replaced by the following weaker versions.*

Weak Axiom of Pair *For any A and B, there is a set C such that $A \in C$ and $B \in C$.*

Weak Axiom of Union *For any S, there exists U such that if $X \in A$ and $A \in S$, then $X \in U$.*

Weak Axiom of Power Set *For any set S, there exists P such that $X \subseteq S$ implies $X \in P$.*

Prove the Axiom of Pair, the Axiom of Union, and the Axiom of Power Set using these weaker versions.

PROOF. We just prove the first axiom. By the Weak Axiom of Pair, for any A and B, there exists a set C' such that $A \in C'$ and $B \in C'$. Now by the Axiom Schema of Comprehension, there is a set C such that $C = \{x \in C' : x = A \text{ or } x = B\}$. □

1.4 ELEMENTARY OPERATIONS ON SETS

► EXERCISE 8 (1.4.1). *Prove all the displayed formulas in this section and visualize them using Venn diagrams.*

PROOF. Omitted. □

► EXERCISE 9 (1.4.2). *Prove*

a. $A \subseteq B$ *if and only if* $A \cap B = A$ *if and only if* $A \cup B = B$ *if and only if* $A \smallsetminus B = \varnothing$.

b. $A \subseteq B \cap C$ *if and only if* $A \subseteq B$ *and* $A \subseteq C$.

c. $B \cup C \subseteq A$ *if and only if* $B \subseteq A$ *and* $C \subseteq A$.

d. $A \smallsetminus B = (A \cup B) \smallsetminus B = A \smallsetminus (A \cap B)$.

e. $A \cap B = A \smallsetminus (A \smallsetminus B)$.

f. $A \smallsetminus (B \smallsetminus C) = (A \smallsetminus B) \cup (A \cap C)$.

g. $A = B$ *if and only if* $A \Delta B = \varnothing$.

PROOF. **(a)** We first prove that $A \subseteq B \implies A \cap B = A$. Suppose $A \subseteq B$. Note that $A \cap B \subseteq A$ is clear since $a \in A \cap B \implies a \in A$ and $a \in B \implies a \in A$. To prove $A \subseteq A \cap B$ under the assumption that $A \subseteq B$, notice that $[a \in A] \wedge [A \subseteq B] \implies [a \in A] \wedge [a \in B] \implies a \in A \cap B$. Hence, $A \subseteq B \implies A \cap B = A$. To see $A \cap B = A \implies A \subseteq B$, note that $A = A \cap B \implies A \subseteq A \cap B \implies [A \subseteq A] \wedge [A \subseteq B] \implies A \subseteq B$.

To see $A \subseteq B \implies A \cup B = B$, notice first that $B \subseteq A \cup B$ holds trivially. Hence, we need only to show $A \cup B \subseteq B$. But this is true because $[a \in A \cup B] \wedge [A \subseteq B] \implies [a \in A \vee a \in B] \wedge [a \in A \implies a \in B] \implies a \in B$. The direction $A \cup B = B \implies A \subseteq B$ holds because $A \cup B = B \implies A \cup B \subseteq B \implies A \subseteq B$.

$A \subseteq B \implies A \smallsetminus B = \varnothing$ holds by definition of difference of sets: $A \smallsetminus B := \left\{x \in A \,\middle|\, x \notin B\right\}$. By this definition, if $A \subseteq B$ and $a \in A$, then $a \in B$, which contradicts the requirement $a \notin B$; hence, $A \smallsetminus B = \varnothing$ when $A \subseteq B$. To prove $A \smallsetminus B = \varnothing \implies A \subseteq B$, we use its false antecedent. Suppose $B \subsetneq A$. Then there exists $a \in A$ and $a \notin B$ since B is a proper subset of A, but which means that $A \smallsetminus B \neq \varnothing$.

(b) If $A \subseteq B \cap C$, then $a \in A \implies a \in B \cap C \implies [a \in B] \wedge [a \in C]$. The other direction is just by definition.

(c) To see $B \cup C \subseteq A \implies B \subseteq A$ and $C \subseteq A$, let $a \in B$ $[a \in C]$, then $a \in B \cup C \subseteq A$ $[a \in B \cup C \subseteq A]$. To prove the inverse direction, let $a \in B$ or $a \in C$; that is, $a \in B \cup C$. But $B \subseteq A$ and $C \subseteq A$, we have $a \in A$, too.

(d) To prove $A \smallsetminus B = (A \cup B) \smallsetminus B$, notice that $a \in (A \cup B) \smallsetminus B \iff [a \in A \vee a \in B] \wedge \left[a \notin B\right] \iff [a \in A] \wedge \left[a \notin B\right] \iff a \in A \smallsetminus B$. To prove $A \smallsetminus B = A \smallsetminus (A \cap B)$, notice that

$$\begin{aligned} a \in A \smallsetminus (A \cap B) &\iff [a \in A] \wedge \left[\neg\,(a \in A \cap B)\right] \\ &\iff [a \in A] \wedge \left[\neg\,(a \in A \wedge a \in B)\right] \\ &\iff [a \in A] \wedge \left[a \notin A \vee a \notin B\right] \\ &\iff [a \in A] \wedge \left[a \notin B\right] \\ &\iff a \in A \smallsetminus B. \end{aligned}$$

(e) $a \in A \smallsetminus (A \smallsetminus B) \iff [a \in A] \wedge \left[\neg\,(a \in A \smallsetminus B)\right] \iff [a \in A] \wedge \left[a \notin A \vee a \in B\right] \iff [a \in A] \wedge [a \in B] \iff a \in A \cap B$.

(f) First, $a \in A \smallsetminus (B \smallsetminus C)$ iff $[a \in A] \wedge \left[\neg\,(a \in B \smallsetminus C)\right]$ iff $[a \in A] \wedge \left[a \notin B \vee a \in C\right]$. Then, $a \in (A \smallsetminus B) \cup (A \cap C) \iff \left[a \in A \wedge a \notin B\right] \vee [a \in A \wedge a \in C] \iff [a \in A] \wedge \left[a \notin B \vee a \in C\right]$.

(g) $A = B \iff [A \subseteq B] \wedge [B \subseteq A] \overset{(a)}{\iff} [A \smallsetminus B = \varnothing] \wedge [B \smallsetminus A = \varnothing] \iff (A \smallsetminus B) \cup (B \smallsetminus A) = \varnothing \iff A \Delta B = \varnothing$. □

► EXERCISE 10 (1.4.3). *Omitted.*

▶ Exercise 11 (1.4.4). *Let A be a set; show that a "complement" of A does not exist.*

Proof. Suppose A^c exists. Then, by the Axiom of Union, there is a set $V = A \cup A^c$. But in this case, V is a universe. A contradiction [See Exercise 3 (a)]. □

▶ Exercise 12 (1.4.5). *Let $S \neq \varnothing$ and A be sets.*

a. *Set $T_1 = \{Y \in \mathcal{P}(A) \colon Y = A \cap X$ for some $X \in S\}$, and prove $A \cap \bigcup S = \bigcup T_1$ (generalized distributive law).*

b. *Set $T_2 = \{Y \in \mathcal{P}(A) \colon Y = A \smallsetminus X$ for some $X \in S\}$, and prove $A \smallsetminus \left(\bigcup S\right) = \bigcap T_2$, $A \smallsetminus \left(\bigcap S\right) = \bigcup T_2$ (generalized De Morgan laws).*

Proof. **(a)** $x \in A \cap \bigcup S$ iff $x \in A$ and there is $X \in S$ such that $x \in X$ iff there exists $X \in S$ such that $x \in A \cap X$ iff $x \in T_1$.

(b) We have

$$\begin{aligned}
x \in A \smallsetminus \left(\bigcup S\right) &\iff [x \in A] \wedge \left[\neg\left(x \in \bigcup S\right)\right] \\
&\iff [x \in A] \wedge \left[\neg\left(\exists\, X \in S \text{ such that } x \in X\right)\right] \\
&\iff [x \in A] \wedge \left[x \notin X \ \forall\ X \in S\right] \\
&\iff \left[x \in A \wedge x \notin X\right]\ \forall\ X \in S \\
&\iff [x \in A \smallsetminus X]\ \forall\ X \in S \\
&\iff x \in \bigcap (A \smallsetminus X) \\
&\iff x \in \bigcap T_2,
\end{aligned}$$

and

$$\begin{aligned}
x \in A \smallsetminus \left(\bigcap S\right) &\iff [x \in A] \wedge \left[\neg\left(x \in \bigcap S\right)\right] \\
&\iff [x \in A] \wedge \left[\neg\left(x \in X\ \forall\ X \in S\right)\right] \\
&\iff [x \in A] \wedge \left[\exists\, X \in S \text{ such that } x \notin X\right] \\
&\iff \exists\, X \in S \text{ such that } \left[x \in A \wedge x \notin X\right] \\
&\iff \exists\, X \in S \text{ such that } [x \in A \smallsetminus X] \\
&\iff x \in \bigcup (A \smallsetminus X) \\
&\iff x \in \bigcup T_2.
\end{aligned}$$

□

▶ Exercise 13 (1.4.6). *Prove that $\bigcap S$ exists for all $S \neq \varnothing$. Where is the assumption $S \neq \varnothing$ used in the proof?*

Proof. If $S \neq \varnothing$, we can take a set $A \in S$. Let $\mathbf{P}(x)$ denote "$x \in X$ for all $X \in S$". Then

$$\bigcap S = \{x \in A : \mathbf{P}(x)\}$$

exists by the Axiom Schema of Comprehension.

But if $S = \varnothing$, then $\bigcap S$ is a "set of all sets"; that is, $x \in \bigcap \varnothing$ for all x. Suppose not, then there must exist a set $A \in \varnothing$ such that $x \notin A$, but obviously we cannot find such a set A. □

Remark. While $\bigcap \varnothing$ is not defined, we do have

$$\bigcup \varnothing = \varnothing.$$

Suppose not, then there exists $x \in \bigcup \varnothing$, that is, there exists $A \in \varnothing$ such that $x \in A$. Now consider the antecedent

$$x \notin A \quad \forall\, A \in \varnothing. \tag{1.2}$$

Obviously (1.2) cannot hold since there does not exist such a set $A \in \varnothing$. We thus prove that $\bigcup \varnothing = \varnothing$.

2

RELATIONS, FUNCTIONS, AND ORDERINGS

2.1 Ordered Pairs

▶ Exercise 14 (2.1.1). *Prove that* $(a,b) \in \mathcal{P}(\mathcal{P}(\{a,b\}))$ *and* $a,b \in \bigcup(a,b)$*. More generally, if* $a \in A$ *and* $b \in A$*, then* $(a,b) \in \mathcal{P}(\mathcal{P}(A))$*.*

Proof. Notice that $(a,b) = \big\{\{a\},\{a,b\}\big\}$, and $\mathcal{P}(\{a,b\}) = \big\{\varnothing,\{a\},\{b\},\{a,b\}\big\}$. Therefore, $(a,b) \subset \mathcal{P}(\{a,b\})$ and so $(a,b) \in \mathcal{P}\left(\mathcal{P}(\{a,b\})\right)$. Further, $\bigcup(a,b) = \bigcup\big\{\{a\},\{a,b\}\big\} = \{a,b\}$; hence, $a,b \in \bigcup(a,b)$.

If $a \in A$ and $b \in A$, then $\{a\} \subseteq A$ and $\{a,b\} \subseteq A$. Then $\{a\} \in \mathcal{P}(A)$ and $\{a,b\} \in \mathcal{P}(A)$; that is, $\big\{\{a\},\{a,b\}\big\} \subseteq \mathcal{P}\left(\{A\}\right)$. Then by the Axiom of Power Set, $(a,b) = \big\{\{a\},\{a,b\}\big\} \in \mathcal{P}(\mathcal{P}(A))$. □

Remark. If $a \in A$ and $b \in B$, then $(a,b) \in \mathcal{P}(\mathcal{P}(\{A \cup B\}))$.

Proof. We have $\{a\} \subseteq A \subseteq A \cup B$, $\{b\} \subseteq A \cup B$, and $\{a,b\} \subseteq A \cup B$. Then $\{a\},\{a,b\} \in \mathcal{P}(A \cup B)$; that is, $\{\{a\},\{a,b\}\} \subseteq \mathcal{P}(A \cup B)$. Hence, $(a,b) = \{\{a\},\{a,b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. □

▶ Exercise 15 (2.1.2). *Prove that* (a,b)*,* (a,b,c)*, and* (a,b,c,d) *exist for all* a,b,c*, and* d*.*

Proof. By The Axiom of Pair, both $\{a\} = \{a,a\}$ and $\{a,b\}$ exist. Then, use this axiom once again, we know $(a,b) = \{\{a\},\{a,b\}\}$ exists. Since $(a,b,c) = ((a,b),c)$, it follows that the ordered triple exists. (a,b,c,d) exists because $(a,b,c,d) = ((a,b,c),d)$. □

▶ Exercise 16 (2.1.3). *Prove: If* $(a,b) = (b,a)$*, then* $a = b$*.*

Proof. Let $(a,b) = (b,a)$, that is, $\big\{\{a\},\{a,b\}\big\} = \big\{\{b\},\{a,b\}\big\}$. If $a \neq b$, then $\{a\} = \{b\}$, which implies that $a = b$. A contradiction. □

▶ Exercise 17 (2.1.4). *Prove that* $(a,b,c) = (a',b',c')$ *implies* $a = a'$*,* $b = b'$*, and* $c = c'$*. State and prove an analogous property of quadruples.*

PROOF. Note that $(a,b,c) = (a',b',c')$ iff $((a,b),c) = ((a',b'),c')$, iff $(a,b) = (a',b')$ and $c = c'$. Now, $(a,b) = (a',b')$ iff $a = a'$ and $b = b'$. The quadruples case can be easily extended. □

▶ EXERCISE 18 (2.1.5). *Find a, b, and c such that $((a,b),c) \neq (a,(b,c))$. Of course, we could use the second set to define ordered triples, with equal success.*

PROOF. Let $a = b = c$. Then

$$((a,a),a) = \{\{(a,a)\},\{(a,a),a\}\} = \big\{\{\{a\}\},\{\{a\},a\}\big\},$$
$$(a,(a,a)) = \big\{\{a\},\{a,(a,a)\}\big\} = \big\{\{a\},\{a,\{a\}\}\big\}.$$

Thus, $((a,a),a) \neq (a,(a,a))$. Note that while $(A\times B)\times C \neq A\times(B\times C)$ generally, there is a bijection between them. □

▶ EXERCISE 19 (2.1.6). *To give an alternative definition of ordered pairs, choose two different sets $\Box$ and $\triangle$ (for example, $\Box = \varnothing$, $\triangle = \{\varnothing\}$) and define*

$$\langle a,b\rangle = \big\{\{a,\Box\},\{b,\triangle\}\big\}.$$

State and prove an analogue of Theorem 1.2 [p. 18] for this notion of ordered pairs. Define ordered triples and quadruples.

PROOF. We are going to show that

$$\langle a,b\rangle = \langle a',b'\rangle \iff a = a' \text{ and } b = b'.$$

If $a = a'$ and $b = b'$, then $\langle a,b\rangle = \big\{\{a,\Box\},\{b,\triangle\}\big\} = \big\{\{a',\Box\},\{b',\triangle\}\big\} = \langle a',b'\rangle$.

For the inverse direction, let $\big\{\{a,\Box\},\{b,\triangle\}\big\} = \big\{\{a',\Box\},\{b',\triangle\}\big\}$. There are two cases:

- If $a \neq b$, then: (i) If $a = \triangle$ and $b = \Box$ (note that $\Box \neq \triangle$ by assumption), then $\big\{\{a,\Box\},\{b,\triangle\}\big\} = \big\{\{\Box,\triangle\}\big\}$, which enforces $a' = \triangle$ and $b' = \Box$. (ii) If $a \neq \triangle$ or $b \neq \Box$ (or both), then $\{a,\Box\} \neq \{b,\triangle\}$. We first show that it is impossible that $\{a,\Box\} = \{b',\triangle\}$ and $\{b,\triangle\} = \{a',\Box\}$; for otherwise $a = \triangle$ and $b = \Box$. Hence, it must be the case that

  $$\{a,\Box\} = \{a',\Box\} \text{ and } \{b,\triangle\} = \{b',\triangle\},$$

  i.e., $a = a'$ and $b = b'$.

- If $a = b$, then

  $$\big\{\{a,\Box\},\{b,\triangle\}\big\} = \big\{\{a,\Box\},\{a,\triangle\}\big\} = \big\{\{a',\Box\},\{b',\triangle\}\big\}$$

  implies that $\{a,\Box\} = \{a',\Box\}$ and $\{a,\triangle\} = \{b',\triangle\}$; that is, $a = a' = b' = b$. Note that it is impossible that $\{a,\Box\} = \{b',\triangle\}$ and $\{a,\triangle\} = \{a',\Box\}$; for otherwise, $a = \triangle = \Box$. A contradiction. □

2.2 RELATIONS

► EXERCISE 20 (2.2.1). *Let R be a binary relation; let $A = \bigcup\left(\bigcup R\right)$. Prove that $(x, y) \in R$ implies $x \in A$ and $y \in A$. Conclude from this that $\mathfrak{D}_R$ and $\mathfrak{R}_R$ exist.*

PROOF. By the Axiom of Union,

$$\begin{aligned} z \in \bigcup\left(\bigcup R\right) &\iff z \in B \text{ for some } B \in \bigcup R \\ &\iff z \in B \in C \text{ for some } C \in R. \end{aligned}$$

If $(x, y) \in R$, then $C = \{\{x\}, \{x, y\}\} \in R$, $B = \{x, y\} \in C$, and $x, y \in B$; that is, $x \in A$ and $y \in A$. Hence,

$$\mathfrak{D}_R = \left\{x : xRy \text{ for some } y\right\} = \left\{x \in A : xRy \text{ for some } y\right\}.$$

Since $\bigcup\left(\bigcup R\right)$ has been proven exist by the Axiom of Union, the existence of $\mathfrak{D}_R$ follows from the Axiom Schema of Comprehension. The existence of $\mathfrak{R}_R$ can be proved with the same logic. □

► EXERCISE 21 (2.2.2). a. *Show that R^{-1} and $S \circ R$ exist.*

b. *Show that $A \times B \times C$ exist.*

PROOF. (a) Since $R \subseteq \mathfrak{D}_R \times \mathfrak{R}_R$, it follows that $R^{-1} \subseteq \mathfrak{R}_R \times \mathfrak{D}_R$. Since $\mathfrak{D}_R$, $\mathfrak{R}_R$, and $\mathfrak{R}_R \times \mathfrak{D}_R$ exist, we know that R^{-1} exists.

Since $S \circ R = \{(x, z) : (x, y) \in R \text{ and } (y, z) \in S \text{ for some } y\}$, we have $S \circ R \subseteq \mathfrak{D}_R \times \mathfrak{R}_S$. Therefore, $S \circ R$ exists.

(b) Note that $A \times B \times C = (A \times B) \times C$. Since $A \times B$ exists, $(A \times B) \times C$ exists, too. Particularly,

$$A \times B \times C = \left\{(a, b, c) \in \mathcal{P}\left[\mathcal{P}\left[\left(\mathcal{P}(\mathcal{P}(A \cup B))\right) \cup C\right]\right] : a \in A, b \in B, c \in C\right\}. \quad \square$$

► EXERCISE 22 (2.2.3). *Let R be a binary relation and A and B sets. Prove:*

a. $R\left[A \cup B\right] = R[A] \cup R[B]$.

b. $R\left[A \cap B\right] \subseteq R[A] \cap R[B]$.

c. $R\left[A \smallsetminus B\right] \supseteq R[A] \smallsetminus R[B]$.

d. *Show by an example that $\subseteq$ and $\supseteq$ in parts (b) and (c) cannot be replaced by $=$.*

e. *Prove parts (a)—(b) with R^{-1} instead of R.*

f. $R^{-1}\left[R[A]\right] \supseteq A \cap \mathfrak{D}_R$ *and* $R\left[R^{-1}[B]\right] \supseteq B \cap \mathfrak{R}_R$*; give examples where equality does not hold.*

Proof. **(a)** If $y \in R\,[A \cup B]$, then there exists $x \in A \cup B$ such that xRy; that is, either $x \in A$ and xRy, or $x \in B$ and xRy. Hence, $y \in R[A] \cup R[B]$.

Now let $y \in R[A] \cup R[B]$. Then there exists $x \in A$ such that xRy, or there exists $x \in B$ such that xRy. In both case, $x \in A \cup B$, and so $y \in R[A \cup B]$.

(b) If $y \in R[A \cap B]$, then there exists $x \in A \cap B$ such that xRy; that is, there exists $x \in A$ for which xRy, and there exists $x \in B$ for which xRy. Hence, $y \in R[A] \cap R[B]$.

(c) If $y \in R[A] \smallsetminus R[B]$, then there is $x \in A$ such that xRy, but there is no $x' \in B$ such that $x'Ry$. Hence, there exists $x \in A \smallsetminus B$ such that xRy; that is, $y \in R[A \smallsetminus B]$.

(d) Let us consider the following binary relation

$$\bar{R} = \Big\{\big((x,y),(x,0)\big) : (x,y) \in [0,1]^2\Big\};$$

that is, $\bar{R}$ projects the xy-plane onto the x-axis, carrying the point (x,y) into the $(x,0)$; See Figure 2.1.

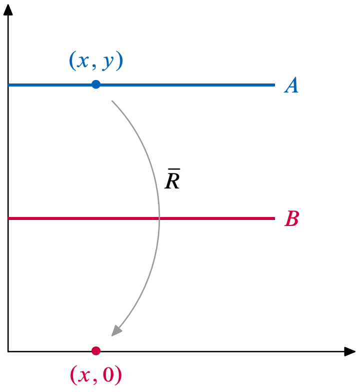

Figure 2.1. $\bar{R}$

- Let $A = \{(x,y) \colon x \in [0,1], y = 1\}$, and $B = \{(x,y) \colon x \in [0,1], y = 1/2\}$. Then $A \cap B = \varnothing$, and consequently, $\bar{R}[A \cap B] = \varnothing$. However, $\bar{R}[A] \cap \bar{R}[B] = [0,1]$.
- Notice that $\bar{R}[A] = \bar{R}[B] = [0,1]$, so $\bar{R}[A] \smallsetminus \bar{R}[B] = \varnothing$. However, $A \smallsetminus B = A$, and consequently, $\bar{R}[A \smallsetminus B] = \bar{R}[A] = [0,1]$.

(e) Just treat R^{-1} as a relation [notice that (a)–(c) hold for an arbitrary binary relation R', so we can let $R^{-1} = R'$].

(f) If $x \in A \cap \mathfrak{D}_R$, then $x \in A$ and there exists $y \in R[A]$ such that $yR^{-1}x$. Hence, $x \in R^{-1}\big[R\,[A]\big]$. To show that the equality does not hold, consider $\bar{R}$ in part (d). Note that $A \cap \operatorname{dom}(\bar{R}) = A$; however, $\bar{R}^{-1}[\bar{R}[A]] = [0,1]^2$.

For the second claim, just notice that R^{-1} is also a binary relation with $\mathfrak{D}_{R^{-1}} = \mathfrak{R}_R$ (see the next exercise). □

► EXERCISE 23 (2.2.4). *Let $R \subseteq X \times Y$. Prove:*

a. $R[X] = \mathfrak{R}_R$ *and* $R^{-1}[Y] = \mathfrak{D}_R$.

b. *If* $a \notin \mathfrak{D}_R$, $R[\{a\}] = \varnothing$; *if* $b \notin \mathfrak{R}_R$, $R^{-1}[\{b\}] = \varnothing$.

c. $\mathfrak{D}_R = \mathfrak{R}_{R^{-1}}$; $\mathfrak{R}_R = \mathfrak{D}_{R^{-1}}$.

d. $(R^{-1})^{-1} = R$.

e. $R^{-1} \circ R \supseteq \mathrm{Id}_{\mathfrak{D}_R}$; $R \circ R^{-1} \supseteq \mathrm{Id}_{\mathfrak{R}_R}$.

PROOF. **(a)** $y \in R[X]$ iff there exists $x \in X$ such that xRy iff $y \in \mathfrak{R}_R$, so $R[X] = \mathfrak{R}_R$. Similarly, $x \in R^{-1}[Y]$ iff there exists $y \in Y$ such that xRy iff $x \in \mathfrak{D}_R$.

(b) Suppose that $R[\{a\}] \neq \varnothing$; let $b \in R[\{a\}]$. But then there exists $b \in \mathfrak{R}_R$ for which aRb; that is, $a \in \mathfrak{D}_R$. A contradiction. Similarly, let $a \in R^{-1}[\{b\}]$. Then aRb; that is, $b \in \mathfrak{R}_R$. A contradiction.

(c) $x \in \mathfrak{D}_R$ iff there exists $y \in Y$ such that xRy, iff there exists $y \in Y$ for which $yR^{-1}x$, iff $x \in \mathfrak{R}_{R^{-1}}$. Similarly, $y \in \mathfrak{R}_R$ iff there exists $x \in X$ such that xRy, iff there exists $x \in X$ such that $yR^{-1}x$, if and only if $y \in \mathfrak{D}_{R^{-1}}$.

(d) For every $(x, y) \in X \times Y$, we have $x(R^{-1})^{-1}y$ iff $yR^{-1}x$ iff xRy. Hence, $(R^{-1})^{-1} = R$.

(e) We have $(x, y) \in \mathrm{Id}_{\mathfrak{D}_R}$ iff $x \in \mathfrak{D}_R$ and $x = y$. We now show that $(x, x) \in R^{-1} \circ R$ for all $x \in \mathfrak{D}_R$. Since $x \in \mathfrak{D}_R$, there exists y such that $(x, y) \in R$, i.e., $(y, x) \in R^{-1}$. Hence, there exists y such that $(x, y) \in R$ and $(y, x) \in R^{-1}$; that is, $(x, x) \in R^{-1} \circ R$.

Now let $(x, y) \in \mathrm{Id}_{\mathfrak{R}_R}$. Then $x = y$ and $y \in \mathfrak{R}_R$. Then there exists x such that $(x, y) \in R$, i.e., $(y, x) \in R^{-1}$. Therefore, $(y, y) \in R \circ R^{-1}$. □

► EXERCISE 24 (2.2.5). *Let* $X = \{\varnothing, \{\varnothing\}\}$, $Y = \mathcal{P}(X)$. *Describe*

a. $\in_Y$;

b. Id_Y.

PROOF. $Y = \mathcal{P}(X) = \Big\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\Big\}$. Then

$$\begin{aligned} \in_Y &= \{(a, b) \colon a \in Y, b \in Y, \text{ and } a \in b\} \\ &= \{(\varnothing, \{\varnothing\}), (\varnothing, \{\varnothing, \{\varnothing\}\}), (\{\varnothing\}, \{\{\varnothing\}\}), (\{\varnothing\}, \{\varnothing, \{\varnothing\}\})\}, \end{aligned}$$

and

$$\begin{aligned} \mathrm{Id}_Y &= \{(a, b) \mid a \in Y, b \in Y, \text{ and } a = b\} \\ &= \{(\varnothing, \varnothing), (\{\varnothing\}, \{\varnothing\}), (\{\{\varnothing\}\}, \{\{\varnothing\}\}), (\{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}\})\}. \end{aligned}$$

□

► EXERCISE 25 (2.2.6). *Prove that for any three binary relations R, S, and T*

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Proof. Let R, S, and T be binary relations. Then

$$\begin{aligned}(w,z) \in T \circ (S \circ R) &\iff \text{there exists } y \text{ for which } w(S \circ R)y, yTz\\ &\iff \text{there exists } y \text{ and } x \text{ for which } wRx, xSy, yTz\\ &\iff \text{there exists } x \text{ for which } x(T \circ S)z, wRx\\ &\iff (w,z) \in (T \circ S) \circ R.\end{aligned}$$ □

► Exercise 26 (2.2.7). *Give examples of sets X, Y, and Z such that*

a. $X \times Y \neq Y \times X$.

b. $X \times (Y \times Z) \neq (X \times Y) \times Z$.

c. $X^3 \neq X \times X^2$ *[i.e., $(X \times X) \times X \neq X \times (X \times X)$].*

Proof. **(a)** Let $X = \{1\}$ and $Y = \{2,3\}$. Then $X \times Y = \{(1,2), (1,3)\}$, but $Y \times X = \{(2,1), (3,1)\}$.

(b) Let $X = \{1\}$, $Y = \{2\}$, and $Z = \{3\}$. Then $X \times (Y \times Z) = \{(1,(2,3))\}$, and $(X \times Y) \times Z = \{((1,2),3)\}$. But $(1,(2,3)) \neq ((1,2),3)$ since $1 \neq (1,2)$ and $(2,3) \neq 3$.

(c) Let $X = \{a\}$. Then $X^3 = \{((a,a),a)\} = \{(\{\{a\}\},a)\}$, but $X \times X^2 = \{(a,(a,a))\} = \{(a,\{\{a\}\})\}$. It is clear that $X^3 \neq X \times X^2$ since $a \neq \{\{a\}\}$. [Remember that $a = (a)$ is an "one-tuple", but $\{\{a\}\} = (a,a)$ is an ordered pair.] □

► Exercise 27 (2.2.8). *Prove:*

a. $A \times B = \varnothing$ *if and only if* $A = \varnothing$ *or* $B = \varnothing$.

b. $(A_1 \cup A_2) \times B = (A_1 \times B) \cup (A_2 \times B)$, *and* $A \times (B_1 \cup B_2) = (A \times B_1) \cup (A \times B_2)$.

c. *Same as part (b), with* $\cup$ *replaced by* $\cap$, $\smallsetminus$, *and* Δ.

Proof. **(a)** $A \times B = \varnothing$ iff $\neg\left[\exists\, a \in A \text{ and } b \in B\right]$ iff $[\nexists\, a \in A] \vee [\nexists\, b \in B]$ iff $A = \varnothing$ or $B = \varnothing$.

(b) We have

$$\begin{aligned}(a,b) \in (A_1 \cup A_2) \times B &\iff a \in A_1 \cup A_2 \text{ and } b \in B\\ &\iff \left[a \in A_1 \text{ and } b \in B\right] \text{ or } \left[a \in A_2 \text{ and } b \in B\right]\\ &\iff \left[(a,b) \in A_1 \times B\right] \text{ or } \left[(a,b) \in A_2 \times B\right]\\ &\iff (a,b) \in (A_1 \times B) \cup (A_2 \times B),\end{aligned}$$

and

$$\begin{aligned}(a,b) \in A \times (B_1 \cup B_2) &\iff a \in A \text{ and } [b \in B_1 \text{ or } b \in B_2]\\ &\iff \left[a \in A \text{ and } b \in B_1\right] \text{ or } \left[a \in A \text{ and } b \in B_2\right]\\ &\iff \left[(a,b) \in A \times B_1\right] \text{ or } \left[(a,b) \in A \times B_2\right]\\ &\iff (a,b) \in (A \times B_1) \cup (A \times B_2).\end{aligned}$$

(c) We just prove the first part.

$$\begin{aligned}(a,b)\in(A_1\cap A_2)\times B &\iff [a\in A_1\wedge a\in A_2]\wedge[b\in B]\\ &\iff [a\in A_1\wedge b\in B]\wedge[a\in A_2\wedge b\in B]\\ &\iff (a,b)\in(A_1\times B)\cap(A_2\times B),\end{aligned}$$

$$\begin{aligned}(a,b)\in(A_1\smallsetminus A_2)\times B &\iff \big[a\in A_1\wedge a\notin A_2\big]\wedge[b\in B]\\ &\iff [a\in A_1\wedge b\in B]\wedge\big[a\notin A_2\big]\\ &\iff \big[(a,b)\in A_1\times B\big]\wedge\big[(a,b)\notin A_2\times B\big]\\ &\iff (a,b)\in(A_1\times B)\smallsetminus(A_2\times B)\,,\end{aligned}$$

and

$$\begin{aligned}(A_1\Delta A_2)\times B &= \big[(A_1\smallsetminus A_2)\cup(A_2\smallsetminus A_1)\big]\times B\\ &= \big[(A_1\smallsetminus A_2)\times B\big]\cup\big[(A_2\smallsetminus A_2)\times B\big]\\ &= \big[(A_1\times B)\smallsetminus(A_2\times B)\big]\cup\big[(A_2\times B)\smallsetminus(A_1\times B)\big]\\ &= (A_1\times B)\Delta(A_2\times B).\end{aligned}$$ □

2.3 Functions

► Exercise 28 (2.3.1). *Prove: If $\Re_f\subseteq\mathfrak{D}_g$, then $\mathfrak{D}_{g\circ f}=\mathfrak{D}_f$.*

Proof. It is clear that $\mathfrak{D}_{g\circ f}=\mathfrak{D}_f\cap f^{-1}[\mathfrak{D}_g]\subseteq\mathfrak{D}_f$. For the other inclusion direction, we have

$$\mathfrak{D}_{g\circ f}=\mathfrak{D}_f\cap f^{-1}[\mathfrak{D}_g]\supseteq\mathfrak{D}_f\cap f^{-1}\big[\Re_f\big]=\mathfrak{D}_f,$$

where we use the fact that $f^{-1}[\Re_f]=\mathfrak{D}_f$:

$$\begin{aligned}x\in f^{-1}\big[\Re_f\big] &\iff \exists\, y\in\Re_f \text{ such that } (y,x)\in f^{-1}\\ &\iff \exists\, y\in\Re_f \text{ such that } (x,y)\in f\\ &\iff x\in\mathfrak{D}_f.\end{aligned}$$ □

► Exercise 29 (2.3.2). *The functions f_i, $i=1,2,3$ are defined as follows:*

$$\begin{aligned}f_1&=\langle 2x-1:x\in\mathbb{R}\rangle\,,\\ f_2&=\Big\langle\sqrt{x}:x>0\Big\rangle,\\ f_3&=\big\langle 1/x:x\in\mathbb{R},x\neq 0\big\rangle.\end{aligned}$$

Describe each of the following functions, and determine their domains and ranges: $f_2\circ f_1$, $f_1\circ f_2$, $f_3\circ f_1$, and $f_1\circ f_3$.

Proof. The domain of $f_2 \circ f_1$ is determined as[1]

$$\begin{aligned}\mathfrak{D}_{f_2 \circ f_1} &= \mathfrak{D}_{f_1} \cap f_1^{-1}\left[\mathfrak{D}_{f_2}\right]\\ &= \mathbb{R} \cap f_1^{-1}\left[\mathbb{R}_{++}\right]\\ &= \{x \in \mathbb{R} \colon x > 1/2\}.\end{aligned}$$

$$\begin{aligned}f_2 \circ f_1 &= \left\{(x,z) : x > 1/2 \text{ and, for some } y, 2x-1 = y \text{ and } \sqrt{y} = z\right\}\\ &= \left\langle \sqrt{2x-1} \colon x > 1/2 \right\rangle.\end{aligned}$$

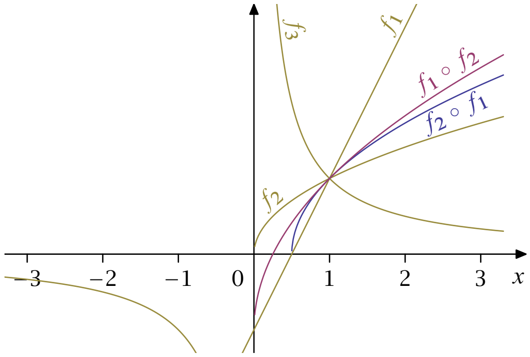

Figure 2.2.

Further, $\mathfrak{D}_{f_1 \circ f_2} = \mathfrak{D}_{f_2} \cap f_2^{-1}\left[\mathfrak{D}_{f_1}\right] = \mathbb{R}_{++} \cap f_2^{-1}[\mathbb{R}] = \mathbb{R}_{++}$, and $f_1 \circ f_2 = \left\langle 2\sqrt{x} - 1 \colon x > 0 \right\rangle$. □

► Exercise 30 (2.3.3). *Prove that the function f_1, f_2, f_3 from Exercise 29 are one-to-one, and find the inverse functions. In each case, verify that $\mathfrak{D}_{f_i} = \mathfrak{R}_{f_i^{-1}}$, $\mathfrak{R}_{f_i} = \mathfrak{D}_{f_i^{-1}}$.*

Proof. As an example, we consider f_2.

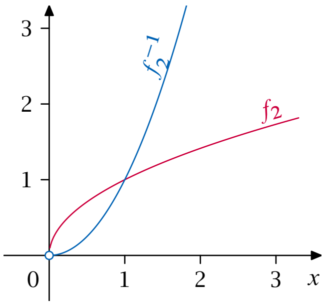

Figure 2.3. f_2 and f_2^{-1}.

[1] Throughout this book, $\mathbb{R}_{++} := \{x \in \mathbb{R} \mid x > 0\}$, and $\mathbb{R}_{+} := \{x \in \mathbb{R} \mid x \geqslant 0\}$.

We have $(x, y) \in f_2^{-1}$ iff $(y, x) \in f_2$ iff $x = \sqrt{y}$ and $y > 0$ iff $y = x^2$ and $x > 0$. □

► EXERCISE 31 (2.3.4). *Prove:*

a. *If f is invertible, $f^{-1} \circ f = \mathrm{Id}_{\mathfrak{D}_f}$, $f \circ f^{-1} = \mathrm{Id}_{\mathfrak{R}_f}$.*

b. *Let f be a function. If there exists a function g such that $g \circ f = \mathrm{Id}_{\mathfrak{D}_f}$ then f is invertible and $f^{-1} = g \restriction \mathfrak{R}_f$. If there exists a function h such that $f \circ h = \mathrm{Id}_{\mathfrak{R}_f}$ then f may fail to be invertible.*

PROOF. **(a)** We have proven in Exercise 23 (e) that [since f is a relation] $f^{-1} \circ f \supseteq \mathrm{Id}_{\mathfrak{D}_f}$ and $f \circ f^{-1} \supseteq \mathrm{Id}_{\mathfrak{R}_f}$; hence, we need only to show the inverse directions. To see $f^{-1} \circ f \subseteq \mathrm{Id}_{\mathfrak{D}_f}$, let $x \in \mathfrak{D}_f$. Then

$$\begin{aligned}(x, y) \in f^{-1} \circ f &\Longrightarrow \exists\, z \text{ such that } (x, z) \in f \text{ and } (z, y) \in f^{-1}\\ &\Longrightarrow \exists\, z \text{ such that } (x, z) \in f \text{ and } (y, z) \in f\\ &\Longrightarrow x = y \text{ since } f \text{ is invertible}\\ &\Longrightarrow (x, y) \in \mathrm{Id}_{\mathfrak{D}_f}.\end{aligned}$$

To see $f \circ f^{-1} \subseteq \mathrm{Id}_{\mathfrak{R}_f}$, let $y \in \mathfrak{R}_f$. Then

$$\begin{aligned}(y, x) \in f \circ f^{-1} &\Longrightarrow \exists\, z \text{ such that } (y, z) \in f^{-1} \text{ and } (z, x) \in f\\ &\Longrightarrow \exists\, z \text{ such that } (z, y) \in f \text{ and } (z, x) \in f\\ &\Longrightarrow y = x\\ &\Longrightarrow (y, x) \in \mathrm{Id}_{\mathfrak{R}_f}.\end{aligned}$$

(b) Suppose that there exists a function g such that $g \circ f = \mathrm{Id}_{\mathfrak{D}_f}$. Let $x, x' \in \mathfrak{D}_f$ with $x \neq x'$. Then $(x, x) \in g \circ f$ and $(x', x') \in g \circ f$. Thus

$$\exists\, y \text{ such that } (x, y) \in f \text{ and } (y, x) \in g, \tag{2.1}$$

$$\exists\, y' \text{ such that } (x', y') \in f \text{ and } (y', x') \in g. \tag{2.2}$$

It follows that $y \neq y'$; for otherwise, by (2.1) and (2.2), we would have $(y, x) \in g$ and $(y, x') \in g$, which contradicts the fact that g is a function.

To see that $f^{-1} = g \restriction \mathfrak{R}_f$, first notice that $g \circ f = \mathrm{Id}_{\mathfrak{D}_f}$ implies that $\mathfrak{D}_f \cap f^{-1}[\mathfrak{D}_g] = \mathfrak{D}_f$, which implies that $\mathfrak{D}_f \subseteq f^{-1}[\mathfrak{D}_g]$, which implies that $f[\mathfrak{D}_f] = \mathfrak{R}_f \subseteq f[f^{-1}[\mathfrak{D}_g] = \mathfrak{D}_g$ since f is invertible. Hence,

$$\mathfrak{D}_{g \restriction \mathfrak{R}_f} = \mathfrak{D}_g \cap \mathfrak{R}_f = \mathfrak{R}_f = \mathfrak{D}_{f^{-1}}.$$

Further, for every $y \in \mathfrak{D}_{f^{-1}}$, there exists x such that $x = f^{-1}(y)$, i.e., $y = f(x)$. Then $g \restriction \mathfrak{R}_f(y) = (g \restriction \mathfrak{R}_f \circ f)(x) = x$. Hence, $g \restriction \mathfrak{R}_f = f^{-1}$.

Finally, as in Figure 2.4, let $f\colon \{x_1, x_2\} \to \{\bar{y}\}$ defined by $f(x_1) = f(x_2) = \bar{y}$. Let $h\colon \{\bar{y}\} \to \{x_1\}$ defined by $h(\bar{y}) = x_1$. Then $f \circ h\colon \{\bar{y}\} \to \{\bar{y}\}$ is given by $(f \circ h)(\bar{y}) = \bar{y}$; that is, $f \circ h = \mathrm{Id}_{\mathfrak{R}_f}$. However, f is not invertible since it is not injective. □

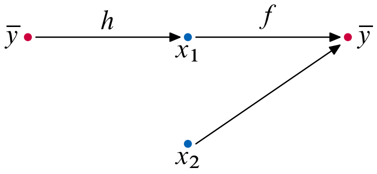

FIGURE 2.4. f is not invertible

► EXERCISE 32 (2.3.5). *Prove: If f and g are one-to-one functions, $g \circ f$ is also a one-to-one function, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

PROOF. Let $x, y \in \mathfrak{D}_{g \circ f}$ and $(g \circ f)(x) = (g \circ f)(y)$. Then $f(x) = f(y)$ since g is injective; then $x = y$ since f is injective. Thus, $g \circ f$ is injective.

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "g \circ f"'] & Y \arrow[d, "g"] \\
 & Z
\end{tikzcd}$$

FIGURE 2.5.

To see that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, notice that

$$\begin{aligned}
(z, x) \in (g \circ f)^{-1} &\iff (x, z) \in g \circ f \\
&\iff \exists\, y \text{ such that } (x, y) \in f \text{ and } (y, z) \in g \\
&\iff \exists\, y \text{ such that } (y, x) \in f^{-1} \text{ and } (z, y) \in g^{-1} \\
&\iff (z, x) \in f^{-1} \circ g^{-1}.
\end{aligned}$$ □

► EXERCISE 33 (2.3.6). *The images and inverse images of sets by functions have the properties exhibited in Exercise 22, but some of the inequalities can now be replaced by equalities. Prove*

a. *If f is a function, $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$.*

b. *If f is a function, $f^{-1}[A \smallsetminus B] = f^{-1}[A] \smallsetminus f^{-1}[B]$.*

PROOF. **(a)** If $x \in f^{-1}[A \cap B]$, then $f(x) \in A \cap B$, so that $f(x) \in A$ and $f(x) \in B$. But then $x \in f^{-1}[A]$ and $x \in f^{-1}[B]$, i.e., $x \in f^{-1}[A] \cap f^{-1}[B]$. Conversely, if $x \in f^{-1}[A] \cap f^{-1}[B]$, then $x \in f^{-1}[A]$ and $x \in f^{-1}[B]$. Therefore, $f(x) \in A$ and $f(x) \in B$, i.e., $f(x) \in A \cap B$. But then $x \in f^{-1}[A \cap B]$.

(b) If $x \in f^{-1}[A \smallsetminus B]$, then $f(x) \in A \smallsetminus B$, so that $f(x) \in A$ and $f(x) \notin B$. But then $x \in f^{-1}[A]$ and $x \notin f^{-1}[B]$, i.e., $x \in f^{-1}[A] \smallsetminus f^{-1}[B]$. Conversely, if

$x \in f^{-1}[A] \smallsetminus f^{-1}[B]$, then $x \in f^{-1}[A]$ and $x \notin f^{-1}[B]$. Therefore, $f(x) \in A$ and $f(x) \notin B$, i.e., $f(x) \in A \smallsetminus B$. But then $x \in f^{-1}[A \smallsetminus B]$. □

► EXERCISE 34 (2.3.7). *Give an example of a function f and a set A such that $f \cap A^2 \neq f \upharpoonright A$.*

PROOF. Let $f(x') = y'$, where $x' \in A$ and $y' \notin A$. Then $(x', y') \in f \upharpoonright A$, but $(x', y') \notin f \cap A^2$. □

► EXERCISE 35 (2.3.8). *Show that every system of sets A can be indexed by a function.*

PROOF. For every system of sets A, consider $\mathrm{Id}\colon A \to A$. Then $A = \{\mathrm{Id}(i)\colon i \in A\}$. □

► EXERCISE 36 (2.3.9). a. *Show that the set B^A exists.*

b. *Let $\langle S_i : i \in I\rangle$ be an indexed system of sets; show that $\prod_{i\in I} S_i$ exists.*

PROOF. **(a)** $f \subseteq A\times B$ for all $f \in B^A$, and so $f \in \mathcal{P}(A\times B)$. Then $B^A \subseteq \mathcal{P}(A\times B)$. Therefore, $B^A = \{f \in \mathcal{P}(A \times B)\colon f\colon A \to B\}$ exists by the Axiom Schema of Comprehension.

(b) By definition, $\prod_{i\in I} S_i = \{f\colon f$ is a function on I and $f_i \in S_i$ for all $i \in I\}$. Hence, for all $f \in \prod_{i\in I} S_i$, if $(i, s_i) \in f$, then $(i, s_i) \in I \times S_i \subseteq I \times \bigcup_{i\in I} S_i$; that is, $f \subseteq I \times \bigcup_{i\in I} S_i$. Hence, $f \in \mathcal{P}(I \times \bigcup_{i\in I} S_i)$ for all $f \in \prod_{i\in I} S_i$, and hence $\prod_{i\in I} S_i \subseteq \mathcal{P}(I \times \bigcup_{i\in I} S_i)$. Therefore, the existence of $\prod_{i\in I} S_i$ follows the Axiom Schema of Comprehension. □

► EXERCISE 37 (2.3.10). *Show that unions and intersections satisfy the following general form of the associative law:*

$$\bigcup_{a\in\bigcup S} F_a = \bigcup_{C\in S}\left(\bigcup_{a\in C} F_a\right), \qquad \bigcap_{a\in\bigcup S} F_a = \bigcap_{C\in S}\left(\bigcap_{a\in C} F_a\right),$$

if S is a nonempty system of nonempty sets.

PROOF. We have

$$\begin{aligned} x \in \bigcup_{a\in\bigcup S} F_a &\iff \exists\, a \in \bigcup S \text{ such that } x \in F_a \\ &\iff \exists\, a \in C \in S, \text{ such that } x \in F_a \\ &\iff x \in \bigcup_{C\in S}\left(\bigcup_{a\in C} F_a\right), \end{aligned}$$

and

$$\begin{aligned} x \in \bigcap_{a \in \bigcup S} F_a &\iff x \in F_a, \forall\, a \in \bigcup S \\ &\iff x \in F_a, \forall\, C \in S, \forall\, a \in C \\ &\iff x \in \bigcap_{C \in S} \left(\bigcap_{a \in C} F_a \right). \end{aligned}$$ □

► EXERCISE 38 (2.3.11). *Other properties of unions and intersections can be generalized similarly.*

De Morgan Laws

$$B \smallsetminus \left(\bigcup_{a \in A} F_a \right) = \bigcap_{a \in A} (B \smallsetminus F_a), \quad B \smallsetminus \left(\bigcap_{a \in A} F_a \right) = \bigcup_{a \in A} (B \smallsetminus F_a).$$

Distributive Laws

$$\begin{aligned} \left(\bigcup_{a \in A} F_a \right) \cap \left(\bigcup_{b \in B} G_b \right) &= \bigcup_{(a,b) \in A \times B} (F_a \cap G_b), \\ \left(\bigcap_{a \in A} F_a \right) \cup \left(\bigcap_{b \in B} G_b \right) &= \bigcap_{(a,b) \in A \times B} (F_a \cup G_b). \end{aligned}$$

PROOF. We have

$$\begin{aligned} x \in B \smallsetminus \left(\bigcup_{a \in A} F_a \right) &\iff [x \in B] \wedge \left[\neg \left(x \in \bigcup_{a \in A} F_a \right) \right] \\ &\iff [x \in B] \wedge \left[\neg \left(\exists\, a \in A \text{ such that } x \in F_a \right) \right] \\ &\iff [x \in B] \wedge \left[\forall\, a \in A\ x \notin F_a \right] \\ &\iff \forall\, a \in A\ \left[x \in B \wedge x \notin F_a \right] \\ &\iff x \in \bigcap_{a \in A} (B \smallsetminus F_a), \end{aligned}$$

and

$$\begin{aligned}
x \in B \setminus \left(\bigcap_{a \in A} F_a \right) &\iff [x \in B] \wedge \left[\neg \left(x \in \bigcap_{a \in A} F_a \right) \right] \\
&\iff [x \in B] \wedge \left[\neg \left(\forall\, a \in A,\ x \in F_a \right) \right] \\
&\iff [x \in B] \wedge \left[\exists\, a \in A \text{ such that } x \notin F_a \right] \\
&\iff \exists\, a \in A \text{ such that } \left[x \in B \wedge x \notin F_a \right] \\
&\iff \exists\, a \in A \text{ such that } [x \in B \setminus F_a] \\
&\iff x \in \bigcup_{a \in A} (B \setminus F_a)\,,
\end{aligned}$$

and

$$\begin{aligned}
x \in \left(\bigcup_{a \in A} F_a \right) \cap \left(\bigcup_{b \in B} G_b \right) &\iff \left[x \in \bigcup_{a \in A} F_a \right] \wedge \left[x \in \bigcup_{b \in B} G_b \right] \\
&\iff \exists\, a \in A \text{ such that } x \in F_a \text{ and} \\
&\ \exists\, b \in B \text{ such that } x \in G_b \\
&\iff \exists\, (a,b) \in A \times B \text{ such that } x \in F_a \cap G_b \\
&\iff x \in \bigcup_{(a,b) \in A \times B} (F_a \cap G_b)\,.
\end{aligned}$$

Finally,

$$\begin{aligned}
x \in \left(\bigcap_{a \in A} F_a \right) \cup \left(\bigcap_{b \in B} G_b \right) &\iff \left[x \in \bigcap_{a \in A} F_a \right] \vee \left[x \in \bigcap_{b \in B} G_b \right] \\
&\iff [\forall\, a \in A,\ x \in F_a] \vee [\forall\, b \in B,\ x \in G_b] \\
&\iff \forall\, (a,b) \in A \times B\ \ [x \in F_a \vee x \in G_b] \\
&\iff x \in \bigcap_{(a,b) \in A \times B} (F_a \cup G_b)\,. \qquad \square
\end{aligned}$$

► Exercise 39 (2.3.12). *Let f be a function. Then*

$$f\left[\bigcup_{a \in A} F_a \right] = \bigcup_{a \in A} f\left[F_a\right], \quad f^{-1}\left[\bigcup_{a \in A} F_a \right] = \bigcup_{a \in A} f^{-1}\left[F_a\right],$$

$$f\left[\bigcap_{a \in A} F_a \right] \subseteq \bigcap_{a \in A} f\left[F_a\right], \quad f^{-1}\left[\bigcap_{a \in A} F_a \right] = \bigcap_{a \in A} f^{-1}\left[F_a\right].$$

If f is one-to-one, then $\subseteq$ in the third formula can be replaced by $=$.

Proof. Let f be a function. Then

$$\begin{aligned} y \in f\left[\bigcup_{a\in A} F_a\right] &\iff \exists\, x \in \bigcup_{a\in A} F_a \text{ such that } (x,y) \in f \\ &\iff \exists\, a \in A,\ \exists\, x \in F_a, \text{ such that } (x,y)\in f \\ &\iff \exists\, a \in A \text{ such that } y \in f\,[F_a] \\ &\iff y \in \bigcup_{a\in A} f\,[F_a], \end{aligned} \tag{2.3}$$

and

$$\begin{aligned} x \in f^{-1}\left[\bigcup_{a\in A} F_a\right] &\iff f(x) \in \bigcup_{a\in A} F_a \\ &\iff \exists\, a \in A \text{ such that } f(x) \in F_a \\ &\iff \exists\, a \in A \text{ such that } x \in f^{-1}\,[F_a] \\ &\iff x \in \bigcup_{a\in A} f^{-1}\,[F_a], \end{aligned} \tag{2.4}$$

and

$$\begin{aligned} y \in f\left[\bigcap_{a\in A} F_a\right] &\iff \exists\, x \in \bigcap_{a\in A} F_a \text{ such that } (x,y) \in f \\ &\iff \forall\, a \in A,\ x \in F_a \text{ such that } (x,y)\in f \quad (*) \\ &\implies \forall\, a \in A,\ y \in f\,[F_a] \quad (**) \\ &\iff y \in \bigcap_{a\in A} f\,[F_a]; \end{aligned} \tag{2.5}$$

hence, $f\left[\bigcap_{a\in A} F_a\right] \subseteq \bigcap_{a\in A} f\,[F_a]$. But if f is not one-to-one, then $(**)$ does not imply $(*)$ in (2.5). For example, let $y \in f[F_1] \cap f[F_2]$, but it is possible that $f(x_1) = f(x_2) = y$, where $x_1 \in F_1$, $x_2 \in F_2$, and $x_1 \neq x_2$. However, if f is one-to-one, then it must be that $x_1 = x_2$. More explicitly, to derive $(*)$ from $(**)$ in (2.5), notice that

$$\begin{aligned} \forall\, a \in A,\ y \in f[F_a] &\implies \exists\,!\, x \in \bigcap_{a\in A} F_a \text{ such that } (x,y) \in f \\ &\iff \forall\, a \in A,\ x \in F_a \text{ such that } (x,y) \in f. \end{aligned}$$

Finally,

$$\begin{aligned} x \in f^{-1}\left[\bigcap_{a\in A} F_a\right] &\iff f(x) \in \bigcap_{a\in A} F_a \\ &\iff \forall\, a \in A,\ f(x) \in F_a \\ &\iff \forall\, a \in A,\ x \in f^{-1}\,[F_a] \\ &\iff x \in \bigcap_{a\in A} f^{-1}\,[F_a]. \end{aligned}$$

□

► EXERCISE 40 (2.3.13). *Prove the following form of the distributive law:*

$$\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right)=\bigcup_{f\in B^A}\left(\bigcap_{a\in A} F_{a,f(a)}\right),$$

assuming that $F_{a,b_1}\cap F_{a,b_2}=\varnothing$ *for all* $a\in A$ *and* $b_1,b_2\in B$, $b_1\neq b_2$.

PROOF. First note that

$$F_{a,f(a)}\subseteq\bigcup_{b\in B} F_{a,b} \tag{2.6}$$

for any $f\in B^A$ since $f\in B^A$ [there exists $b\in B$ such that $b=f(a)$]. Hence

$$\bigcap_{a\in A} F_{a,f(a)}\subseteq\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right) \tag{2.7}$$

follows (2.6), and which proves that

$$\bigcup_{f\in B^A}\left(\bigcap_{a\in A} F_{a,f(a)}\right)\subseteq\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right). \tag{2.8}$$

To prove the inverse direction, pick any $x\in\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right)$. Put $(a,b)\in f$ if and only if $x\in F_{a,b}$. We now need to show that f is a function on A into B. Because $x\in\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right)$, for any $a\in A$,

$$x\in\bigcup_{b\in B} F_{a,b}\iff\exists\, b\in B\text{ such that }x\in F_{a,b};$$

hence, for any $a\in A$, there exists $b\in B$ such that $x\in F_{a,b}$, that is, for any $a\in A$, there exists $b\in B$ such that $(a,b)\in f$, which is just the definition of a function. Since we have proven that $f\in B^A$, we obtain

$$\begin{aligned}
x\in\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right) &\iff \forall\, a\in A,\ x\in\bigcup_{b\in B} F_{a,b}\\
&\iff \forall\, a\in A,\ \exists\, b\in B\text{ such that }x\in F_{a,b}\\
&\Longrightarrow \forall\, a\in A,\ \exists\, f\in B^A\text{ such that }f(a)=b\text{ and }x\in F_{a,f(a)}\\
&\Longrightarrow x\in\bigcap_{a\in A} F_{a,f(a)}\\
&\Longrightarrow x\in\bigcup_{f\in B^A}\left(\bigcap_{a\in A} F_{a,f(a)}\right).
\end{aligned} \tag{2.9}$$

Therefore, (2.8) and (2.9) imply the claim. □

2.4 Equivalences And Partitions

► Exercise 41 (2.4.1). *For each of the following relations, determine whether they are reflexive, symmetric, or transitive:*

a. *Integer x is greater than integer y.*

b. *Integer n divides integer m.*

c. *$x \neq y$ in the set of all natural numbers.*

d. *$\subseteq$ and $\subsetneq$ in $\mathcal{P}(A)$.*

e. *$\varnothing$ in $\varnothing$.*

f. *$\varnothing$ in a nonempty set A.*

Solution. (a) is transitive; (b) is reflexive and transitive; (c) is symmetric; (d): $\subseteq$ is an equivalence relation, but $\subsetneq$ is not reflexive; (e) and (f) are equivalence relations. □

► Exercise 42 (2.4.2). *Let f be a function on A onto B. Define a relation E in A by: aEb if and only if $f(a) = f(b)$.*

a. *Show that E is an equivalence relation on A.*

b. *Define a function φ on A/E onto B by $\varphi([a]_E) = f(a)$ (verify that $\varphi([a]_E) = \varphi([a']_E)$ if $[a]_E = [a']_E$).*

c. *Let j be the function on A onto A/E given by $j(a) = [a]_E$. Show that $\varphi \circ j = f$.*

Proof. **(a)** E is an equivalence relation on A since (i) aEa as $f(a) = f(a)$; (ii) aEb iff $f(a) = f(b)$ iff $f(b) = f(a)$ iff bEa; (iii) Let aEb and bEc; that is, $f(a) = f(b)$ and $f(b) = f(c)$. Then $f(a) = f(c)$ and so aEc.

(b) Let $\varphi([a]_E) = f(a)$ for any $[a]_E \in A/E$. If $[a]_E = [a']_E$, then $a'Ea$. Therefore, $f(a) = f(a')$ by the definition of E. Thus, $\varphi([a]_E) = f(a) = f(a') = \varphi([a']_E)$.

(c) First, $\mathfrak{D}_{\varphi\circ j} = \mathfrak{D}_f = A$ since $\mathfrak{D}_{\varphi\circ j} = \mathfrak{D}_j \cap j^{-1}[\mathfrak{D}_\varphi] = A \cap j^{-1}[A/E] = A$. Next, $(\varphi \circ j)(x) = \varphi([x]_E) = f(x)$ for all $x \in A$. □

► Exercise 43 (2.4.3). *Let $P = \{(r, \gamma) \in \mathbb{R} \times \mathbb{R} : r > 0\}$, where $\mathbb{R}$ is the set of all real numbers. View elements of P as polar coordinates of points in the plane, and define a relation on P by*

$$(r, \gamma) \sim (r', \gamma') \text{ if and only if } r = r' \text{ and } \gamma - \gamma' \text{ is an integer multiple of } 2\pi.$$

Show that $\sim$ is an equivalence relation on P. Show that each equivalence class contains a unique pair (r, γ) with $0 \leqslant \gamma \leqslant 2\pi$. The set of all such pairs is therefore a set of representatives for $\sim$.

Proof. $(r,\gamma) \sim (r,\gamma)$ is obvious: $r = r$ and $\gamma - \gamma = 0 \cdot 2\pi$. To see $\sim$ is symmetric, let $(r,\gamma) \sim (r',\gamma')$; then $r = r'$ and $\gamma - \gamma' = n \cdot 2\pi$, where $n \in \mathbb{Z}$. Therefore, $r' = r$ and $\gamma' - \gamma = (-n) \cdot 2\pi$; that is, $(r',\gamma') \sim (r,\gamma)$. Finally, to see $\sim$ is transitive, let $(r,\gamma) \sim (r',\gamma')$, and $(r',\gamma') \sim (r'',\gamma'')$. In this case, $r = r' = r''$, so $r = r''$, and

$$\gamma - \gamma' = m \cdot 2\pi, \quad \gamma' - \gamma'' = n \cdot 2\pi,$$

where $m, n \in \mathbb{Z}$. But then $\gamma - \gamma'' = (\gamma - \gamma') + (\gamma' - \gamma'') = (m + n) \cdot 2\pi$. Hence, $(r,\gamma) = (r'',\gamma'')$. The above steps show that $\sim$ is an equivalence relation on P.

Consider an arbitrary element of $P/\sim$, say, $[(r',\gamma')]_{\sim}$. Since $\gamma' \in \mathbb{R}$, there must exist γ such that $\gamma' - \gamma = n \cdot 2\pi$, where $n \in \mathbb{Z}$. Then, there exists $\gamma \in \mathbb{R}$ such that $\gamma = \gamma' - n \cdot 2\pi$. Hence, we can find a $\widetilde{n} \in \mathbb{Z}$ satisfying $\gamma'/2\pi - 1 \leqslant \widetilde{n} \leqslant \gamma'/2\pi$, and let $(r,\gamma) = (r', \gamma' - \widetilde{n} \cdot 2\pi)$. □

2.5 Orderings

► Exercise 44 (2.5.1). a. *Let R be an ordering of A, S be the corresponding strict ordering of A, and R^* be the ordering corresponding to S. Show that $R^* = R$.*

b. *Let S be a strict ordering of A, R be the corresponding ordering, and S^* be the strict ordering corresponding to R. Then $S^* = S$.*

Proof. **(a)** Let $(a,b) \in R$, where $a, b \in A$. If $a = b$, then $(a,b) \in R^*$ because orderings are reflexive; if $a \neq b$, then $(a,b) \in S$. But then $(a,b) \in R^*$. Hence, $R \subset R^*$. To see the inverse direction, let $(a,b) \in R^*$. Firstly, $a = b$ implies that $(a,b) \in R$ since R is reflexive. So we suppose $a \neq b$. In this case, $(a,b) \in S$. Because S is R's corresponding strict ordering of A, we know $(a,b) \in S$ if and only if $(a,b) \in R$ and $a \neq b$. Hence, $R^* \subset R$. This proves that $R^* = R$.

(b) Let $(a,b) \in S$, then $a \neq b$. Since R is S's corresponding ordering, we have $(a,b) \in R$. Since $(a,b) \in R$ and $a \neq b$, we have $(a,b) \in S^*$. The revers direction can be proven with the same logic. □

► Exercise 45 (2.5.2). *State the definitions of incomparable elements, maximal, minimal, greatest, and least elements and suprema and infima in terms of strict orderings.*

Solution. If $(P, <)$ is a partially ordered set, X is a nonempty subset of P, and $a \in P$, then:

- a and b are incomparable in $<$ if $a \neq b$ and neither $a < b$ nor $b < a$ holds;
- a is a *maximal* element of X if $a \in X$ and $(\forall\, x \in X)\ a \not< x$;
- a is a *minimal* element of X if $a \in X$ and $(\forall\, x \in X)\ x \not< a$;

- a is the *greatest* element of X if $a \in X$ and $(\forall\ x \in X)\ x \leqslant a$;
- a is the *least* element of X if $a \in X$ and $(\forall\ x \in X)\ a \leqslant x$;
- a is an *upper bound* of X if $(x \in X)\ x \leqslant a$;
- a is a *lower bound* of X if $(\forall\ x \in X)\ a \leqslant x$;
- a is the *supremum* of X if a is the least upper bound of X;
- a is the *infimum* of X if a is the greatest lower bound of X. □

► EXERCISE 46 (2.5.3). *Let R be an ordering of A. Prove that R^{-1} is also an ordering of A, and for $B \subseteq A$,*

a. *a is the least element of B in R^{-1} if and only if a is the greatest element of B in R;*

b. *Similarly for (minimal and maximal) and (supremum and infimum).*

PROOF. **(a)** (i) $aR^{-1}a$ since aRa. (ii) Suppose $(a,b) \in R^{-1}$ and $(b,a) \in R^{-1}$. Then $(b,a) \in R$ and $(a,b) \in R$, and so $a = b$ since R is antisymmetric. (iii) Let $aR^{-1}b$ and $bR^{-1}c$. Then bRa and cRb. Hence, cRa since R is transitive. But which means that $aR^{-1}c$, i.e., R^{-1} is transitive.

(b) If a is the least element of B in R^{-1}, then $a \in B$ and $aR^{-1}x$ for all $x \in B$. But then xRa for all $x \in B$, i.e., a is the greatest element of B in R; if a be the greatest element of B in R, that is, $a \in B$ and xRa for all $x \in B$, then $aR^{-1}x$ for all $x \in B$, and so a is the least element of B in R^{-1}. With the same logic as (a) we can get (b). □

► EXERCISE 47 (2.5.4). *Let R be an ordering of A and let $B \subseteq A$. Show that $R \cap B^2$ is an ordering of B.*

PROOF. (i) For every $b \in B$ we have $(b,b) \in B^2$ and $(b,b) \in R$; hence, $(b,b) \in R \cap B^2$; that is, $R \cap B^2$ is reflexive. (ii) Let $(a,b) \in R \cap B^2$ and $(b,a) \in R \cap B^2$. Then $(a,b) \in R$ and $(b,a) \in R$ imply that $a = b$. Therefore, $R \cap B^2$ is antisymmetric. (iii) Let $(a,b) \in R \cap B^2$ and $(b,c) \in R \cap B^2$. Then $(a,b) \in R$ and $(b,c) \in R$ implies that $(a,c) \in R$. Furthermore, since both $a \in B$ and $c \in B$, we have $(a,c) \in B^2$. Hence, $(a,c) \in R \cap B^2$; that is, $R \cap B^2$ is transitive. □

► EXERCISE 48 (2.5.5). *Give examples of a finite ordered set $(A, \leqslant)$ and a subset B of A so that*

a. *B has no greatest element.*

b. *B has no least element.*

c. *B has no greatest element, but B has a supremum.*

d. *B has no supremum.*

Proof. **(a)** Let $A = \{a,b,c,d\}$, $B = \{a,b,c\}$, and

$$\leqslant = \{(a,a),(b,b),(c,c),(d,d),(a,d),(b,d),(c,d)\}.$$

In this example, a is not the greatest element of B because (a,b), (a,c) are incomparable; similarly, b and c are not the greatest elements of B.

(b) As the example in (a), there is no least element.

(c) As the example in (a), there is no greatest element, but d is an upper bound of B, and it is the least upper bound of B, so d is the supremum of B.

(d) Let $A = \{a,b,c,c\}$, $B = \{a,b,c\}$, and $\leqslant = \{(a,a),(b,b),(c,c),(d,d)\}$. Then there is no upper bound of B, and consequently, B has no supremum. □

► Exercise 49 (2.5.6). a. *Let $(A,<)$ be a strictly ordered set and $b \notin A$. Define a relation $\prec$ in $B = A \cup \{b\}$ as follows:*

$$x \prec y \text{ if and only if } (x,y \in A \text{ and } x < y) \text{ or } (x \in A \text{ and } y = b).$$

Show that $\prec$ is a strict ordering of B and $\prec \cap A^2 = <$.

b. *Generalize part (a): Let $(A_1,<_1)$ and $(A_2,<_2)$ be strict orderings, $A_1 \cap A_2 = \varnothing$. Define a relation $\prec$ on $B = A_1 \cup A_2$ as follows:*

$$\begin{aligned} x \prec y \text{ if and only if } & x,y \in A_1 \text{ and } x <_1 y \\ & \text{or } x,y \in A_2 \text{ and } x <_2 y \\ & \text{or } x \in A_1 \text{ and } y \in A_2. \end{aligned}$$

Show that $\prec$ is a strict ordering of B and $\prec \cap A_1^2 = <_1$, $\prec \cap A_2^2 = <_2$.

Proof. **(a)** Let $x \prec y$. Then either $x,y \in A$ and $x < y$ or $x \in A$ and $y = b$. In the first case, $y \not\prec x$ because $y \not< x$; in the later case, $y \not\prec x$ be definition. Therefore, $\prec$ is asymmetric.

Let $x \prec y$ and $y \prec z$. Then $y \neq b$; otherwise, $y \prec z$ cannot hold. With the same logic, $x \neq b$, too. If $z = b$, then $x \prec z = b$ by definition; if $z \in A$, then $x < y$ and $y < z$ implies $x < z$ and so $x \prec z$.

To prove $(\prec \cap A^2) = <$, let $(x,y) \in (\prec \cap A^2)$. Then $x,y \in A$ and $(x,y) \in \prec$, which means that $(x,y) \in <$. Now let $(x,y) \in <$. Then $x,y \in A \Longrightarrow (x,y) \in A^2$ and $(x,y) \in \prec$ by definition of $\prec$; hence, $(x,y) \in (\prec \cap A^2)$.

(b) Let $x \prec y$. If $x,y \in A_1$, then $x <_1 y$ and so $y \not\prec x$; if $x,y \in A_2$, then $x <_2 y$ and so $y \not\prec x$; if $x \in A_1$ and $y \in A_2$, then $y \not\prec x$ by definition.

Let $x \prec y$ and $y \prec z$. There are four cases:

- $x,y,z \in A_1$. In this case, $x <_1 y <_1 z \Longrightarrow x <_1 z \Longrightarrow x \prec z$.
- $x,y,z \in A_2$. In this case, $x <_2 y <_2 z \Longrightarrow x <_2 z \Longrightarrow x \prec z$.
- $x,y \in A_1$ and $z \in A_2$. In this case, $x \prec z$ by definition.

- $x \in A_1$ and $y, z \in A_2$. In this case, $x \prec z$ by definition.

To prove $\left(\prec \cap A_1^2\right) = <_1$, suppose $(x, y) \in \left(\prec \cap A_1^2\right)$ firstly. Then $(x, y) \in \prec$ and $x, y \in A_1$; hence $x \prec y \Longrightarrow x <_1 y$. Now suppose $(x, y) \in <_1$. Then $x \prec y$ and $x, y \in A_1$; that is, $(x, y) \in \left(\prec \cap A_1^2\right)$.

The result that $\left(\prec \cap A_2^2\right) = <_2$ can be proved with the same logic. □

▶ Exercise 50 (2.5.7). *Let R be a reflexive and transitive relation in A (R is called a* preordering *of A). Define E in A by*

$$aEb \text{ if and only if } aRb \text{ and } bRa.$$

Show that E is an equivalence relation on A. Define the relation R/E in A/E by

$$[a]_E\,(R/E)[b]_E \text{ if and only if } aRb.$$

Show that the definition does not depend on the choice of representatives for $[a]_E$ and $[b]_E$. Prove that R/E is an ordering of A/E.

Proof. We first show that E is an equivalence relation on A. (i) E is reflexive since R is. (ii) E is symmetric: if aEb, then aRb and bRa, i.e., bRa and aRb; therefore, bEa by the definition of E. (iii) E is transitive: if aEb and bEc, then aRb and bRa, and bRc and cRb. Hence, aRc and cRa by the transitivity of R. We thus have aEc.

Let $[a]_E(R/E)[b]_E$ if and only if aRb. We show that if $c \in [a]_E$ and $d \in [b]_E$, then $[a]_E(R/E)[b]_E$ if and only if cRd. We firt focus on the "IF" part. Since $c \in [a]_E$, we have cEa, i.e., aRc and cRa; similarly, dRb and bRd. Let cRd. We first have aRd since aRc; we also have dRb; hence aRb, i.e., cRd implies that $[a]_E(R/E)[b]_E$. To prove the "ONLY IF" part, let $[a]_E(R/E)[b]_E$. Then aRb. Since cRa and bRd, we have cRd.

R/E is an ordering of A/E since (i) R/E is reflexive: for any $[a]_E \in A/E$, we have $a \in [a]_E$ and aRa, so $[a]_E(R/E)[a]_E$; (ii) R/E is antisymmetric: if $[a]_E(R/E)[b]_E$ and $[b]_E(R/E)[a]_E$, then aRb and bRa, i.e., aEb. Hence, $[a]_E = [b]_E$; (iii) R/E is transitive: if $[a]_E(R/E)[b]_E$ and $[b]_E(R/E)[c]_E$, then aRb and bRc and so aRc, that is, $[a]_E(R/E)[c]_E$. □

▶ Exercise 51 (2.5.8). *Let $A = \mathcal{P}(X)$, $X \neq \varnothing$. Prove:*

a. *Any $S \subseteq A$ has a supremum in the ordering $\subseteq_A$;* $\sup S = \bigcup S$.

b. *Any $S \subseteq A$ has an infimum in $\subseteq_A$;* $\inf S = \bigcap S$ *if $S \neq \varnothing$;* $\inf \varnothing = X$.

Proof. (a) Let $U = \left\{u \in A \mid s \subseteq_A u,\ \forall\, s \in S\right\}$, i.e., U is the set of all the upper bounds of S according to $\subseteq_A$. Note that $U \neq \varnothing$ since $X \in U$. Now we show that the least element of U exists, and which is $\bigcup S$. Since $s \subseteq_A s \subseteq_A \bigcup S$ for any $s \in S$, we have $\bigcup S \in U$; to see that $\bigcup S$ is the least element of U, take any $u \in U$. Then $s \subseteq_A u$ for all $s \in S$ and so $\bigcup S \subseteq_A u$; therefore, $\sup S = \bigcup S$.

(b) Let $L = \{\ell \in A \mid \ell \subseteq_A s, \ \forall\, s \in S\}$, i.e., L is the set of all the lower bounds of S according to $\subseteq_A$, and $L \neq \varnothing$ since $\varnothing \in L$. We first consider the case that $S \neq \varnothing$, and show that $\sup L = \bigcap S$. Firstly, it is clear that $\bigcap S \in L$; secondly, if $\ell \in L$, then $\ell \subseteq_A s$ for all $s \in S$, so $\ell \subseteq_A \bigcap S$. Therefore, $\inf S = \bigcap S$ if $S \neq \varnothing$.

Finally, let $S = \varnothing$. Then $\inf \varnothing = X$ because for all $B \subseteq X$, $B \subseteq_A C$, $\forall\, C \in \varnothing = S$. Suppose it were not the case. Then there exists $C' \in \varnothing$ such that $B \not\subseteq_A C'$. However, there does not exist such a $C' \in \varnothing$ since there is no element in $\varnothing$. Therefore, all subsets of X, including X itself, is a lower bound of $\varnothing$ according to $\subseteq_A$. Then the greatest element according to $\subseteq_A$ is X. □

▶ Exercise 52 (2.5.9). *Let* $\operatorname{Fn}(X,Y)$ *be the set of all functions mapping a subset of* X *into* Y *[i.e.,* $\operatorname{Fn}(X,Y) = \bigcup_{Z\subseteq X} Y^Z$*]. Define a relation* $\preccurlyeq$ *in* $\operatorname{Fn}(X,Y)$ *by*

$$f \preccurlyeq g \text{ if and only if } f \subseteq g.$$

a. *Prove that* $\preccurlyeq$ *is an ordering of* $\operatorname{Fn}(X,Y)$.

b. *Let* $F \subseteq \operatorname{Fn}(X,Y)$. *Show that* $\sup F$ *exists if and only if* F *is a compatible system of functions; then* $\sup F = \bigcup F$.

Proof. **(a)** The relation $\preccurlyeq$ is *reflexive* since $f \subseteq f$ for any $f \in \operatorname{Fn}(X,Y)$. If $f \preccurlyeq g$ and $g \preccurlyeq f$, then $f \subseteq g$ and $g \subseteq f$. By the Axiom of Extentionality, we have $f = g$; hence, $\preccurlyeq$ is *antisymmetric*. Finally, let $f \preccurlyeq g$, and $g \preccurlyeq h$, where $f, g, h \in \operatorname{Fn}(X,Y)$. Then $f \subseteq g$ and $g \subseteq h$ implies that $f \preccurlyeq g$; that is, $\preccurlyeq$ is *transitive*. Therefore, $\preccurlyeq$ is an ordering of $\operatorname{Fn}(X,Y)$.

(b) Let $F \subseteq \operatorname{Fn}(X,Y)$. If $\sup F$ exists, there is a function $\sup F \in \operatorname{Fn}(X,Y)$ such that for any $f, g \in \operatorname{Fn}(X,y)$, $f \subseteq \sup F$ and $g \subseteq \sup F$. Suppose $(x,y) \in f$, and $(x,z) \in g$. Then $(x,y) \in \sup F$, and $(x,z) \in \sup F$. Hence, it must be the case that $y = z$; otherwise, $\sup F$ would be not a function. This proves F is a compatible system of functions.

Now suppose F is a compatible system of functions. Then, $\bigcup F$ is a function with $\mathfrak{D}_F = \bigcup\{\mathfrak{D}_f \mid f \in F\} \subseteq X$; therefore, $\bigcup F \in \operatorname{Fn}(X,Y)$. It is easy to see that $\bigcup F$ is an upper bound of F since $f \subseteq \bigcup F \iff f \preccurlyeq \bigcup F$ for any $f \in F$. Finally, let G be any upper bound of F, then $f \subseteq G$ for any $f \in F$; consequently,

$$\left[\bigcup F = \bigcup_{f\in F} f \subseteq G\right] \Longrightarrow \bigcup F \preccurlyeq G,$$

for any upper bound of F. This proves that $\sup F = \bigcup F$. □

▶ Exercise 53 (2.5.10). *Let* $A \neq \varnothing$*; let* $\operatorname{Pt}(A)$ *be the set of all partitions of* A. *Define a relation* $\preccurlyeq$ *in* $\operatorname{Pt}(A)$ *by*

$$S_1 \preccurlyeq S_2 \text{ if and only if for every } C \in S_1 \text{ there is } D \in S_2 \text{ such that } C \subseteq D.$$

(We say that the partition S_1 *is a* refinement *of the partition* S_2 *if* $S_1 \preccurlyeq S_2$ *holds.)*

a. *Show that $\preccurlyeq$ is an ordering.*

b. *Let $S_1, S_2 \in \mathrm{Pt}(A)$. Show that $\{S_1, S_2\}$ has an infimum. How is the equivalence relation E_S related to the equivalence E_{S_1} and E_{S_2}?*

c. *Let $T \subseteq \mathrm{Pt}(A)$. Show that* $\inf T$ *exists.*

d. *Let $T \subseteq \mathrm{Pt}(A)$. Show that* $\sup T$ *exists.*

Proof. (a) It is clear that $\preccurlyeq$ is reflexive. To see $\preccurlyeq$ is antisymmetric, let $S_1 \preccurlyeq S_2$ and $S_2 \preccurlyeq S_1$, where $S_1, S_2 \in \mathrm{Pt}(A)$. Since $S_1 \preccurlyeq S_2$, for every $C_1 \in S_1$ there is $D_2 \in S_2$ such that $C_1 \subseteq D_2$. Suppose that $C_1 \subset D_2$. Since $S_2 \preccurlyeq S_1$, there is $D_1 \in S_1$ such that $D_2 \subseteq D_1$. Then $C_1 \subset D_1$. But then $C_1 \cap D_1 \neq \varnothing$ A contradiction. Hence, $S_1 \subseteq S_2$. Similarly, $S_2 \subseteq S_1$.

To verify that $\preccurlyeq$ is transitive, let $S_1 \preccurlyeq S_2$, and $S_2 \preccurlyeq S_3$, where $S_1, S_2, S_3 \in \mathrm{Pt}(A)$. Then for every $C \in S_1$, there is $D \in S_2$ and $E \in S_3$ such that $C \subseteq D \subseteq E$; that is, $C \subseteq E$. Hence, $S_1 \preccurlyeq S_3$.

(b) Let $S_1, S_2 \in \mathrm{Pt}(A)$. Let $\mathscr{L} = \{S \in \mathrm{Pt}(A) : S \preccurlyeq S_1 \text{ and } S \preccurlyeq S_2\}$. Note that $\mathscr{L} \neq \varnothing$ because $\{\{a\} : a \in A\} \in \mathscr{L}$. We now show

$$M = \{C \cap D : C \in S_1 \text{ and } D \in S_2\}$$

is the greatest element of $\mathscr{L}$. If $m \in M$, then there exist $C \in S_1$ and $D \in S_2$ such that $m = C \cap D$. Then $m \subseteq C$ and $m \subseteq D$; that is, $M \preccurlyeq S_1$ and $M \preccurlyeq S_2$; that is, $M \in \mathscr{L}$.

Pick an arbitrary $N \in \mathscr{L}$. Then for every $n \in N$, there exists $C \in S_1$ such that $n \subseteq C$, and there exists $D \in S_2$ such that $n \subseteq D$; that is, $n \subseteq C \cap D \in M$. Hence, $N \preccurlyeq M$ and so $M = \inf\{S_1, S_2\}$.

(c) The same as (b).

(d) Let $T \subseteq \mathrm{Pt}(A)$. Define $\mathcal{U} = \{S \in \mathrm{Pt}(A) : t \preccurlyeq S \ \forall\, t \in T\}$. Notice that $\mathcal{U} \neq \varnothing$ because $A \in \mathcal{U}$. Now we show that

$$\sup T = \left\{ \bigcup_{C_i \in t_i} C_i : t_i \in T \right\} = P.$$

This can be proved as follows:

- $P \in \mathcal{U}$. For any $C_i \in t_i \in T$, $C_i \subseteq C_i \cup \bigcup_{C_j \in t_j} C_j \in P$, where $j \neq i$; hence $t_i \preccurlyeq P$, $\forall\, t_i \in T$.

- P is the least element of $\mathcal{U}$. Suppose $Q \in \mathcal{U}$. Then $t_i \preccurlyeq Q$, $\forall\, t_i \in T$; then, for any $C_i \in t_i$, there exists $q \in Q$ such that $C_i \subseteq q$, for all $t_i \in T$. But which means that $\bigcup_{C_i \in t_i} C_i \subseteq q, \quad \forall\, t_i \in T$. Hence, $P \preccurlyeq Q$, $\forall\, Q \in \mathcal{U}$. □

► Exercise 54 (2.5.11). *Show that if $(P, <)$ and $(Q, \prec)$ are isomorphic strictly ordered sets and $<$ is a linear ordering, then $\prec$ is a linear ordering.*

Proof. Let $h\colon P \to Q$ be the isomorphism. Pick any $q_1, q_2 \in Q$ with $q_1 \neq q_2$. There exist $p_1, p_2 \in P$ with $p_1 \neq p_2$ such that $q_1 = h(p_1)$ and $q_2 = h(p_2)$. Since $<$ is a linear ordering, p_1 and p_2 are comparable, say, $p_1 < p_2$. Then $h(p_1) = q_1 \prec q_2 = h(p_2)$. □

► Exercise 55 (2.5.12). *The identity function on P is an isomorphism between $(P, <)$ and $(P, <)$.*

Proof. The function $\mathrm{Id}_P\colon P \to P$ is bijective, and $p_1 < p_2$ iff $\mathrm{Id}_P(p_1) < \mathrm{Id}_P(p_2)$. □

► Exercise 56 (2.5.13). *If h is an isomorphism between $(P, <)$ and $(Q, \prec)$, then h^{-1} is an isomorphism between $(Q, \prec)$ and $(P, <)$.*

Proof. Since $\mathfrak{D}_{h^{-1}} = \mathfrak{R}_h = Q$, and $\mathfrak{R}_{h^{-1}} = \mathfrak{D}_h = P$, the function $h^{-1}\colon Q \to P$ is bijective. For all $q_1, q_2 \in Q$, there exists unique $p_1, p_2 \in P$ such that $q_1 = h(p_1)$ and $q_2 = h(p_2)$; then

$$q_1 \prec q_2 \iff h(p_1) \prec h(p_2) \iff p_1 < p_2 \iff h^{-1}(q_1) < h^{-1}(q_2). \qquad \square$$

► Exercise 57 (2.5.14). *If f is an isomorphism between $(P_1, <_1)$ and $(P_2, <_2)$, and if g is an isomorphism between $(P_2, <_2)$ and $(P_3, <_3)$, then $g \circ f$ is an isomorphism between $(P_1, <_1)$ and $(P_3, <_3)$.*

Proof. First, $\mathfrak{D}_{g \circ f} = \mathfrak{D}_f \cap f^{-1}[\mathfrak{D}_g] = P_1 \cap f^{-1}[P_2] = P_1$. Next, for every $p_3 \in P_3$, there exists $p_2 \in P_2$ such that $p_3 = g(p_2)$, and for every $p_2 \in P_2$, there exists $p_1 \in P_1$ such that $p_2 = f(p_1)$. Therefore, for every $p_3 \in P_3$, there exists $p_1 \in P_1$ such that $p_3 = g(p_2) = g(f(p_1)) = (g \circ f)(p_1)$. Hence, $g \circ f\colon P_1 \to P_3$ is surjective.

To see that $g \circ f$ is injective, let $p_1 \neq p_1'$. Then $f(p_1) \neq f(p_1')$, and so $g(f(p_1)) \neq g(f(p_1'))$.

Finally, to see $g \circ f$ is order-preserving, notice that

$$p_1 <_1 p_1' \iff f(p_1) <_2 f(p_1') \iff (g \circ f)(p_1) <_3 (g \circ f)(p_1'). \qquad \square$$

3

NATURAL NUMBERS

3.1 Introduction to Natural Numbers

► Exercise 58 (3.1.1). *$x \subseteq S(x)$ and there is no z such that $x \subset z \subset S(x)$.*

Proof. It is clear that $x \subseteq x \cup \{x\} = S(x)$. Given x, suppose there exists a set z such that $x \subset z$. Then there must exist some set $a \neq \varnothing$ such that $z = x \cup a$. If $a = \{x\}$, then $z = S(x)$; if $a \neq \{x\}$, then there must exist $d \in a$ such that $d \neq x$. Therefore, we have $a \nsubseteq \{x\}$. Consequently, $z = x \cup a \nsubseteq x \cup \{x\} = S(x)(d)$. □

3.2 Properties of Natural Numbers

► Exercise 59 (3.2.1). *Let $n \in \mathbb{N}$. Prove that there is no $k \in \mathbb{N}$ such that $n < k < n + 1$.*

Proof. (Method 1) Let $n \in \mathbb{N}$. Suppose there exists $k \in \mathbb{N}$ such that $n < k$. Then $n \in k$; that is, $n \subset k$ [See Exercise 65]. If $k < n + 1$, then $k \subset n + 1 = S(n)$. That is impossible by Exercise 58.

(Method 2) Suppose there exists k such that $k < n+1$. By Lemma 2.1, $k < n+1$ if and only if $k < n$ or $k = n$. Therefore, it cannot be the case that $n < k$. □

► Exercise 60 (3.2.2). *Use Exercise 59 to prove for all $m, n \in \mathbb{N}$: if $m < n$, then $m + 1 \leqslant n$. Conclude that $m < n$ implies $m + 1 < n + 1$ and that therefore the successor $S(n) = n + 1$ defines a one-to-one function in $\mathbb{N}$.*

Proof. $m < m + 1$ for all $m \in \mathbb{N}$. It follows from Exercise 59 that there is no $n \in \mathbb{N}$ satisfying $m < n < m + 1$. Since $<$ is linear on $\mathbb{N}$, it must be the case that $m + 1 \leqslant n$. Then $m + 1 \leqslant n < n + 1$ implies that $m + 1 < n + 1$. To see $S(n)$ is one-to-one, let $m < n$. Then $S(m) = m + 1$, $S(n) = n + 1$, and so $m + 1 < n + 1$. □

► Exercise 61 (3.2.3). *Prove that there is a one-to-one mapping of $\mathbb{N}$ onto a proper subset of $\mathbb{N}$.*

Proof. Just consider $S\colon n \mapsto n+1$. By Exercise 60, S is injective. By definition, S is defined on $\mathbb{N}$, i.e., $\mathfrak{D}_S = \mathbb{N}$, and by the following Exercise 62, $\mathfrak{R}_S = \mathbb{N} \smallsetminus \{0\}$. Therefore, $S\colon \mathbb{N} \to \mathbb{N} \smallsetminus \{0\}$, as desired. □

► Exercise 62 (3.2.4). *For every $n \in \mathbb{N}$, $n \neq 0$, there is a unique $k \in \mathbb{N}$ such that $n = k+1$.*

Proof. We use the induction principle in Exercise 69 to prove this claim. Let $\mathbf{P}(x)$ be "there is a unique $k \in \mathbb{N}$ such that $x = k+1$". It is clear that $\mathbf{P}(1)$ holds since $1 = 0+1$. The uniqueness of $0 = \varnothing$ is from Lemma 3.1 in Chapter 1. Now suppose that $\mathbf{P}(n)$ holds and consider $\mathbf{P}(n+1)$. We have $n+1 = (k+1)+1$ by the induction assumption $\mathbf{P}(n)$. Note that $k+1 = S(k) \in \mathbb{N}$. Let $k+1 = k'$. The uniqueness of k implies that k' is unique. We thus complete the proof. □

► Exercise 63 (3.2.5). *For every $n \in \mathbb{N}$, $n \neq 0, 1$, there is a unique $k \in \mathbb{N}$ such that $n = (k+1)+1$.*

Proof. We know from Exercise 62 that for every nonzero $n \in \mathbb{N}$ there is a unique $k' \in \mathbb{N}$, such that $n = k'+1$. Now consider $k' \in \mathbb{N}$. If $n \neq 1$, then $k' \neq 0$. Therefore, we can impose the result of Exercise 62 on k'; that is, there is a unique $k \in \mathbb{N}$ such that $k' = k+1$. Combining these above two steps, we know for all $n \in \mathbb{N}$, $n \neq 0, 1$, there is a unique $k \in \mathbb{N}$ such that $n = (k+1)+1$. □

► Exercise 64 (3.2.6). *Prove that each natural number is the set of all smaller natural numbers; i.e., $n = \{m \in \mathbb{N} : m < n\}$.*

Proof. Let $\mathbf{P}(x)$ denote "$x = \{m \in \mathbb{N} : m < x\}$". It is evident that $\mathbf{P}(0)$ holds trivially. Assume that $\mathbf{P}(n)$ holds and let us consider $\mathbf{P}(n+1)$. We have

$$n+1 = n \cup \{n\} = \{m \in \mathbb{N} : m < n\} \cup \{n\} = \{m \in \mathbb{N} : m < n+1\}. \qquad \square$$

► Exercise 65 (3.2.7). *For all $m, n \in \mathbb{N}$, $m < n$ if and only if $m \subset n$.*

Proof. Let $\mathbf{P}(x)$ be the property "$m < x$ if and only if $m \subset x$". It is clear that $\mathbf{P}(0)$ holds trivially. Assume that $\mathbf{P}(n)$ holds. Let us consider $\mathbf{P}(n+1)$. First let $m < n+1$; then $m < n$ or $m = n$. If $m < n$, then $m \subset n \subset (n+1)$ by the induction assumption $\mathbf{P}(n)$; if $m = n$, then $m = n \subset (n+1)$, too. Now assume that $m \subset (n+1)$. Then either $m = n$ or $m \subset n$. We get $m < n+1$ in either case. □

► Exercise 66 (3.2.8). *Prove that there is no function $f\colon \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$, $f(n) > f(n+1)$. (There is no infinite decreasing sequence of natural numbers.)*

Proof. Suppose there were such a function f. Then $\varnothing \neq \{f(n) \in \mathbb{N} : n \in \mathbb{N}\} \subseteq \mathbb{N}$. Because $(\mathbb{N}, <)$ is well-ordered, the set $\{f(n) \in \mathbb{N} : n \in \mathbb{N}\}$ has a least element α; that is, there is $m \in \mathbb{N}$ such that $f(m) = \alpha$. But $f(m+1) < f(m) = \alpha$, which contradicts the assumption that α is the least element. □

► EXERCISE 67 (3.2.9). *If $X \subseteq \mathbb{N}$, then $\langle X, < \cap X^2 \rangle$ is well-ordered.*

PROOF. Let $Y \subseteq X$ be nonempty. Y has a least element y when Y is embedded in $\mathbb{N}$. But clearly y is still a least element of Y when Y is embedded in $X \subseteq \mathbb{N}$. □

► EXERCISE 68 (3.2.10). *In Exercise 49, let $A = \mathbb{N}$, $b = \mathbb{N}$. Prove that $\prec$ as defined there is a well-ordering of $B = \mathbb{N} \cup \{\mathbb{N}\}$. Notice that $x \prec y$ if and only if $x \in y$ holds for all $x, y \in B$.*

PROOF. The relation $\prec$ in $B = \mathbb{N} \cup \{\mathbb{N}\}$ is defined as

$$x \prec y \iff (x, y \in \mathbb{N} \text{ and } x < y) \text{ or } (x \in \mathbb{N} \text{ and } y = \mathbb{N}) \iff x \in y.$$

Let $X \subseteq B = \mathbb{N} \cup \{\mathbb{N}\}$ be nonempty. There are two cases:

- If $\mathbb{N} \notin X$, then $X \subseteq \mathbb{N}$, and so X has a least element since $(\mathbb{N}, <)$ is well-ordered.
- If $\mathbb{N} \in X$, then $X = Y \cup \{\mathbb{N}\}$, where $Y \subseteq \mathbb{N}$. Hence, Y has a least element α. But $\alpha \prec \mathbb{N}$ since $\alpha \in \mathbb{N}$; that is, α is the least element of X. □

► EXERCISE 69 (3.2.11). *Let $\mathbf{P}(x)$ be a property. Assume that $k \in \mathbb{N}$ and*

a. *$\mathbf{P}(k)$ holds.*

b. *For all $n \geqslant k$, if $\mathbf{P}(n)$ then $\mathbf{P}(n+1)$.*

Then $\mathbf{P}(n)$ holds for all $n \geqslant k$.

PROOF. If $k = 0$, then this is the original Induction Principle. So assume that $k > 0$ and $\mathbf{P}(k)$ holds. Then, by Exercise 62, there is a unique $k' \in \mathbb{N}$ such that $k' + 1 = k$. Define

$$B = \{n \in \mathbb{N} : n \leqslant k'\}, \quad \text{and} \quad C = \left\{n \in \mathbb{N} : n \geqslant k \text{ and } \mathbf{P}(n)\right\}.$$

Notice that $B \cap C = \varnothing$.

We now show that $A = B \cup C$ is inductive. Obviously, $0 \in A$. If $n \in B$, then either $n < k'$ and so $n + 1 \in B$, or $n = k'$ and so $n + 1 = k \in C$. If $n \in C$, then $n + 1 \in C$ by assumption. Hence, $\mathbb{N} = A$ (since $A \subseteq \mathbb{N}$), and so $\{n \in \mathbb{N} : n \geqslant k\} = \mathbb{N} \smallsetminus B = C$. □

► EXERCISE 70 (3.2.12, Finite Induction Principle). *Let $\mathbf{P}(x)$ be a property. Assume that $k \in \mathbb{N}$ and*

a. *$\mathbf{P}(0)$.*

b. *For all $n < k$, $\mathbf{P}(n)$ implies $\mathbf{P}(n+1)$.*

Then $\mathbf{P}(n)$ holds for all $n \leqslant k$.

PROOF. Suppose there were $n < k$ such that $\neg\mathbf{P}(n)$. Then it must be the case that $\neg\mathbf{P}\ (m)$, where $m + 1 = n$. Thus, $X = \{a \in \mathbb{N} \colon a < k \text{ and } \neg\mathbf{P}(a)\} \neq \varnothing$, and so X has a least element, α. Also $\alpha \neq 0$ since $\mathbf{P}(0)$ holds by assumption.

However, if $\neg\mathbf{P}(\alpha)$, then $\neg\mathbf{P}(\beta)$, where $\beta + 1 = \alpha$, is also true. But $\beta < \alpha$, which contradicts the assumption that α is the least element of X. Therefore, $\mathbf{P}(n)$ holds for all $n < k$.

To see $\mathbf{P}(k)$ holds, too, notice that there exists $m \in \mathbb{N}$ and $m < k$ such that $m + 1 = k$ (by Exercise 62). Because we have shown that $\mathbf{P}(m)$ holds, $\mathbf{P}(m + 1) = \mathbf{P}(k)$ also holds. □

► EXERCISE 71 (3.2.13, Double Induction). *Let $\mathbf{P}(x, y)$ be a property. Assume*

$$\text{If } \mathbf{P}(k, \ell) \text{ holds for all } k, \ell \in \mathbb{N} \text{ such that } k < m \text{ or } (k = m \text{ and } \ell < n), \text{ then } \mathbf{P}(m, n) \text{ holds.} \tag{$**$}$$

Conclude that $\mathbf{P}\ (m, n)$ holds for all $m, n \in \mathbb{N}$.

PROOF. We proceed by induction on m. Fix $n \in \mathbb{N}$. Then $\mathbf{P}(m, n)$ is true for all $m \in \mathbb{N}$ by the second version of Induction Principle. Now for every $m \in \mathbb{N}$, (m, n) is true for all n by the second version of Induction Principle. Hence, $\mathbf{P}(m, n)$ holds for all $m, n \in \mathbb{N}$. □

3.3 THE RECURSION THEOREM

► EXERCISE 72 (3.3.1). *Let f be an infinite sequence of elements of A, where A is ordered by $\prec$. Assume that $f_n \prec f_{n+1}$ for all $n \in \mathbb{N}$. Prove that $n < m$ implies $f_n \prec f_m$ for all $n, m \in \mathbb{N}$.*

PROOF. We proceed by induction on m in the form of Exercise 69. For an arbitrary $n \in \mathbb{N}$, let $\mathbf{P}(x)$ denote "$f_n \prec f_x$ if $n < x$". Let $k = n + 1$. then $\mathbf{P}\ (k)$ holds since $f_n \prec f_{n+1} = f_k$ by assumption.

Suppose that $\mathbf{P}(m)$ holds, where $m \geqslant k$, and consider $\mathbf{P}(m + 1)$. Since $f_m \prec f_{m+1}$ by the assumption of the exercise, and $f_n \prec f_m$ by induction hypothesis of $\mathbf{P}(m)$, we have $f_n \prec f_{m+1}$.

Using the Induction Principle in the form of Exercise 69, we conclude that $\mathbf{P}(m)$ holds for all $m \geqslant k = n + 1 > n$. □

► EXERCISE 73 (3.3.2). *Let $(A, \prec)$ be a linearly ordered set and $p, q \in A$. We say that q is a* successor *or p if $p \prec q$ and there is no $r \in A$ such that $p \prec r \prec q$. Note that each $p \in A$ can have at most one successor. Assume that $(A, \prec)$ is nonempty and has the following properties:*

a. *Every $p \in A$ has a successor.*

b. *Every nonempty subset of A has a $\prec$-least element.*

c. *If $p \in A$ is not the $\prec$-least element of A, then p is a successor of some $q \in A$.*

Prove that $(A, \prec)$ is isomorphic to $(\mathbb{N}, <)$. Show that the conclusion need not hold if one of the conditions (a)–(c) is omitted.

PROOF. We first show that each $p \in A$ can have at most one successor. If q_1 and q_2 are both the successors of p, and $q_1 \neq q_2$, say, $q_1 \prec q_2$, then $p \prec q_1 \prec q_2$, in contradiction to the assumption that q_2 is a successor of p.

Let a be the least element of A (by (b)) and let $g(x, n)$ be the successor of x (for all n). Then $a \in A$ and $g\colon A \times \mathbb{N} \to A$ is well defined by (a). The Recursion Theorem guarantees the existence of a function $f\colon \mathbb{N} \to A$ such that

- $f_0 = a =$ the least element of A;
- $f_{n+1} = g(f_n, n) =$ the successor of f_n.

By definition, $f_n \prec f_{n+1}$ for all $n \in \mathbb{N}$; by Exercise 72 $f_n \prec f_m$ whenever $n < m$. Consequently, f is injective. It remains to show that f is surjective.

If not, $A \smallsetminus \mathcal{R}_f \neq \varnothing$; let p be the least element of $A \smallsetminus \mathcal{R}_f$. Then $p \neq a$, the least element of A. It follows from (c) that there exists $q \in A$ such that p is the successor of q. There exists $m \in \mathbb{N}$ such that $f_m = q$; for otherwise $q \in A \smallsetminus \mathcal{R}_f$ and $q \prec p$. Hence, $f_{m+1} = p$ by the recursive condition. Consequently, $p \in \mathcal{R}_f$, a contradiction. □

► EXERCISE 74 (3.3.3). *Give a direct proof of Theorem 3.5 in a way analogous to the proof of the Recursion Theorem.*

PROOF. We first show that there exists a unique infinite sequence of finite sequences $\langle F^n \in \mathrm{Seq}(S)\colon n \in \mathbb{N}\rangle = F$ satisfying

$$F^0 = \langle\,\rangle, \tag{A}$$

$$F^{n+1} = G\left(F^n, n\right), \tag{B}$$

where

$$G\left(F^n, n\right) = \begin{cases} F^n \cup \left\{\langle n, g(F_0^n, \dots, F_{n-1}^n)\rangle\right\} & \text{if } F^n \text{ is a sequence of length } n \\ \langle\,\rangle & \text{otherwise.} \end{cases}$$

It is easy to see that $G\colon \mathrm{Seq}(S) \times \mathbb{N} \to \mathrm{Seq}(S)$.

Let $T\colon (m+1) \to \mathrm{Seq}(S)$ be an m-step computation based on $F_0 = \langle\,\rangle$ and G. Then

$$T^0 = \langle\,\rangle, \quad \text{and} \quad T^{k+1} = G(T^k, k) \text{ for } 0 \leqslant k < m.$$

Notice that $T \in \mathcal{P}(\mathbb{N} \times \mathrm{Seq}(S))$. Let

$$\mathcal{F} = \left\{T \in \mathcal{P}(\mathbb{N} \times \mathrm{Seq}(S))\colon T \text{ is an } m\text{-step computation for some } m \in \mathbb{N}\right\}.$$

Let $F = \bigcup \mathcal{F}$. Then

- *F is a function.* We need only to prove the system of functions $\mathcal{F}$ is compatible. Let $T, U \in \mathcal{F}$, $\mathfrak{D}_T = m \in \mathbb{N}$, $\mathfrak{D}_U = n \in \mathbb{N}$. Assume, e.g., $m \leqslant n$; then $m \subseteq n \Longrightarrow m \cap n = m$, and it suffices to show that

  $$\left\langle T_0^k, \ldots, T_{k-1}^k \right\rangle = T^k = U^k = \left\langle U_0^k, \ldots, U_{k-1}^k \right\rangle$$

  for all $k < m$. This can be done by induction [Exercise 70]. Surely, $T^0 = \langle\,\rangle = U^0$. Next let k be such that $k + 1 < m$, and assume $T^k = U^k$. Then

  $$T^{k+1} = T^k \cup \left\{ \left\langle k, g(T^k) \right\rangle \right\} = U^k \cup \left\{ \left\langle k, g(U^k) \right\rangle \right\} = U^{k+1}.$$

  Thus, $T^k = U^k$ for all $k < m$.

- $\mathfrak{D}_F = \mathbb{N}$*;* $\Re_F \subseteq \mathrm{Seq}(S)$. We know that $\mathfrak{D}_F = \bigcup \left\{ \mathfrak{D}_T \mid T \in \mathcal{F} \right\} \subseteq \mathbb{N}$, and $\Re_F \subseteq \mathbb{N}$. To show that $\mathfrak{D}_F = \mathbb{N}$, it suffices to prove that for each $n \in \mathbb{N}$ there is an n-step computation T. We use the Induction Principle. Clearly, $T = \{\langle 0, \langle\,\rangle \rangle\}$ is a 0-step computation.

  Assume that T is an n-step computation. Then the following function T_+ on $(n + 1) + 1$ is an $(n + 1)$-step computation:

  $$\begin{cases} T_+^k = T^k, & \text{if } k \leqslant n \\ T_+^{n+1} = T^n \cup \left\{ \langle n, g(T^n) \rangle \right\}. \end{cases}$$

  We conclude that each $n \in \mathbb{N}$ is in the domain of some computation $T \in \mathcal{F}$, so $\mathbb{N} \subseteq_{T \in \mathcal{F}} \mathfrak{D}_T = \mathfrak{D}_F$.

- *F satisfies condition* (A) *and* (B). Clearly, $F_0 = \langle\,\rangle$ since $T^0 = \langle\,\rangle$ for all $T \in \mathcal{F}$. To show that $F_{n+1} = G(F_n, n)$ for any $n \in \mathbb{N}$, let T be an $(n + 1)$-step computation; then $T^k = F_k$ for all $k \in \mathfrak{D}_T$, so $F_{n+1} = T^{n+1} = G(T^n, n) = G(F_n, n)$.

  Let $H : \mathbb{N} \to \mathrm{Seq}(S)$ be such that

  $$H_0 = \langle\,\rangle, \tag{A$'$}$$

and

$$H_{n+1} = G(H_n, n) \quad \forall\, n \in \mathbb{N}. \tag{B$'$}$$

We show that $F_n = H_n$, $\forall\, n \in \mathbb{N}$, again using induction. Certainly $F_0 = H_0$. If $F_n = H_n$, then $F_{n+1} = G(F_n, n) = G(H_n, n) = H_{n+1}$; therefore, $F = H$, as claimed.

Now we can define a function f by

$$f = \bigcup_{n \in \mathbb{N}} F^n. \qquad \square$$

► Exercise 75 (3.3.4). *Derive the "parametric" version of the Recursion Theorem: Let* $a\colon P \to A$ *and* $g\colon P \times A \times \mathbb{N} \to A$ *be functions. There exists a unique function* $f\colon P \times \mathbb{N} \to A$ *such that*

a. $f(p, 0) = a(p)$ *for all* $p \in P$*;*

b. $f(p, n + 1) = g\left(p, f(p, n), n\right)$ *for all* $n \in \mathbb{N}$ *and* $p \in P$*.*

Proof. Define $G\colon A^P \times \mathbb{N} \to A^P$ by

$$G(x, n)(p) = g(p, x(p), n)$$

for $x \in A^P$ and $n \in \mathbb{N}$. Define $F\colon \mathbb{N} \to A^P$ by recursion:

$$F_0 = a \in A^P, \quad F_{n+1} = G(F_n, n). \tag{3.1}$$

Then, by the Recursion Theorem, there exists a unique $F\colon \mathbb{N} \to A^P$ satisfying (3.1). Now let $f(p, n) = F_n(p)$. Then

- $f(p, 0) = F_0(p) = a(p)$, and
- $f(p, n + 1) = F_{n+1}(p) = G(F_n, n)(p) = g(p, F_n(p), n) = g(p, f(p, n), n)$. □

► Exercise 76 (3.3.5). *Prove the following version of the Recursion Theorem:*

Let g *be a function on a subset of* $A \times \mathbb{N}$ *into* A*,* $a \in A$*. Then there is a unique sequence* f *of elements of* A *such that*

a. $f_0 = a$*;*

b. $f_{n+1} = g(f_n, n)$ *for all* $n \in \mathbb{N}$ *such that* $(n + 1) \in \mathfrak{D}_f$*;*

c. f *is either an infinite sequence or* f *is a finite sequence of length* $k + 1$ *and* $g(f_k, k)$ *is undefined.*

Proof. Let $\overline{A} = A \cup \{\overline{a}\}$ where $\overline{a} \notin A$. Define $\overline{g}\colon \overline{A} \times \mathbb{N} \to \overline{A}$ as follows:

$$\overline{g}(x, n) = \begin{cases} g(x, n) & \text{if defined} \\ \overline{a} & \text{otherwise.} \end{cases} \tag{3.2}$$

Then, by the Recursion Theorem, there exists a unique infinite sequence $\overline{f}\colon \mathbb{N} \to \overline{A}$ such that

$$\overline{f}_0 = a, \quad \overline{f}_{n+1} = \overline{g}(\overline{f}_n, n).$$

If $\overline{f}_\ell = \overline{a}$ for some $\ell \in \mathbb{N}$, consider $\overline{f} \restriction \ell$ for the least such ℓ. □

► Exercise 77 (3.3.6). *Prove: If* $X \subseteq \mathbb{N}$*, then there is a one-to-one (finite or infinite) sequence* f *such that* $\mathfrak{R}_f = X$*.*

Proof. Define $g\colon X \times \mathbb{N} \to X$ by

$$g(x, n) = \min\{y \in X : y > x\}.$$

Let $a = \min X$. Then, by Exercise 76, there exists a unique function f satisfying $f_0 = a$ and $f_{n+1} = g(f_n, n)$.

For every $m \in \mathbb{N}$, we have $f_{m+1} \geqslant f_m + 1 > f_m$; hence, f is injective. It follows from the previous exercise that f is surjective. □

3.4 Arithmetic of Natural Numbers

► Exercise 78 (3.4.1). *Prove the associative low of addition:* $(k+m)+n = k+(m+n)$ *for all* $k, m, n \in \mathbb{N}$.

Proof. We use induction on n. So fix $k, m \in \mathbb{N}$. If $n = 0$, then

$$(k+m)+0 = k+m,$$

and

$$k+(m+0) = k+m.$$

Assume that $(k+m)+n = k+(m+n)$ and consider $n+1$:

$$\begin{aligned}(k+m)+(n+1) &= [(k+m)+n]+1\\ &= [k+(m+n)]+1\\ &= k+[(m+n)+1]\\ &= k+[m+(n+1)].\end{aligned}$$ □

► Exercise 79 (3.4.2). *If* $m, n, k \in \mathbb{N}$*, then* $m < n$ *if and only if* $m+k < n+k$*.*

Proof. We first need to prove the following proposition: for any $m, n \in \mathbb{N}$,

$$m < n \iff m+1 < n+1. \tag{3.3}$$

The "$\Longrightarrow$" half has been proved in Exercise 60, so we need only to show the "$\Longleftarrow$" part. Assume that $m+1 < n+1$. Then $m < m+1 \leqslant n$. Hence, $m < n$.

For the "$\Longrightarrow$" half we use induction on k. Consider fixed $m, n \in \mathbb{N}$ with $m < n$. Clearly, $m < n \iff m+0 < n+0$. Assume that $m < n \Longrightarrow m+k < n+k$. Then by (3.3), $(m+k)+1 < (n+k)+1$, i.e., $m+(k+1) < n+(k+1)$.

For the "$\Longleftarrow$" half we use the trichotomy law and the "$\Longrightarrow$" half. If $m+k < n+k$, then we cannot have $m = n$ (lest $n+k < n+k$) nor $n < m$ (lest $n+k < m+k < n+k$). The only alternative is $m < n$. □

► Exercise 80 (3.4.3). *If* $m, n \in \mathbb{N}$ *then* $m \leqslant n$ *if and only if there exists* $k \in \mathbb{N}$ *such that* $n = m+k$*. This* k *is unique, so we can denote it* $n - m$*, the* difference *of* n *and* m*.*

Proof. For the "$\Longrightarrow$" half we use induction on n. If $n = 0$, the proposition trivially hods since there is no natural number $m < 0$. Assume that $m < n$ implies that there exists a unique $k_{m,n} \in \mathbb{N}$ such that $m + k_{m,n} = n$. Now consider $n+1$. If $m < n+1$, then $m = n$ or $m < n$. If $m = n$, let $k_{m,n+1} = 1$ and so $m + k_{m,n+1} = n+1$; if $m < n$, then by the induction hypothesis, there exists a unique $k_{m,n} \in \mathbb{N}$ such that $m + k_{m,n} = n$. Let $k_{m,n+1} = k_{m,n} + 1$. Then

$$m + k_{m,n+1} = m + (k_{m,n} + 1) = (m + k_{m,n}) + 1 = n + 1.$$

For the "$\Longleftarrow$" half we use induction on k. If $k = 0$, it is obvious that $m = n$. Now assume that $m + k = n$ implies that $m \leqslant n$. Let us suppose that for all $m, n \in \mathbb{N}$ there exists a unique $k+1$ such that $m + (k+1) = n$. Then by Exercise 79 we have

$$\begin{aligned} 0 < k+1 &\Longrightarrow m + 0 < m + (k+1) \\ &\Longrightarrow m < n. \end{aligned} \qquad \square$$

► EXERCISE 81 (3.4.4). *There is a unique function* $\star$ *(*multiplication*) from* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that*

$$\begin{gathered} m \star 0 = 0 \quad \text{for all } m \in \mathbb{N}; \\ m \star (n+1) = m \star n + m \quad \text{for all } m, n \in \mathbb{N}. \end{gathered}$$

PROOF. We use the parametric version of the Recursion Theorem. Let $a\colon \mathbb{N} \to \mathbb{N}$ be defined as $a(p) = 0$, and $g\colon \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined as $g(p, x, n) = x + p$. Then, there exists a unique function $\star\colon \mathbb{N} \to \mathbb{N}$ such that

$$m \star 0 = a(m) = 0,$$

and

$$m \star (n+1) = g(m, m \star n, n) = m \star n + m. \qquad \square$$

► EXERCISE 82 (3.4.5). *Prove that multiplication is commutative, associative, and distributive over addition.*

PROOF. ($\cdot$ is commutative) We first show that 0 commutes by showing $0 \cdot m = 0$ (since $m \cdot 0 = 0$) for all $m \in \mathbb{N}$. Clearly, $0 \cdot 0 = 0$, and if $0 \cdot m = 0$, then

$$0 \cdot (m+1) = 0 \cdot m + 0 = 0.$$

Let us now assume that n commutes, and let us show that $n+1$ commutes. We prove, by induction on m, that

$$m \cdot (n+1) = (n+1) \cdot m \quad \text{for all } m \in \mathbb{N}. \tag{3.4}$$

If $m = 0$, then (3.4) holds, as we have already shown. Thus let us assume that (3.4) holds for m, and let us prove that

$$(m+1) \cdot (n+1) = (n+1) \cdot (m+1). \tag{3.5}$$

We derive (3.5) as follows:

$$\begin{aligned}(m+1)\cdot(n+1) = [(m+1)\cdot n] + (m+1) &= [n\cdot(m+1)] + (m+1)\\ &= (n\cdot m + n) + (m+1)\\ &= (n\cdot m + m) + (n+1)\\ &= (m\cdot n + m) + (n+1)\\ &= m\cdot(n+1) + (n+1)\\ &= (n+1)\cdot m + (n+1)\\ &= (n+1)\cdot(m+1).\end{aligned}$$

($\cdot$ is distributive over addition) We show that for all $m, n, p \in \mathbb{N}$,

$$m\cdot(n+p) = m\cdot n + m\cdot p. \tag{3.6}$$

Fix $m, n \in \mathbb{N}$. We use induction on p. It is clear that $m\cdot(n+0) = m\cdot n = m\cdot n + 0 = m\cdot n + m\cdot 0$. Now assume that (3.6) holds for p, and let us consider $p+1$:

$$\begin{aligned}m\cdot[n+(p+1)] &= m\cdot[(n+p)+1]\\ &= m\cdot(n+p)+m\\ &= m\cdot n + m\cdot p + m\\ &= m\cdot n + (m\cdot p + m)\\ &= m\cdot n + m\cdot(p+1).\end{aligned}$$

($\cdot$ is associative) Fix $m, n \in \mathbb{N}$. We use induction on p. Clearly, $m\cdot(n\cdot 0) = m\cdot 0 = 0$, and $(m\cdot n)\cdot 0 = 0$ as well. Now suppose that

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

Then

$$\begin{aligned}m\cdot[n\cdot(p+1)] &= m\cdot(n\cdot p + n)\\ &= m\cdot(n\cdot p) + m\cdot n\\ &= (m\cdot n)\cdot p + m\cdot n\\ &= (m\cdot n)\cdot(p+1).\end{aligned}$$ □

► EXERCISE 83 (3.4.6). *If $m, n \in \mathbb{N}$ and $k > 0$, then $m < n$ if and only if $m\cdot k < n\cdot k$.*

PROOF. For the "$\Longrightarrow$" half we fix $m, n \in \mathbb{N}$ and use induction on k. Clearly, $m\cdot 1 < n\cdot 1$ since

$$m\cdot 1 = m\cdot(0+1) = m\cdot 0 + m = m,$$

and similarly for $n\cdot 1$. Let us assume that $m < n$ implies $m\cdot k < n\cdot k$ with $k > 0$, and let us consider $k+1$:

$$\begin{aligned} m \cdot (k+1) &= m \cdot k + m \\ &< n \cdot k + m \\ &< n \cdot k + n \\ &= n \cdot (k+1), \end{aligned}$$

where the inequalities follow from Exercise 79.

The other half then follows exactly as in Exercise 79. □

► Exercise 84 (3.4.7). *Define exponentiation of nature numbers as follows:*

$$\begin{aligned} m^0 &= 1 \quad \textit{for all } m \in \mathbb{N} \textit{ (in particular, } 0^0 = 1\textit{);} \\ m^{n+1} &= m^n \cdot m \quad \textit{for all } m, n \in \mathbb{N} \textit{ (in particular, } 0^n = 0 \textit{ for } n > 0\textit{).} \end{aligned}$$

Prove the usual laws of exponents.

Proof. We show that $m^{n+p} = m^n \cdot m^p$ for all $m, n, p \in \mathbb{N}$ using induction on p. It is evident that

$$m^{n+0} = m^n = m^n \cdot 1 = m^n \cdot m^0,$$

so let us assume $m^{n+p} = m^n \cdot m^p$ and consider $p+1$:

$$\begin{aligned} m^{n+(p+1)} &= m^{(n+p)+1} \\ &= m^{n+p} \cdot m \\ &= (m^n \cdot m^p) \cdot m \\ &= m^n \cdot (m^p \cdot m) \\ &= m^n \cdot m^{p+1}. \end{aligned}$$ □

3.5 Operations and Structures

► Exercise 85 (3.5.1). *Which of the following sets are closed under operations of addition, subtraction, multiplication, and division of real number?*

a. *The set of all positive integers.*

b. *The set of all integers.*

c. *The set of all rational numbers.*

d. *The set of all negative rational numbers.*

e. *The empty set.*

Solution. See the following table:

	+	−	×	division of real numbers
(a)	Yes	No	Yes	No
(b)	Yes	Yes	Yes	No
(c)	Yes	Yes	Yes	No
(d)	Yes	No	Yes	No
(e)	Yes	Yes	Yes	Yes

□

► EXERCISE 86 (3.5.4). *Let $A \neq \varnothing$, $B = \mathcal{P}(A)$. Show that $(B, \cup_B, \cap_B)$ and $(B, \cap_B, \cup_B)$ are isomorphic structures.*

PROOF. Define a function $h\colon B \to B$ as $h(x) = B \smallsetminus x$. It is evident that h is injective. To see h is surjective, notice that if $y \in B$, then $y \subseteq A$ and so $A \smallsetminus y \in B$; hence $h(A \smallsetminus y) = y$.

Since $B = \mathcal{P}(A)$, both $\cup_B$ and $\cap_B$ are well defined. For all $x, y \in B$,

$$h(x \cup_B y) = B \smallsetminus (x \cup_B y) = (B \smallsetminus x) \cap_B (B \smallsetminus y) = h(x) \cap_B h(y),$$

and similarly, $h(x \cap_B y) = h(x) \cup_B h(y)$. □

► EXERCISE 87 (3.5.5). *Refer to Example 5.7 for notation.*

a. *There is a real number $a \in A$ such that $a + a = a$ (namely, $a = 0$). Prove from this that there is $a' \in A'$ such that $a' \times a' = a'$. Find this a'.*

b. *For every $a \in A$ there is $b \in A$ such that $a + b = 0$. Show that for every $a' \in A'$ there is $b' \in A'$ such that $a' \times b' = 1$. Find this b'.*

PROOF. It is from Example 5.7 that $(A, \leqslant_A, +) \cong (A', \leqslant_{A'}, \times)$, and the isomorphism $h\colon A \to A'$ is $h(x) = e^x$.

(a) If $a + a = a$, then

$$h(a + a) = e^{a+a} = e^a \times e^a = e^a.$$

Hence, there exists $a' = e^a = e^0 = 1$ such that $a' \times a' = a'$.

(b) For every $a' \in A'$, there exists a unique $a \in A$ such that $h(a) = a'$. Let $b \in A$ such that $a + b = 0$. Then

$$h(a + b) = h(a) \times h(b) = a' \times h(b) = e^0 = 1.$$

Hence, for every $a' \in A'$, there exists $b' = h(b)$ such that $a' \times b' = 1$. □

► EXERCISE 88 (3.5.6). *Let $\mathbb{Z}^+$ and $\mathbb{Z}^-$ be, respectively, the sets of all positive and negative integers. Show that $(\mathbb{Z}^+, <, +)$ is isomorphic to $(\mathbb{Z}^-, >, +)$ (where $<$ is the usual ordering of integers).*

PROOF. Define $h\colon \mathbb{Z}^+ \to \mathbb{Z}^-$ by letting $h(z) = -z$. Then h is bijective. Let $z_1, z_2 \in \mathbb{Z}^+$. Then $z_1 < z_2$ iff $-z_1 > -z_2$ iff $h(z_1) > h(z_2)$. It is evident that both operations on $\mathbb{Z}^+$ and $\mathbb{Z}^-$ are well defined, and $h(z_1 + z_2) = -(z_1 + z_2) = (-z_1) + (-z_2) = h(z_1) + h(z_2)$. Thus, $(\mathbb{Z}^+, <, +) \cong (\mathbb{Z}^-, >, +)$. □

► EXERCISE 89 (3.5.14). *Construct the sets C_0, C_1, C_2, and C_3 in Theorem 5.10 for*

a. $\mathfrak{A} = (\mathbb{R}, S)$ *and* $C = \{0\}$.

b. $\mathfrak{A} = (\mathbb{R}, +, -)$ *and* $C = \{0, 1\}$.

PROOF. (a) $C_0 = C = \{0\}$, $C_1 = C_0 \cup S[C_0] = \{0\} \cup \{1\} = \{0, 1\}$, $C_2 = C_1 \cup S[C_1] = \{0, 1\} \cup \{1, 2\} = \{0, 1, 2\}$, and $C_3 = C_2 \cup S[C_2] = \{0, 1, 2\} \cup \{1, 2, 3\} = \{0, 1, 2, 3\}$.

(b) $C_0 = C = \{0, 1\}$, $C_1 = C_0 \cup +[C_0^2] \cup -[C_0^2] = \{0, 1\} \cup \{0, 1, 2\} \cup \{-1, 0, 1\} = \{-1, 0, 1, 2\}$, $C_2 = C_1 \cup +[C_1^2] \cup -[C_1^2] = \{-1, 0, 1, 2\} \cup \{-2, -1, 0, 1, 2, 3, 4\} \cup \{-3, -2, -1, 0, 1, 2, 3\} = \{-3, -2, -1, 0, 1, 2, 3, 4\}$, and $C_3 = C_2 \cup +[C_2^2] \cup -[C_2^2] = \{-7, -6, \cdots, 7, 8\}$. □

4

FINITE, COUNTABLE, AND UNCOUNTABLE SETS

4.1 Cardinality of Sets

▶ Exercise 90 (4.1.1). *Prove Lemma 1.5.*

a. *If* $|A| \leqslant |B|$ *and* $|A| = |C|$*, then* $|C| \leqslant |B|$*.*

b. *If* $|A| \leqslant |B|$ *and* $|B| = |C|$*, then* $|A| \leqslant |C|$*.*

c. $|A| \leqslant |A|$*.*

d. *If* $|A| \leqslant |B|$ *and* $|B| \leqslant |C|$*, then* $|A| \leqslant |C|$*.*

Proof. **(a)** If $|A| = |C|$, then $|C| = |A|$, and so there is a bijection $f: C \to A$. Since $|A| \leqslant |B|$, there is an injection $g: A \to B$. Then $g \circ f: C \to B$ is an injection and so $|C| \leqslant |B|$.

(b) Since $|A| \leqslant |B|$, there is a bijection $g: A \to \Re_g$, where $\Re_g \subseteq B$ is the image of A under g. Since $|B| = |C|$, there is a bijection $f: B \to C$. Let $h := f \restriction \Re_g$ be the restriction of f on $\Re_g$. Let $D' := \Re_h \subseteq C$. Then $h: \Re_g \to D'$ is a bijection. To prove $|A| \leqslant |C|$, consider $h \circ g: A \to D'$. This is a one-to-one correspondence from A to $D' \subseteq C$.

(c) This claim follows two facts: (i) Id_A is a one-to-one mapping of A onto A, and (ii) $A \subseteq A$.

(d) Since $|A| \leqslant |B|$, there is a bijection $f: A \to \Re_f$, where $\Re_f \subseteq B$. Since $|B| \leqslant |C|$, there is a bijection $g: B \to \Re_g$, where $\Re_g \subseteq C$. Let $h := g \restriction \Re_f$. Then $h \circ f: A \to C$ is a injection and so $|A| \leqslant |C|$. □

▶ Exercise 91 (4.1.2). *Prove*

a. *If* $|A| < |B|$ *and* $|B| \leqslant |C|$*, then* $|A| < |C|$*.*

b. *If* $|A| \leqslant |B|$ *and* $|B| < |C|$*, then* $|A| < |C|$*.*

Proof. **(a)** $|A| < |B|$ means $|A| \leqslant |B|$ and $|A| \neq |B|$. We thus have $|A| \leqslant |C|$ by Exercise 90 (d). If $|A| = |C|$, then $|B| \leqslant |A|$ by Exercise 90 (b). But then $|A| = |B|$ by the Cantor-Bernstein Theorem. A contradiction.

(b) $|B| < |C|$ means $|B| \leqslant |C|$ and $|B| \neq |C|$. We thus have $|A| \leqslant |C|$ by Exercise 90 (d). If $|A| = |C|$, then $|C| \leqslant |B|$ by Exercise 90 (a). But then $|B| = |C|$ by the Cantor-Bernstein Theorem. A contradiction. □

► EXERCISE 92 (4.1.3). *If $A \subseteq B$, then $|A| \leqslant |B|$.*

PROOF. Just consider Id_A. This is an embedding on B, and so $|A| \leqslant |B|$. □

► EXERCISE 93 (4.1.4). *Prove:*

a. $|A \times B| = |B \times A|$.

b. $|(A \times B) \times C| = |A \times (B \times C)|$.

c. $|A| \leqslant |A \times B|$ *if* $B \neq \varnothing$.

PROOF. **(a)** Let $f: (a,b) \mapsto (b,a)$ for all $(a,b) \in A \times B$. It is easy to see f is a function. To see f is injective, let $(a_1,b_1) \neq (a_2,b_2)$. Then $f(a_1,b_1) = (b_1,a_1) \neq (b_2,a_2) = f(a_2,b_2)$. To see f is surjective, let $(b,a) \in B \times A$. There must exist $(a,b) \in A \times B$ such that $f(a,b) = (b,a)$. We thus proved that $f: A \times B \to B \times A$ is bijective; consequently, $|A \times B| = |B \times A|$.

(b) Remember that $(A \times B) \times C \neq A \times (B \times C)$ [see Exercise 26 (b)], but as we are ready to prove, these two sets are equipotent. Let

$$f: \big((a,b),c\big) \mapsto \big(a,(b,c)\big), \quad \forall\ \big((a,b),c\big) \in (A \times B) \times C.$$

With the same logic as in (a), we see that f is bijective and so $|(A \times B) \times C| = |A \times (B \times C)|$.

(c) If $B \neq \varnothing$, we can choose some $b \in B$. Let $f: a \mapsto (a,b)$ for all $a \in A$. Then $f: A \to A \times b \subseteq A \times B$ is bijective, and so $|A| \leqslant |A \times B|$ if $B \neq \varnothing$. □

► EXERCISE 94 (4.1.5). *Show that $|S| \leqslant |\mathcal{P}(S)|$.*

PROOF. If $a \in S$, then $\{a\} \subseteq S$; hence, $\{a\} \in \mathcal{P}(S)$ for each $a \in S$. Define

$$\mathcal{A} = \big\{\{a\} : a \in S\big\}.$$

It is clear that $\mathcal{A} \subseteq \mathcal{P}(S)$. Consider the embedding $f: a \mapsto \{a\}$ for all $a \in S$. Then $f: S \to \mathcal{A}$ is bijective, and so $|S| \leqslant |\mathcal{P}(S)|$.

In fact, $|S| < |\mathcal{P}(S)|$. To prove this, we need the following claim.

CLAIM. There is a one-to-one mapping from $A \neq \varnothing$ to B iff there is a mapping from B onto A.

Proof. If $f: A \to B$ is one-to-one, and $\mathcal{R}_f = B^* \subseteq B$, then let

$$g(x) = \begin{cases} f^{-1}(x) & \text{if } x \in B^* \\ a_0 & \text{if } x \in B \smallsetminus B^*, \text{ where } a_0 \in A. \end{cases}$$

Then this g is a mapping from B onto A.

Conversely, let $g\colon B \to A$ be a mapping of B onto A. The relation "$x \sim y$ if $g(x) = g(y)$" is an equivalence relation on B [See Exercise 42, p. 22]. Let h be a choice function on the set of equivalence classes, i.e., if $[x]_\sim$ is an equivalence class, then $h\left([x]_\sim\right)$ is an element of $[x]_\sim$. It is clear that the map $f(x) = \left(h \circ g^{-1}\right)(x)$ is a one-to-one mapping of A into B.

To verify$|S| <|\mathcal{P}(S)|$, we want to show that there is no mapping from S onto $\mathcal{P}(S)$ [note that $\mathcal{P}(S) \neq \varnothing$ since $\varnothing \in \mathcal{P}(S)$ at least; hence here $\mathcal{P}(S)$ takes the role of A in the above claim]. Let $f\colon S \to \mathcal{P}(S)$ be any mapping. We have to show that f is not onto $\mathcal{P}(S)$. Let

$$A := \left\{a \in S : a \notin f(a)\right\} \in \mathcal{P}(S).$$

[Notice that by the Axiom Schema of Comprehension, A is a subset of S, and so is an element of $\mathcal{P}(S)$ by the Axiom of Power Set.] We claim that A does not have a preimage under f. In fact, suppose that is not the case, and $f(a_0) = A$ with some $a_0 \in S$. Then, because $A \subseteq S$, there are two possibilities:

- $a_0 \in A$, i.e., $a_0 \in f(a_0)$ which is not possible for then a_0 cannot be in A by the definition of A.
- $a_0 \notin A$, which is gain not possible, for then $a_0 \notin f(a_0)$, so a_0 should belong to A.

Thus, in either case we have arrived at a contradiction, which means that a_0 with the property $f(a_0) = A$ does not exist. □

► EXERCISE 95 (4.1.6). *Show that*$|A| \leqslant \left|A^S\right|$ *for any A and any $S \neq \varnothing$.*

PROOF. For every $a \in A$, we construct a constant function $f_a\colon S \to A$ by letting $f_a(s) = a$ for all $s \in S$. Now $F := \{f_a : a \in A\} \subseteq A^S$. Let $g\colon a \mapsto f_a$. It is easy to see that g is surjective. To see g is injective, let $a, a' \in A$ and $a \neq a'$; then $g(a) = f_a \neq f_{a'} = g\left(a'\right)$. This proves that $|A| = |F|$; that is, $|A| \leqslant \left|A^S\right|$, where $S \neq \varnothing$. □

► EXERCISE 96 (4.1.7). *If $S \subseteq T$, then*$\left|A^S\right| \leqslant \left|A^T\right|$*; in particular,* $|A^n| \leqslant |A^m|$ *if $n \leqslant m$.*

PROOF. For any $f \in A^S$, we define a corresponding function $g_f \in A^T$ as follows

$$g_f(x) = \begin{cases} f(x) & \text{if } x \in S \\ a_0 & \text{if } x \in T \smallsetminus S, \text{where } a_0 \in A. \end{cases}$$

Then $B := \left\{g_f \in A^T : f \in A^S\right\} \subseteq A^T$. Hence, we have a bijection $A^S \to B$. If $n \leqslant m$, then either $n = m$ or $n \in m$. Therefore,$|A^n| \leqslant |A^m|$ if $n < m$. □

► EXERCISE 97 (4.1.8). $|T| \leqslant \left|S^T\right|$ *if*$|S| \geqslant 2$.

PROOF. Since $|S| \geqslant 2$, we can pick $u, v \in S$ with $u \neq v$. For any $t \in T$, define a function $f_t \in S^T$ as follows

$$f_t(x) = \begin{cases} u & \text{if } x = t \\ v & \text{if } x \neq t. \end{cases}$$

Notice that $A := \left\{ f_t \in S^T : t \in T \right\} \subseteq S^T$. Then we can define a function $g \colon T \to A$ as $g(t) = f_t$. It is clear g is a one-to-one mapping from T onto B; therefore, $|T| \leqslant \left| S^T \right|$. □

► EXERCISE 98 (4.1.9). *If $|A| \leqslant |B|$ and if A is nonempty then there exists a mapping f of B onto A.*

PROOF. $|A| \leqslant |B|$ implies that there is a one-to-one correspondence f from $A \neq \varnothing$ onto $f[A] \subseteq B$. Define $g \colon B \to A$ as follows:

$$g(x) = \begin{cases} f^{-1}(x) & \text{if } x \in f[A] \\ a_0 & \text{if } x \in B \smallsetminus f[A], \end{cases}$$

where $a_0 \in A$. See also the claim in Exercise 94. □

(For Exercise 99–Exercise 101) Let F be a function on $\mathcal{P}(A)$ into $\mathcal{P}(A)$. A set $X \subseteq A$ is called *a fixed point* of F if $F(X) = X$. The function F is called *monotone* if $X \subseteq Y \subseteq A$ implies $F(X) \subseteq F(Y)$.

► EXERCISE 99 (4.1.10). *Let $F \colon \mathcal{P}(A) \to \mathcal{P}(A)$ be monotone. Then F has a fixed point.*

PROOF. Let $\mathcal{T} = \{X \subseteq A \colon F(X) \subseteq X\}$. Note that $\mathcal{T} \neq \varnothing$ since, e.g., $A \in \mathcal{T}$. Now let $\bar{X} = \bigcap \mathcal{T}$ and so $\bar{X} \subseteq X$ for any $X \in \mathcal{T}$. Since F is monotone, we have $F(\bar{X}) \subseteq F(X) \subseteq X$ for every $X \in \mathcal{T}$. Then

$$F\left(\bar{X}\right) \subseteq \bar{X}. \tag{4.1}$$

Hence, $\bar{X} \in \mathcal{T}$.

On the other hand, (4.1) and the monotonicity of F implies that

$$F\left(F\left(\bar{X}\right)\right) \subseteq F\left(\bar{X}\right). \tag{4.2}$$

But (4.2) implies that $F\left(\bar{X}\right) \in \mathcal{T}$, too. Then, by the definition of $\bar{X}$, we have

$$\bar{X} \subseteq F\left(\bar{X}\right). \tag{4.3}$$

Therefore, (4.1) and (4.3) imply that $F\left(\bar{X}\right) = \bar{X}$, i.e., $\bar{X}$ is a fixed point of F. □

▶ EXERCISE 100 (4.1.11). *Use Exercise 99 to give an alternative proof of the Cantor-Bernstein Theorem.*

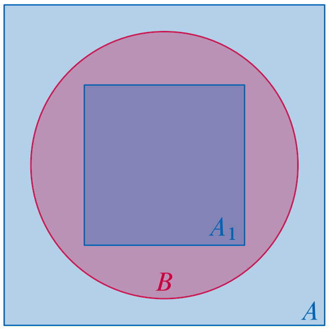

FIGURE 4.1. Cantor-Bernstein Theorem

PROOF. We use Exercise 99 to prove Lemma 4.1.7: *If* $A_1 \subseteq B \subseteq A$ *and*$|A_1| = |A|$, *then*$|B| = |A|$. Let $F\colon \mathcal{P}(A) \to \mathcal{P}(A)$ be defined by

$$F(X) = (A \setminus B) \cup f[X],$$

where $f\colon A \to A_1$ is a bijection from A onto A_1. Then F is monotone since f is, and so there exists a fixed point $C \subseteq A$ of F such that

$$C = (A \setminus B) \cup f[C].$$

Let $D = A \setminus C$. Define a function $g\colon A \to B$ as

$$g(x) = \begin{cases} f(x), & \text{if } x \in C \\ x, & \text{if } x \in D. \end{cases}$$

We now show that g is bijective.

g is surjective We have

$$\begin{aligned} \mathcal{R}_g = f[C] \cup D = f[C] \cup (A \setminus C) &= f[C] \cup \Big\{A \setminus \big[(A \setminus B) \cup f[C]\big]\Big\} \\ &= f[C] \cup \big[(A \cap B) \cap f^c[C]\big] \\ &= f[C] \cup \big(B \cap f^c[C]\big) \\ &= f[C] \cup B \\ &= B, \end{aligned}$$

where the last equality holds since $f[C] \subseteq A_1 \subseteq B$ [remember that $f\colon A \leftrightarrow A_1$]. Thus, g is surjective indeed.

g is injective Both $g \restriction C$ and $g \restriction D$ are injective functions, so we need only to show $f[C] \cap D = \varnothing$. This holds because

$$f[C] \cap D = f[C] \cap \big(B \cap f^c[C]\big) = \varnothing.$$

Therefore, $g\colon A \to B$ is bijective, and so$|B| =|A|$. □

▶ Exercise 101 (4.1.12). *Prove that $\bar{X}$ in Exercise 99 is the least fixed point of F, i.e., if $F(X) = X$ for some $X \subseteq A$, then $\bar{X} \subseteq X$.*

Proof. Notice that if $F(X) = X$, then $F(X) \subseteq X$, and so $X \in \mathcal{T}$. Then we obtain the conclusion just because $\bar{X} = \bigcap \mathcal{T}$. □

(For Exercise 102 and Exercise 103) A function $F : \mathcal{P}(A) \to \mathcal{P}(A)$ is *continuous* if

$$F\left(\bigcup_{i \in \mathbb{N}} X_i\right) = \bigcup_{i \in \mathbb{N}} F\left(X_i\right)$$

holds for any nondecreasing sequence of subsets of A. [$\langle X_i : i \in \mathbb{N}\rangle$ is *nondecreasing* if $X_i \subseteq X_j$ holds whenever $i \leqslant j$.]

▶ Exercise 102 (4.1.13). *Prove that F used in Exercise 100 is continuous.*

Proof. Let $\langle X_i : i \in \mathbb{N}\rangle \subseteq \mathcal{P}(A)$ be a nondecreasing sequence of A. Then

$$\begin{aligned} F\left(\bigcup_{i \in \mathbb{N}} X_i\right) = (A \smallsetminus B) \cup f\left[\bigcup_{i \in \mathbb{N}} X_i\right] &= (A \smallsetminus B) \cup \left[\bigcup_{i \in \mathbb{N}} f\left[X_i\right]\right] \\ &= \bigcup_{i \in \mathbb{N}} \left[(A \smallsetminus B) \cup f\left[X_i\right]\right] \\ &= \bigcup_{i \in \mathbb{N}} F\left(X_i\right). \end{aligned}$$

□

▶ Exercise 103 (4.1.14). *Prove that if $\bar{X}$ is the least fixed point of a monotone continuous function $F\colon \mathcal{P}(A) \to \mathcal{P}(A)$, then $\bar{X} = \bigcup_{i \in \mathbb{N}} X_i$, where we define recursively $X_0 = \varnothing$, $X_{i+1} = F(X_i)$.*

Proof. We prove this statement with several steps.

(1) We first show that the infinite sequence $\langle X_i : i \in \mathbb{N}\rangle$ defined by $X_0 = \varnothing$, $X_{i+1} = F\left(X_i\right)$ is nondecreasing [$\langle X_i : i \in \mathbb{N}\rangle$ exists by the Recursion Theorem]. We use the Induction Principle to prove this property. Let $\mathbf{P}(x)$ denote "$X_x \subseteq X_{x+1}$". Then

- $\mathbf{P}(0)$ holds because $X_0 = \varnothing$.
- Assume that $\mathbf{P}(n)$ holds, i.e., $X_n \subseteq X_{n+1}$. We need to show $\mathbf{P}(n+1)$. Notice that

$$X_{(n+1)+1} = F\left(X_{n+1}\right) \overset{\langle 1\rangle}{\supseteq} F\left(X_n\right) = X_{n+1},$$

where ⟨1⟩ holds because $X_n \subseteq X_{n+1}$ by $\mathbf{P}(n)$ and since F is monotone. We thus prove $\mathbf{P}(n+1)$

Therefore, by the Induction Principle, $X_n \subseteq X_{n+1}$, for any $n \in \mathbb{N}$. Then by Exercise 72, $X_i \subseteq X_j$ holds whenever $i \leqslant j$, i.e., $\langle X_i : i \in \mathbb{N}\rangle$ is a nondecreasing infinite sequence.

(2) We now show $\bigcup_{i\in\mathbb{N}} X_i$ is a fixed point of F. Since F is continuous and $\langle X_i : i \in \mathbb{N}\rangle$ is nondecreasing, we have

$$\begin{aligned} F\left(\bigcup_{i\in\mathbb{N}} X_i\right) = \bigcup_{i\in\mathbb{N}} F(X_i) = F(X_0) \cup F(X_1) \cup \cdots &= \varnothing \cup F(X_0) \cup F(X_1)\cdots \\ &= X_0 \cup X_1 \cup X_2 \cup \cdots \\ &= \bigcup_{i\in\mathbb{N}} X_i; \end{aligned}$$

therefore, $\bar{X} := \bigcup_{i\in\mathbb{N}} X_i$ is a fixed point of F.

(3) To see $\bar{X}$ is the least fixed point of F, let X be any fixed point of F, that is, $F(X) = X$. Then, since $\varnothing \subseteq X$, we have $F(\varnothing) \subseteq F(X) = X$ as F is monotone and X is a fixed point of F. Furthermore, $X_1 := F(\varnothing) \subseteq X$ means that $X_2 = F(X_1) \subseteq F(X) = X$. With this process, we have $X_{i+1} = F(X_i) \subseteq X$. Therefore, $\bar{X} = \bigcup_{i\in\mathbb{N}} X_i \subseteq X$ for any fixed point X of F; that is, $\bar{X}$ is the least fixed point of F.

(4) Till now, we have just proved that $\bar{X} = \bigcup_{i\in\mathbb{N}} X_i$ is a least fixed point of F, but the exercise asks us to prove the inverse direction. However, that direction must hold because there is only one least element in the set of all fixed points of F. □

4.2 Finite Sets

► Exercise 104 (4.2.1). *If $S = \{X_0, \dots, X_{n-1}\}$ and the elements of S are mutually disjoint, then* $\left|\bigcup S\right| = \sum_{i=0}^{n-1} |X_i|$.

Proof. We use the Induction Principle to prove this claim. The statement is true if $|S| = 0$. Assume that it is true for all S with $|S| = n$, and let $S = \{X_0, \dots, X_{n-1}, X_n\}$ be a set with $n+1$ elements, where each $X_i \in S$ is finite, and the elements of S are mutually disjoint. By the induction hypothesis, $|\bigcup_{i=1}^{n-1} X_i| = \sum_{i=0}^{n-1} |X_i|$, and we have

$$|S| = \left|\left(\bigcup_{i=1}^{n-1} X_i\right) \cup X_n\right| \overset{\langle 1\rangle}{=} \left|\bigcup_{i=1}^{n-1} X_i\right| + |X_i| \overset{\langle 2\rangle}{=} \sum_{i=1}^{n-1} |X_i| + |X_n| = \sum_{i=1}^{n} |X_i|,$$

where ⟨1⟩ is from Theorem 4.2.7, and ⟨2⟩ is from the induction hypothesis. □

► Exercise 105 (4.2.2). *If X and Y are finite, then $X \times Y$ is finite, and* $|X \times Y| = |X| \times |Y|$.

Proof. Let $X = \{x_0, \dots, x_{m-1}\}$, and let $Y = \{y_0, \dots, y_{n-1}\}$, where $\langle x_0, \dots, x_{m-1}\rangle$ and $\langle y_0, \dots, y_{n-1}\rangle$ are injective finite sequences. Then

$$X \times Y = \big\{(x, y) \colon x \in X \text{ and } y \in Y\big\} = \bigcup_{x' \in X} \big\{(x', y) \colon y \in Y\big\}.$$

Note that $\big\{(x', y) \colon y \in Y\big\}$ is finite for a fixed $x' \in X$ since Y is finite. Precisely, since $|Y| = m$, there is a bijective function $f \colon m \to Y$, so we can construct a bijective function $g \colon m \to \big\{(x', y) \colon y \in Y\big\}$ as $g_i = (x', f_i)$ for all $i \leqslant m - 1$. Therefore, $\big|\{(x', y) \colon y \in Y\}\big| = m$ for all $x' \in X$. Thus, by Theorem 4.2.7, a finite union of finite sets is finite, we conclude that $X \times Y$ is finite, and

$$|X \times Y| = \left|\bigcup_{x' \in X} \big\{(x', y) \colon y \in Y\big\}\right| = \sum_{x' \in X} \Big|\big\{(x', y) \colon y \in Y\big\}\Big| = \sum_{x' \in X} |Y| = |X| \times |Y|,$$

where the second equality comes from Exercise 104 because $\big\{(x', y) \colon y \in Y\big\} \cap \big\{(x'', y) \colon y \in Y\big\} = \varnothing$ whenever $x', x'' \in X$ and $x' \neq x''$. □

► Exercise 106 (4.2.3). *If X is finite, then* $|\mathcal{P}(X)| = 2^{|X|}$.

Proof. We proceed by induction on the number of elements of X. The statement is true if $|X| = 0$: in this case, $\mathcal{P}(\varnothing) = \{\varnothing\}$, and so $|\mathcal{P}(\varnothing)| = 1 = 2^0$. Assume that it is true for all X with $|X| = n$. Let Y be a set with $n + 1$ elements, i.e., $Y = \{y_0, \dots, y_{n-1}, y_n\}$. Let $X = \{y_0, \dots, y_{n-1}\}$ and $\mathcal{U} = \big\{U \colon U \subseteq Y \text{ and } y_n \in U\big\}$. Then $\mathcal{P}(Y) = \mathcal{P}(X) \cup \mathcal{U}$. Since $\mathcal{P}(X) \cap \mathcal{U} = \varnothing$, and $|\mathcal{P}(X)| = |\mathcal{U}|$, we have by Exercise 104

$$|\mathcal{P}(Y)| = |\mathcal{P}(X)| + |\mathcal{U}| = |\mathcal{P}(X)| + |\mathcal{P}(X)| = 2^n + 2^n = 2^{n+1} = 2^{|Y|}. \qquad \square$$

► Exercise 107 (4.2.4). *If X and Y are finite, then X^Y has $|X|^{|Y|}$ elements.*

Proof. Let $X = \{x_0, \dots, x_{m-1}\}$ and $Y = \{y_0, \dots, y_n\}$, where $\langle x_0, \dots, x_{m-1}\rangle$ and $\langle y_0, \dots, y_n\rangle$ are injective finite sequences. We use the Induction Principle on Y to prove this claim. If $|Y| = 0$, then $X^Y = X^\varnothing = \{\langle\,\rangle\} = \{\varnothing\}$, and so $\left|X^Y\right| = 1 = |X|^0 = |X|^{|Y|}$. Assume that for any finite X, $\left|X^Y\right| = |X|^{|Y|}$ if $|Y| = n \in \mathbb{N}$. Now consider a finite set Y with $|Y| = n + 1$. Let $Y = \{y_0, \dots, y_n\}$. Let $Y' = \{y_0, \dots, y_{n-1}\}$; that is, $\left|Y'\right| = n$. By the induction hypothesis, $\left|X^{Y'}\right| = |X|^{|Y'|} = m^n$, i.e., there are m^n functions in $X^{Y'}$. For any $f \in X^{Y'}$, we can construct a set $F(f)$ as follows:

$$F(f) := \left\{ g_i \in X^Y \colon g_i(y) = \begin{cases} f(y) & \text{if } y \in Y' \\ x_i & \text{if } y = y_n \end{cases}, \text{ and } i \leqslant m - 1 \right\}.$$

It is easy to see that $X^Y = \bigcup_{f \in X^{Y'}} F(f)$, and $|F(f)| = |X| = m$. Since $\left|X^{Y'}\right| = m^n$ by induction hypothesis, and for each f there is a corresponding set $F(f)$ with m elements; furthermore, $F(f) \cap F(f') = \varnothing$ whenever $f \neq f'$. It then follows from Exercise 104 that

$$\left|X^Y\right| = \sum_{f \in X^{Y'}} |F(f)| = m^n \cdot m = m^{n+1} = |X|^{|Y|}. \qquad \square$$

► EXERCISE 108 (4.2.5). *If $|X| = n \geqslant k = |Y|$, then the number of one-to-one functions $f : Y \to X$ is $n \cdot (n-1) \cdot \dots \cdot (n-k+1)$.*

PROOF. Let $X = \{x_0, \dots, x_{n-1}\}$ and $Y = \{y_0, \dots, y_{k-1}\}$, where $\langle x_0, \dots, x_{n-1}\rangle$ and $\langle y_0, \dots, y_{k-1}\rangle$ are injective finite sequences. To construct a injective function $f : Y \to X$, we just pick k different elements from X. Because there are $n \cdot (n-1) \cdot \dots \cdot (n-k+1)$ different ways to pick n elements from $k \geqslant n$ elements, there are $n \cdot (n-1) \cdot \dots \cdot (n-k+1)$ injective functions $f : Y \to X$. □

► EXERCISE 109 (4.2.6). *X is finite iff every nonempty system of subsets of X has a $\subseteq$-maximal elements.*

PROOF. To see the $\Longrightarrow$ half, let $X = \{x_0, \dots, x_{n-1}\}$. If $\varnothing \neq \mathcal{U} \subseteq \mathcal{P}(X)$, let $m := \max\left\{|Y| : Y \in \mathcal{U}\right\}$. Such a set m exists since X is finite, so $Y \subseteq X$ is finite [see Theorem 4.2.4], and $\mathcal{P}(X)$ is finite, too [see Theorem 4.2.8]. Let $\widetilde{Y} \in \mathcal{U}$ satisfying $\left|\widetilde{Y}\right| = m$. Now we show $\widetilde{Y}$ is a $\subseteq$-maximal element in $\mathcal{U}$. Suppose not; then there exists $Y' \in \mathcal{P}(X)$ such that $\widetilde{Y} \subset Y'$, but then $\left|\widetilde{Y}\right| < \left|Y'\right|$. A contradiction.

For the $\Longleftarrow$ half, assume that X is infinite, and every nonempty system of X has a $\subseteq$-maximal element. Let

$$\mathcal{V} := \left\{Y \subseteq X : Y \text{ is finite}\right\}.$$

However, there are no maximal elements in $\mathcal{V}$. To see this, suppose $Y \in \mathcal{V}$ is a $\subseteq$-maximal element, then consider $Y' = Y \cup \{y\}$, where $y \notin Y$ [such a y exists since X is infinite]; then $Y \subset Y'$ and Y' is finite. A contradiction. □

► EXERCISE 110 (4.2.7). *Use Lemma 2.6 and Exercise 105 and Exercise 107 to give easy proofs of commutativity and associativity for addition and multiplication of natural numbers, distributivity of multiplication over addition, and the usual arithmetic properties of exponentiation.*

PROOF. As an example, we only prove the commutativity of addition of natural numbers. Let $|X| = m$ and $|Y| = n$, where $X \cap Y = \varnothing$ and $m, n \in \mathbb{N}$. It follows from Lemma 2.6 that

$$|X \cup Y| = |X| + |Y| = m + n.$$

Similarly, we have $|Y \cup X| = |Y| + |X| = n + m$. Since $|X \cup Y| = |Y \cup X|$, we know that $m + n = n + m$. □

► EXERCISE 111 (4.2.8). *If A, B are finite and $X \subseteq A \times B$, then* $|X| = \sum_{a \in A} k_a$, *where* $k_a = \big|X \cap (\{a\} \times B)\big|$.

PROOF. Let $K_a = X \cap (\{a\} \times B)$ for all $a \in A$. We first show $\bigcup_{a \in A} K_a = X$. Since $K_a \subseteq X$ for all $a \in A$, we have $\bigcup_{a \in A} K_a \subseteq X$. Let $(a, b) \in X$. Then $a \in A$ and $b \in B$, so there exists K_a such that $(a, b) \in \{a\} \times B$; therefore, $(a, b) \in X \cap K_a$. Consequently, $X \subseteq \bigcup_{a \in A} K_a$. We then show that $K_a \cap K_{a'} = \varnothing$ if $a \neq a'$, but this is straightforward because $(a, b) \neq (a', b')$ for any $b, b' \in B$ when $a \neq a'$. Now, follows Exercise 104, we have

$$|X| = \left|\bigcup_{a \in A} K_a\right| = \sum_{a \in A} |K_a| = \sum_{a \in A} k_a. \qquad \square$$

4.3 COUNTABLE SETS

REMARK. We verify that the mapping $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$f(x, y) = \frac{(x + y)(x + y + 1)}{2} + x$$

is bijective (see Figure 4.2).

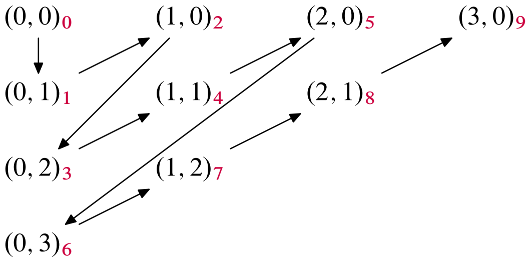

FIGURE 4.2. $(x, y) \mapsto (x + y)(x + y + 1)/2 + x$.

Look at the diagonal where $x + y = 3$ (positions 6, 7, 8, 9 in the diagram). $(x+y)(x+y+1)/2 = 6$ is the sum of the first $x+y = 3$ integers, which accounts for all previous diagonals ($x + y = 0, 1, 2$). Then x locates the position within the diagonal; e.g., $x = 0$ yields position 6, $x = 1$ position 7, $x = 2$ position 8, $x = 3$ position 9.

To go backwards, say we are given the integer 11. Since $1 + 2 + 3 + 4 = 10 < 11 < 1+2+3+4+5$, we are on the diagonal with $x + y = 4$; $x = 0$ gives position 10, $x = 1$ gives 11. Therefore $x = 1$, $y = 4 - 1 = 3$.

► EXERCISE 112 (4.3.1). *Let* $|A_1| = |B_1|, |A_2| = |B_2|$. *Prove*

a. *If* $A_1 \cap A_2 = \varnothing$, $B_1 \cap B_2 = \varnothing$, *then* $|A_1 \cup A_2| = |B_1 \cup B_2|$.

b. $|A_1 \times A_2| = |B_1 \times B_2|$.

c. $|\mathrm{Seq}(A_1)| = |\mathrm{Seq}(B_1)|$.

Remark. See the original exercise. I am afraid that there are some mistakes in the original one.

Proof. **(a)** Let $f\colon A_1 \to A_2$, and $g\colon B_1 \to B_2$ be bijections. Define a function $h : (A_1 \cup A_2) \to (B_1 \cup B_2)$ as follows:

$$h(a) = \begin{cases} f(a) & \text{if } a \in A_1 \\ g(a) & \text{if } a \in A_2. \end{cases}$$

It can be see that

$$h = f \cup g\colon (A_1 \cup A_2) \to (B_1 \cup B_2)$$

is bijective since $A_1 \cap A_2 = B_1 \cap B_2 = \varnothing$.

(b) Let f and g be defined as in part (a). We define a function $h : A_1 \times A_2 \to B_1 \times B_2$ as follows:

$$h(a_1, a_2) = \big(f(a_1), g(a_2)\big).$$

Then h is bijective.

(c) We know that $\left|A_1^n\right| = \left|B_1^n\right|$, $\forall\, n \in \mathbb{N}$ [see Lemma 5.1.6]. Notice that $\mathrm{Seq}(A_1) = \bigcup_{n\in\mathbb{N}} A^n$, and $\mathrm{Seq}(B_1) = \bigcup_{n\in\mathbb{N}} B_1^n$, and

$$A_1^m \cap A_1^n = \varnothing, \quad B_1^m \cap B_1^n,$$

for any $m \neq n$, $m, n \in \mathbb{N}$ [because, say, A_1^m and A_1^n have different domains]. Therefore,

$$|\mathrm{Seq}(A_1)| = \left|\bigcup_{n\in\mathbb{N}} A_1^n\right| = \sum_{n\in\mathbb{N}} \left|A_1^n\right| = \sum_{n\in\mathbb{N}} \left|B_1^n\right| = \left|\bigcup_{n\in\mathbb{N}} B_1^n\right| = |\mathrm{Seq}(B_1)|. \qquad \square$$

► Exercise 113 (4.3.2). *The union of a finite set and a countable set is countable.*

Proof. Let $|A| = m$, $|B| = \aleph_0$, and $A' = B \smallsetminus A$. Then $C = A \cup B = A' \cup B$. Since A is finite, $\left|A'\right| = n \leqslant m$. Then there exists two bijections $f : n \to A'$ and $g\colon \mathbb{N} \to B$. Define a function $h : \mathbb{N} \to A' \cup B$ as follows

$$h(i) = \begin{cases} f(i) & \text{if } i < n \\ g(i-n) & \text{if } i \geqslant n. \end{cases}$$

It is easy to see that h is a bijection; thus $|A \cup B| = \left|A' \cup B\right| = \aleph_0$. $\square$

► Exercise 114 (4.3.3). *If $A \neq \varnothing$ is finite and B is countable, then $A \times B$ is countable.*

Proof. Write A as $A = \{a_0, \dots, a_{n-1}\}$, where $\langle a_0, \dots, a_{n-1} \rangle$ is a one-to-one finite sequence. Since B is countable, there is a bijection $f: \mathbb{N} \to B$. Pick $a_i \in A$ and consider the set

$$A_i = \left\{ (a_i, f(n)) \colon f(n) \in B \text{ and } n \in \mathbb{N} \right\}.$$

Then A_i is countable because there is a bijection $g \colon n \mapsto (a_i, f(n))$.

Since $A \times B = \bigcup_{i \in n} A_i$, that is, $A \times B$ is the union of a finite system of countable sets, and so it is countable by Corollary 4.3.6. □

► Exercise 115 (4.3.4). *If $A \neq \varnothing$ is finite, then* Seq(A) *is countable.*

Proof. It suffices to prove for $A = n \in \mathbb{N}$. We first show that $|\text{Seq}(n)| \geqslant \aleph_0$. Because $n \neq 0$, we can pick an $i \in n$. Consider the following set of finite sequences on n:

$$S = \left\{ s_0 = \langle\ \rangle, s_1 = \langle i \rangle, s_2 = \langle i, i \rangle, s_3 = \langle i, i, i \rangle, \dots \right\}.$$

Define $f: \mathbb{N} \to S$ by letting $f(n) = s_n$; then f is bijective. Because $S \subseteq \text{Seq}(n)$, we have $\aleph_0 = |S| \leqslant |\text{Seq}(n)|$.

We then show that Seq$(n) \leqslant \aleph_0$. This is simply because Seq$(n) \subseteq$ Seq$(\mathbb{N})$ and Seq$(\mathbb{N}) = \aleph_0$.

Now, by Cantor-Bernstein Theorem, $|\text{Seq}(n)| = \aleph_0$. □

► Exercise 116 (4.3.5). *Let A be countable. The set $[A]^n = \left\{ S \subseteq A : |S| = n \right\}$ is countable for all $n \in \mathbb{N}$, $n \neq 0$.*

Proof. It is enough to prove the statement for $A = \mathbb{N}$. We use the Induction Principle in Exercise 69. $[A]^1$ is countable since $[A]^1 = \left\{ \{a\} : a \in A \right\}$, and we can define a bijection $f : A \to [A]^1$ by letting $f(a) = \{a\}$ for all $a \in A$. Therefore, $\left| [A]^1 \right| = |A| = \aleph_0$. Assume that $[A]^n$ is countable; particularly, we write $[A]^n$ as $[A]^n = \{S_1, S_2, \dots\}$. We need to prove that $[A]^{n+1}$ is countable, too. For any $S_i \in [A]^n$, we construct a set

$$\mathcal{S}_i = \left\{ S_i \cup \{j\} : j \in \mathbb{N} \setminus S_i \right\}.$$

Notice that $J_i = \mathbb{N} \setminus S_i$ is countable; in particular, there exists a bijection $g \colon \mathbb{N} \to J_i$. Define a bijection $h \colon J_i \to \mathcal{S}_i$ by letting $h(j) = S_i \cup \{j\}$, and we see that $|\mathcal{S}_i| = \aleph_0$.

Since $[A]^{n+1} = \bigcup_{i \in \mathbb{N}} \mathcal{S}_i$, the set $[A]^{n+1}$ is a countable union of countable sets. Now for each $i \in \mathbb{N}$, let $a_i = \langle a_i(n) \colon n \in \mathbb{N} \rangle$, where

$$a_i(n) = S_i \cup \{g(n)\}.$$

Then $\mathcal{S}_i = \{a_i(n) \colon n \in \mathbb{N}\}$. It follows from Theorem 4.3.9, $[A]^{n+1}$ is countable. □

► EXERCISE 117 (4.3.6). *A sequence* $\langle s_n \rangle_{n=0}^{\infty}$ *of natural numbers is* eventually constant *if there is* $n_0 \in \mathbb{N}$, $s \in \mathbb{N}$ *such that* $s_n = s$ *for all* $n \geqslant n_0$. *Show that the set of eventually constant sequences of natural numbers is countable.*

PROOF. Let $\mathcal{C}$ be the set of eventually constant sequences of natural numbers. A generic element of $\mathcal{C}$ is $\langle b_0, \dots, b_{n_0-1}, s, s, \dots \rangle$, where $\langle b_0, \dots, b_{n_0-1} \rangle \in \mathbb{N}^{n_0}$, and $s \in \mathbb{N}$.

Let Seq($\mathbb{N}$) be the set of all finite sequences of elements of $\mathbb{N}$. Define $f_{n_0} \colon \mathcal{C} \to \mathrm{Seq}(\mathbb{N})$ as follows:

$$f\left(\langle b_0, \dots, b_{n_0-1}, s, s, \dots \rangle\right) = \langle b_0, \dots, b_{n_0-1}, s \rangle .$$

Then f is bijective, and so $|\mathcal{C}| = \aleph_0$. □

► EXERCISE 118 (4.3.7). *A sequence* $\langle s_n \rangle_{n=0}^{\infty}$ *of natural numbers is (eventually)* periodic *if there are* $n_0, p \in \mathbb{N}$, $p \geqslant 1$, *such that for all* $n \geqslant n_0$, $s_{n+p} = s_n$. *Show that the set of all periodic sequences of natural numbers is countable.*

PROOF. Let $\mathcal{P}$ be the set of all eventually periodic sequences of natural numbers. A generic element of $\mathcal{P}$ is

$$\langle b_0, \dots, b_{n_0-1}, a_{n_0}, a_{n_0+1}, \dots, a_{n_0+p-1}, a_{n_0}, a_{n_0+1}, \dots, a_{n_0+p-1}, a_{n_0}, \dots \rangle .$$

Define $f : \mathcal{P} \to \mathrm{Seq}(\mathbb{N})$ by letting

$$\begin{aligned} f&\left(\langle b_0, \dots, b_{n_0-1}, a_{n_0}, a_{n_0+1}, \dots, a_{n_0+p-1}, a_{n_0}, a_{n_0+1}, \dots, a_{n_0+p-1}, a_{n_0}, \dots \rangle\right) \\ &= \langle b_0, \dots, b_{n_0-1}, a_{n_0}, a_{n_0+1}, \dots, a_{n_0+p-1} \rangle . \end{aligned}$$

f is bijective, and so $|\mathcal{P}| = \aleph_0$. □

► EXERCISE 119 (4.3.8). *A sequence* $\langle s_n \rangle_{n=0}^{\infty}$ *of natural numbers is called an* arithmetic progression *if there is* $d \in \mathbb{N}$ *such that* $s_{n+1} = s_n + d$ *for all* $n \in \mathbb{N}$. *Prove that the set of all arithmetic progressions is countable.*

PROOF. Let $\mathcal{A}$ be the set of all arithmetic progressions. A generic element of $\mathcal{A}$ is

$$\langle a, a + d, a + 2d, a + 3d, \dots \rangle .$$

Now define a function $f : \mathcal{A} \to \mathbb{N} \times \mathbb{N}$ by letting

$$f\left(\langle a, a + d, a + 2d, \dots \rangle\right) = \langle a, d \rangle .$$

f is bijection and so $|\mathcal{A}| = \aleph_0$. □

► EXERCISE 120 (4.3.9). *For every* $\boldsymbol{s} = \langle s_0, \dots, s_{n-1} \rangle \in \mathrm{Seq}(\mathbb{N} \smallsetminus \{0\})$, *let* $f(\boldsymbol{s}) = p_0^{s_0} \cdots p_{n-1}^{s_{n-1}}$, *where* p_i *is the* i*-th prime number. Show that* f *is one-to-one and use this fact to give another proof of* $|\mathrm{Seq}(\mathbb{N})| = \aleph_0$.

Proof. (i) We use the Induction Principle on n to show that $f(\boldsymbol{s}) \neq f(\boldsymbol{s}')$, whereever $\boldsymbol{s}, \boldsymbol{s}' \in \mathrm{Seq}(\mathbb{N} \smallsetminus \{0\})$ and $\boldsymbol{s} \neq \boldsymbol{s}'$. It is clear that $p_0^{s_0} \neq p_0^{s_0'}$ if $s_0 \neq s_0'$, i.e., this claim holds for $|\boldsymbol{s}| = 1$. Assume which holds for $|\boldsymbol{s}| = n$. We need to show it holds for $|\boldsymbol{s}| = n + 1$.

Suppose $|\boldsymbol{s}| = |\boldsymbol{s}'| = n + 1$ and $\boldsymbol{s} \neq \boldsymbol{s}'$, but $f(\boldsymbol{s}) = f(\boldsymbol{s}')$; that is,

$$p_0^{s_0} \cdot p_{n-1}^{s_{n-1}} \cdot p_n^{s_n} = p_0^{s_0'} \cdots p_{n-1}^{s_{n-1}'} \cdot p_n^{s_n'}. \tag{4.4}$$

There are two cases make (4.4) hold:

- $s_n = s_n'$. In this case, $\langle s_0, \ldots, s_{n-1} \rangle \neq \langle s_0', \ldots, s_{n-1}' \rangle$, and by the inductive hypothesis, $p_0^{s_0} \cdots p_{n-1}^{s_{n-1}} \neq p_0^{s_0'} \cdots p_{n-1}^{s_{n-1}'}$. Therefore, (4.4) implies that

$$p_n^{s_n} \neq p_n^{s_n'}, \tag{4.5}$$

  but which means that $s_n \neq s_n'$. A contradiction.

- $s_n \neq s_n'$. In this case, (4.5) must hold. Under this case, there are two cases further:

  ◇ $\langle s_0, \ldots, s_{n-1} \rangle = \langle s_0', \ldots, s_{n-1}' \rangle$. Then,

$$p_0^{s_0} \cdots p_{n-1}^{s_{n-1}} = p_0^{s_0'} \cdots p_{n-1}^{s_{n-1}'}. \tag{4.6}$$

  However, (4.6) and (4.5) imply that (4.4) fails to hold.

  ◇ $\langle s_0, \ldots, s_{n-1} \rangle \neq \langle s_0', \ldots, s_{n-1}' \rangle$. In this case, we know by the inductive hypothesis that

$$p_0^{s_0} \cdots p_{n-1}^{s_{n-1}} \neq p_0^{s_0'} \cdots p_{n-1}^{s_{n-1}'}, \tag{4.7}$$

  Without loss of generality, we assume that $s_n < s_n'$. Then (4.4) implies that

$$p_0^{s_0} \cdots p_{n-1}^{s_{n-1}} = p_0^{s_0'} \cdots p_{n-1}^{s_{n-1}'} \cdot p_n^{s_n' - s_n}. \tag{4.8}$$

  But we know from the *Unique Factorization Theorem* [see, for example, Apostol 1974] that every natural number $n > 1$ can be represented as a product of prime factors in only one way, apart form the order of the factors. Therefore, (4.8) cannot hold since $p_n \neq p_i$, $\forall\ i \leqslant n - 1$, and $s_n' - s_n > 0$.

(ii) We now show f is indeed onto $\mathbb{N} \smallsetminus \{0, 1\}$. This is follows the Unique Factorization Theorem again; hence, $|\mathrm{Seq}(\mathbb{N} \smallsetminus 0)| = \aleph_0$. To prove $|\mathrm{Seq}(\mathbb{N})| = \aleph_0$, we consider the following function $g\colon\ \mathrm{Seq}(\mathbb{N}) \to \mathbb{N}$

$$g(\boldsymbol{s}^0) = f\left(\boldsymbol{s}^0 + \mathbf{1}\right), \quad \forall\ \boldsymbol{s}^0 \in \mathrm{Seq}(\mathbb{N}),$$

where $\mathbf{1}$ is the finite sequence $\langle 1, 1, \ldots \rangle$ which has the same length as $\boldsymbol{s}^0$. Then g is one-to-one and onto $\mathbb{N} \smallsetminus \{0, 1\}$, which mean that

$$|\mathrm{Seq}(\mathbb{N})| = \aleph_0. \qquad \square$$

► EXERCISE 121 (4.3.10). *Let $(S,<)$ be a linearly ordered set and let $\langle A_n : n \in \mathbb{N}\rangle$ be an infinite sequence of finite subsets of S. Then $\bigcup_{n=0}^{\infty} A_n$ is at most countable.*

PROOF. Because $(S,<)$ is a linearly ordered set, and $A_n \subseteq S$ is finite for all $n \in \mathbb{N}$, we can write A_n as

$$A_n = \left\{s_0, s_1, \ldots, s_{|A_n|-1}\right\},$$

and rank the elements of A_n as

$$s_0 < s_1 < \ldots < s_{|A_n|-1}.$$

Then we can construct $\left\langle a_n(k) : k < |A_n| - 1\right\rangle$, a unique enumeration of A_n, by letting $a_n(k) = s_k$. Therefore, $\bigcup_{n=0}^{\infty} A_n$ is at most countable. □

► EXERCISE 122 (4.3.11). *Any partition of an at most countable set has a set of representatives.*

PROOF. Let $\mathscr{P}$ be a partition of A. Then there exists an equivalence relation $\sim$ on A induced by $\mathscr{P}$. Since A is at most countable, the set of equivalence classes, $A/\sim = \{[a]_\sim : a \in A\}$, is at most countable. Hence,

$$A/\sim = \langle [a_1]_\sim, [a_2]_\sim, \ldots\rangle,$$

and so there is a set of representatives: $\{a_1, a_2, \ldots\}$. □

4.4 LINEAR ORDERINGS

► EXERCISE 123 (4.4.1). *Assume that $(A_1,<_1)$ is similar to $(B_1,\prec_1)$ and $(A_2,<_2)$ is similar to $(B_2,\prec_2)$.*

a. *The sum of $(A_1,<_1)$ and $(A_2,<_2)$ is similar to the sum of $(B_1,\prec_1)$ and $(B_2,\prec_2)$, assuming that $A_1 \cap A_2 = \varnothing = B_1 \cap B_2$.*

b. *The lexicographic product of $(A_1,<_1)$ and $(A_2,<_2)$ is similar to the lexicographic product of $(B_1,\prec_1)$ and $(B_2,\prec_2)$.*

PROOF. We use $(A,<) \cong (B,\prec)$ to denote that $(A,<)$ is similar to $(B,\prec)$.

(a) Let $(A,<)$ be the sum of $(A_1,<_1)$ and $(A_2,<_2)$, and let $(B,\prec)$ be the sum of $(B_1,\prec_1)$ and $(B_2,\prec_2)$. Then both $(A,<)$ and $(B,\prec)$ are linearly ordered sets (by Lemma 4.4.5 and Exercise 49). Because $(A_1,<_1) \cong (B_1,\prec_1)$, there is an isomorphism $f_1 : (A_1,<_1) \to (B_1,\prec_1)$; similarly, there is an isomorphism $f_2 : A_2 \to B_2$ since $(A_2,<_2) \cong (B_2,\prec_2)$. Define a bijection $g : A \to B$ by $g = f_1 \cup f_2$.

To see $a_1 < a_2$ iff $g(a_1) \prec g(a_2)$, notice that (i) If $a_1, a_2 \in A_1$, then $g(a_1) = f_1(a_1)$ and $g(a_2) = f_2(a_2)$; hence, $a_1 <_1 a_2$ iff $a_1 < a_2$ iff $f_1(a_1) \prec_1 f_1(a_2)$ iff $g(a_1) \prec g(a_2)$. (ii) If $a_1, a_2 \in A_2$ we get the similarly result. (iii) If $a_1 \in A_1$ and $a_2 \in A_2$, then $a_1 < a_2$ by the definition of $<$. Moreover, by the definition of g,

$g(a_1) \in B_1$ and $g(a_2) \in B_2$; then by the definition of $\prec$, we have $g(a_1) \prec g(a_2)$. For the inverse direction, suppose $g(a_1) \prec g(a_2)$. However, since $a_1 \in A_1$ and $a_2 \in A_2$, we know immediately that $a_1 < a_2$ by definition of $<$. We thus proved $(A, <) \cong (B, \prec)$.

(b) Let $A = A_1 \times A_2$ and $B = B_1 \times B_2$. We need to show that $(A, <) \cong (B, \prec)$, where $<$ and $\prec$ are the lexicographic orderings of A and B. First notice that both $(A, <)$ and $(B, \prec)$ are linearly ordered sets by Lemma 4.4.6. For any $(a_1, a_2) \in A$, let $f : A \to B$ be defined as

$$f(a_1, a_2) = \left(f_1(a_1), f_2(a_2)\right),$$

where $f_1 : A_1 \to B_1$ and $f_2 : A_2 \to B_2$ are isomorphisms. It is easy to see that f is bijective.

Now let $(a_1, a_2), (a_1', a_2') \in A$. Suppose $(a_1, a_2) < (a_1', a_2')$; then either $a_1 <_1 a_1'$, or $a_1 = a_1'$ and $a_2 <_2 a_2'$. In the first case, $f_1(a_1) \prec_1 f_1(a_1')$, and so $(f_1(a_1), f_2(a_2)) \prec (f_1(a_1'), f_2(a_2'))$; in the second case, $f_1(a_1) = f_1(a_1')$ and $f_2(a_2) \prec_2 f_2(a_2')$ and so $(f_1(a_1), f_2(a_2)) \prec (f_1(a_1'), f_2(a_2'))$.

To see the inverse direction, let $(f_1(a_1), f_2(a_2)) \prec (f_1(a_1'), f_2(a_2'))$. Then either $f_1(a_1) \prec_1 f_1(a_1')$ or $f_1(a_1) = f_1(a_1')$ and $f_2(a_2) \prec_2 f_2(a_2')$. In the first case, $f_1(a_1) \prec_1 f_1(a_1')$ and so $a_1 <_1 a_1'$ and so $(a_1, a_2) < (a_1', a_2')$; in the second case, $a_1 = a_1'$ and $a_2 <_2 a_2'$ and so $(a_1, a_2) < (a_1', a_2')$. □

► EXERCISE 124 (4.4.2). *Give an example of linear orderings $(A_1, <_1)$ and $(A_2, <_2)$ such that the sum of $(A_1, <_1)$ and $(A_2, <_2)$ does not have the same order type as the sum of $(A_2, <_2)$ and $(A_1, <_1)$ ("addition of order types is not commutative"). Do the same thing for lexicographic product.*

PROOF. (i) Let $(A_1, <_1) = \left(\mathbb{N} \smallsetminus \{0\}, <^{-1}\right)$, and $(A_2, <_2) = (\mathbb{N}, <)$, where $<$ denotes the usual ordering of numbers by size. Then the sum of $\left(\mathbb{N} \smallsetminus \{0\}, <^{-1}\right)$ and $(\mathbb{N}, <)$ is just $(\mathbb{Z}, <)$. Particularly, there is no greatest element in $(\mathbb{Z}, <)$. However, there is a greatest element in the sum of $(\mathbb{N}, <)$ and $\left(\mathbb{N} \smallsetminus \{0\}, <^{-1}\right)$, namely, -1.

(ii) This is just the case of lexicographic ordering and antilexicographic ordering. □

► EXERCISE 125 (4.4.3). *Prove that the sum and the lexicographic product of two well-orderings are well-orderings.*

PROOF. Let $(A_1, <_1)$ and $(A_2, <_2)$ be two well-ordered sets.

(i) Let $A_1 \cap A_2 = \varnothing$ and $(A, <)$ be the sum of $(A_1, <_1)$ and $(A_2, <_2)$. Let $B \subseteq A$ be nonempty. Write $B = (B \cap A_1) \cup (B \cap A_2)$. Let $B \cap A_1 = B_1$ and $B \cap A_2 = B_2$. Then $B_1 \subseteq A_1$, $B_2 \subseteq A_2$, and $B_1 \cap B_2 = \varnothing$. There are three cases:

- If $B_1 \neq \varnothing$ and $B_2 \neq \varnothing$, then B_1 has a least element b_1, and B_2 has a least element b_2. By definition, $b_1 < b_2$ and so b_1 is the least element of B.

- If $B_1 \neq \varnothing$ and $B_2 = \varnothing$, then B's least element is just b_1.

- If $B_1 = \varnothing$ and $B_2 \neq \varnothing$, then B's least element is just b_2.

(ii) Let $<$ be the lexicographic ordering on $A = A_1 \times A_2$. Take an arbitrary nonempty subset $C \subseteq A$. Let C_1 be the projection of C on A_1. Then $C_1 \neq \varnothing$ and so has a least element $\widehat{c}_1$. Now take the set $\{c_2 \in A_2 \colon (\widehat{c}_1, c_2) \in C\}$. This set is nonempty hence has a least element $\widehat{c}_2$. We now show that $(\widehat{c}_1, \widehat{c}_2)$ is the least element of C: for every $(c_1, c_2) \in C$, either $\widehat{c}_1 < c_1$, or $\widehat{c}_1 = c_1$ and $\widehat{c}_2 < c_2$. In both case, $(\widehat{c}_1, \widehat{c}_2) < (c_1, c_2)$. Thus, $(A, <)$ is well-ordered. □

▶ EXERCISE 126 (4.4.4). *If $\langle A_i : i \in \mathbb{N}\rangle$ is an infinite sequence of linearly ordered sets of natural numbers and$|A_i| \geqslant 2$ for all $i \in \mathbb{N}$, then the lexicographic ordering of $\bigtimes_{i \in \mathbb{N}} A_i$ is* not *a well-ordering.*

PROOF. Because $|A_i| \geqslant 2$ for all $i \in \mathbb{N}$, we can pick $a_i^1 \in A_i$, $a_i^2 \in A_i$, and $a_i^1 < a_i^2$, where $<$ is the usual linear ordering on $\mathbb{N}$. Consider the infinite sequence $\langle \boldsymbol{a}_0, \boldsymbol{a}_1, \ldots\rangle$, where

$$\begin{aligned}
\boldsymbol{a}_0 &= \left\langle a_0^2, a_1^2, a_2^2, a_3^2, a_4^2, \ldots \right\rangle, \\
\boldsymbol{a}_1 &= \left\langle a_0^1, a_1^2, a_2^2, a_3^2, a_4^2, \ldots \right\rangle, \\
\boldsymbol{a}_2 &= \left\langle a_0^1, a_1^1, a_2^2, a_3^2, a_4^2, \ldots \right\rangle, \\
&\cdots
\end{aligned}$$

In this sequence, $\boldsymbol{a}_{n+1} \prec \boldsymbol{a}_n$ by the lexicographic ordering $\prec$. More explicitly, $\operatorname{diff}(\boldsymbol{a}_{n+1}, \boldsymbol{a}_n) = n$, and $\boldsymbol{a}_{n+1}(n) = a_n^1 < a_n^2 = \boldsymbol{a}_n(n)$. Then the set $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots\}$ does not have a least element, that is, the lexicographic ordering of $\bigtimes_{i \in \mathbb{N}} A_i$ is not well-ordering. □

▶ EXERCISE 127 (4.4.5). *Let $\langle (A_i, <_i) : i \in I\rangle$ be an indexed system of mutually disjoint linearly ordered sets, $I \subseteq \mathbb{N}$. The relation $\prec$ on $\bigcup_{i \in I} A_i$ defined by: $a \prec b$ iff either $a, b \in A_i$ and $a <_i b$ for some $i \in I$ or $a \in A_i$, $b \in A_j$ and $i < j$ (in the usual ordering of natural numbers) is a linear ordering. If all $<_i$ are well-orderings, so is $\prec$.*

PROOF. We first show that $\prec$ is a linear ordering (compare with Exercise 49). (Transitivity) Let $a, b, c \in \bigcup_{i \in I} A_i$ with $a \prec b$ and $b \prec c$. If $a, b, c \in A_i$ for some $i \in I$, then $a <_i b$ and $b <_i c$ imply that $a \prec c$; if $a, b \in A_i$, $c \in A_j$, and $i < j$, then $a \prec c$; if $a \in A_i$, $b, c \in A_j$, and $i < j$, then $a \prec c$. (Asymmetry) Let $a, b \in \bigcup_{i \in I} A_i$ and $a \prec b$. If $a, b \in A_i$, then $a <_i b$, which implies that $a \not>_i b$, which implies that $a \not\succ b$; if $a \in A_i$, $b \in A_j$, and $i < j$, then, by definition, $a \not\succ b$. (Linearity) Given $a, b \in \bigcup_{i \in I} A_i$, one of the following cases has to occur: If $a, b \in A_i$ for some $i \in I$, then a, b is comparable since $<_i$ is; if $a \in A_i$, $b \in A_j$, and $i < j$, then $a \prec b$; if $a \in A_i$, $b \in A_j$, and $i > j$, then $b \prec a$.

Now suppose that all $<_i$ are well-orderings. Pick an arbitrary nonempty subset $A \subseteq \bigcup_{i \in I} A_i$. For each $a \in A$, there exists a unique $i_a \in I$ such that $a \in A_{i_a}$. Let

$$I_A = \{i \in I : a \in A_i \text{ for some } a \in A\}.$$

Notice that $I_A \neq \varnothing$. Then I_A has a least element i'. Since $A_{i'}$ is also nonempty, $A_{i'}$ has a least element $a_{i'}$. Hence, $a_{i'}$ is the least element of A. □

► Exercise 128 (4.4.6). *Let $(\mathbb{Z}, <)$ be the set of all integers with the usual linear ordering. Let $\prec$ be the lexicographic ordering of $\mathbb{Z}^{\mathbb{N}}$ as defined in Theorem 4.4.7. Finally, let $FS \subseteq \mathbb{Z}^{\mathbb{N}}$ be the set of all eventually constant elements of $\mathbb{Z}^{\mathbb{N}}$; i.e., $\langle a_i : i \in \mathbb{N}\rangle \in FS$ iff there exists $n_0 \in \mathbb{N}$, $a \in \mathbb{Z}$ such that $a_i = a$ for all $i \geqslant n_0$ (compare with Exercise 117). Prove that FS is countable and $(FS, \prec \cap FS^2)$ is a dense linear ordered set without endpoints.*

Proof. The countability of *FS* is obtained by a similar proof as in Exercise 117. It is also easy to see that $(FS, \prec \cap FS^2)$ is a linear ordered set without endpoints. So we just show that it is dense.

Take two arbitrary elements $\boldsymbol{a} = \langle a_i : i \in \mathbb{N}\rangle$ and $\boldsymbol{b} = \langle b_i : i \in \mathbb{N}\rangle$ in *FS*, and assume that $\boldsymbol{a} \prec \boldsymbol{b}$. Then there exists $n_0 \in \mathbb{N}$ such that $a_{n_0} < b_{n_0}$, where n_0 is the least element of $\operatorname{diff}(\boldsymbol{a}, \boldsymbol{b})$. Define $\boldsymbol{c} = \langle c_i : i \in \mathbb{N}\rangle$ by letting

$$c_i = \begin{cases} a_i & \text{if } i \leqslant n_0 \\ \max\{a_i, b_i\} & \text{if } i > n_0. \end{cases}$$

This infinite sequence $\boldsymbol{c}$ is well-defined since both $\boldsymbol{a}$ and $\boldsymbol{b}$ are eventually constant. Then $\boldsymbol{a} \prec \boldsymbol{c} \prec \boldsymbol{b}$. □

► Exercise 129 (4.4.7). *Let $\prec$ be the lexicographic ordering of $\mathbb{N}^{\mathbb{N}}$ (where $\mathbb{N}$ is assumed to be ordered in the usual way) and let $P \subseteq \mathbb{N}^{\mathbb{N}}$ be the set of all eventually periodic, but not eventually constant, sequences of natural numbers (see Exercises 117 and 118 for definitions of these concepts). Show that $(P, \prec \cap P^2)$ is a countable dense linearly ordered set without endpoints.*

Proof. It is evident that $(P, \prec \cap P^2)$ is a countable linearly ordered set, so we focus on density. Take two arbitrary elements $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}^{\mathbb{N}}$ with $\boldsymbol{a} \prec \boldsymbol{b}$. Then there exists $n_0 \in \mathbb{N}$ such that $a_{n_0} < b_{n_0}$, where n_0 is defined as in the previous exercise. Define $\boldsymbol{c} \in P$ as in the previous exercise, we have $\boldsymbol{a} \prec \boldsymbol{c} \prec \boldsymbol{b}$. □

► Exercise 130 (4.4.8). *Let $(A, <)$ be linearly ordered. Define $\prec$ on $\operatorname{Seq}(A)$ by: $\langle a_0, \ldots, a_{m-1}\rangle \prec \langle b_0, \ldots, b_{n-1}\rangle$ iff there is $k < n$ such that $a_i = b_i$ for all $i < k$ and either $a_k < b_k$ or a_k is undefined (i.e., $k = m < n$). Prove that $\prec$ is a linear ordering. If $(A, <)$ is well-ordered, $(\operatorname{Seq}(A), \prec)$ is also well-ordered.*

Proof. *Transitivity*: Let $\langle a_0, \ldots, a_{m-1}\rangle \prec \langle b_0, \ldots, b_{n-1}\rangle \prec \langle c_0, \ldots, c_{\ell-1}\rangle$. Then there exists $k_1 < n$ such that $a_i = b_i$ for all $i < k_1$ and either $a_{k_1} < b_{k_1}$ or a_{k_1} is undefined. Similarly, there exists $k_2 < \ell$ such that $b_i < c_i$ for all $i < k_2$ and either $b_{k_2} < c_{k_2}$ or b_{k_2} is undefined. Assume that $k_1 < k_2$.

- If $a_i = b_i$ for all $i < k_1$, $a_{k_1} < b_{k_1}$, $b_i = c_i$ for all $i < k_2$, and $b_{k_2} < c_{k_2}$, then $a_i = c_i$ for all $i < k_1$, and $a_{k_1} < c_{k_1}$, i.e., $\langle a_0, \ldots, a_{m-1}\rangle \prec \langle c_0, \ldots, c_{\ell-1}\rangle$.

- If $a_i = b_i$, $k_1 = m < n$, $b_i = c_i$ for all $i < k_2$, and $b_{k_2} < c_{k_2}$, then $a_i = b_i = c_i$ for all $i < k_1$, and a_{k_1} is undefined, i.e., $\langle a_0, \dots, a_{m-1} \rangle \prec \langle c_0, \dots, c_{\ell-1} \rangle$.

- If $a_i = b_i$ for all $i < k_1$, $a_{k_1} < b_{k_1}$, $b_i = c_i$ for all $i < k_2$, and $k_2 = n < \ell$, then $a_i = b_i = c_i$ for all $i < k_1$, and $a_{k_1} < b_{k_1} = c_{k_1}$, i.e., $\langle a_0, \dots, a_{m-1} \rangle \prec \langle c_0, \dots, c_{\ell-1} \rangle$.

We can see that $\langle a_0, \dots, a_{m-1} \rangle \prec \langle c_0, \dots, c_{\ell-1} \rangle$ also holds for $k_1 \geqslant k_2$.

Asymmetry: Follows from definition immediately.

Linearity: Given $\langle a_0, \dots, a_{m-1} \rangle, \langle b_0, \dots, b_{n-1} \rangle \in \operatorname{Seq}(A)$. If $m < n$, then either there exists $k < m$ such that $a_i = b_i$ for all $i < k$ and $a_k < b_k$ or $a_k > b_k$, which implies that $\langle a_0, \dots, a_{m-1} \rangle \prec \langle b_0, \dots, b_{n-1} \rangle$ or $\langle a_0, \dots, a_{m-1} \rangle \succ \langle b_0, \dots, b_{n-1} \rangle$; or $a_i = b_i$ for all $i < m$, which implies that $\langle a_0, \dots, a_{m-1} \rangle \prec \langle b_0, \dots, b_{n-1} \rangle$. All other cases can be analyzed similarly.

Well-ordering: Let $X \subseteq \operatorname{Seq}(A)$ be nonempty, and $(A, <)$ be well-ordered. Let

$$B_i = \{a_i \in A \colon \langle a_0, \dots, a_i, \dots, a_{n-1} \rangle \in X\}.$$

Then $B_i \subseteq A$ is nonempty and so has a least element b_i. The sequence $\langle b_0, \dots, b_{\ell-1} \rangle$ is the least element of X and so $(\operatorname{Seq}(A), \prec)$ is well-ordered. □

► EXERCISE 131 (4.4.10). *Let $(A, <)$ be a linearly ordered set without endpoints, $A \neq \varnothing$. A* closed interval *$[a, b]$ is defined for $a, b \in A$ by $[a, b] = \{x \in A \colon a \leqslant x \leqslant b\}$. Assume that each closed interval $[a, b]$, $a, b \in A$, has a finite number of elements. Then $(A, <)$ is similar to the set $\mathbb{Z}$ of all integers in the usual ordering.*

PROOF. Take arbitrary $a, b \in A$ with $a \leqslant b$. Denote $[a, b]$ as $\{a_{i_0}, a_{i_1}, \dots, a_{i_k}\}$ (since it is finite), where $a_{i_0} = a$ and $a_{i_k} = k$, with $a_{i_0} < \cdots < a_{i_k}$. Let

$$h_{[a,b]} = \left\{(a_{i_0}, 0), (a_{i_1}, 1), \dots, (a_{i_k}, k)\right\}.$$

Clearly, h is a partial isomorphism. Now for any $c \in A$, either $c < a$ or $c > b$. For example, assume that $c < a$. Let $[c, a] = \{c_{j_\ell}, \dots, c_{j_0}\}$, where $c_{j_\ell} = c$ and $c_{j_0} = a$, with $c_{j_\ell} < \cdots < c_{j_0}$. Let

$$h_{[c,a]} = \left\{(c_{j_\ell}, -\ell), \dots, (c_{j_1}, -1), (c_{j_0}, 0)\right\}.$$

Let $h = \bigcup_{a,b \in A} h_{[a,b]}$. Then h is an isomorphism and so $(A, <) \cong (\mathbb{Q}, <)$. □

► EXERCISE 132 (4.4.11). *Let $(A, <)$ be a dense linearly ordered set. Show that for all $a, b \in A$, $a < b$, the closed interval $[a, b]$, as defined in Exercise 131, has infinitely many elements.*

PROOF. If $[a, b]$ has finitely element, then $(A, <) \cong (\mathbb{Z}, <)$. However, $(\mathbb{Z}, <)$ is not dense. □

► EXERCISE 133 (4.4.12). *Show that all countable dense linearly ordered sets with both endpoints are similar.*

PROOF. Let $(P, \prec)$ and $(Q, <)$ be such two sets. Let $\langle p_n \colon n \in \mathbb{N} \rangle$ be an injective sequence such that $P = \{p_n \colon n \in \mathbb{N}\}$, and let $\langle q_n \colon n \in \mathbb{N} \rangle$ be an injective sequence such that $Q = \{q_n \colon n \in \mathbb{N}\}$. We also assume that $p_0 \prec p_1 \prec \cdots \prec \overline{p}$ and $q_0 < q_1 < \cdots < \overline{q}$, where $\overline{p}$ is the greatest element of P and $\overline{q}$ is the greatest element of Q.

Let $h_0 \colon p_0 \mapsto q_0$. Having defined $h_n \colon \{p_0, \ldots, p_n\} \to \{q_0, \ldots, q_n\}$, we let $h_{n+1} \colon h_n \cup \{(p_{n+1}, q_{n+1})\}$. Now let $h = \bigcup_{=0}^{\infty} h_i$. Then h is an isomorphism and so $(P, \prec) \cong (Q, <)$. □

► EXERCISE 134 (4.4.13). *Let* $(\mathbb{Q}, <)$ *be the set of all rational numbers in the usual ordering. Find subsets of* $\mathbb{Q}$ *similar to*

a. *the sum of two copies of* $(\mathbb{N}, <)$*;*

b. *the sum of* $(\mathbb{N}, <)$ *and* $(\mathbb{N}, <^{-1})$*;*

c. *the lexicographic product of* $(\mathbb{N}, <)$ *and* $(\mathbb{N}, <)$*.*

PROOF. For (a) and (b), we take the subset as $\mathbb{Z}$. For (c), let $A = \{m - 1/(n + 1) \colon m, n \in \mathbb{N}, \text{irreducible}\}$. We show that $A \cong \mathbb{N} \times \mathbb{N}$. Let $h \colon A \to \mathbb{N} \times \mathbb{N}$ be defined as $h(m - 1/(n + 1)) = (m, n)$. It is clear that h is bijective. First assume that $m_1 - 1/(n_1 + 1) < m_2 - 1/(n_2 + 1)$. Then it is impossible that $m_1 > m_2$; for otherwise,

$$\frac{1}{n_1 + 1} - \frac{1}{n_2 + 1} > m_2 - m_1 \geqslant 1,$$

which is impossible. If $m_1 < m_2$, there is nothing to prove. So assume that $m_1 = m_2$, but then $n_1 < n_2$ and hence $(m_1, n_1) < (m_2, n_2)$. The other hand can be proved similarly. □

4.5 COMPLETE LINEAR ORDERINGS

REMARK (p. 87). Let $(P, <)$ be a dense linearly ordered set. $(P, <)$ is complete iff it does not have any gaps.

PROOF. We first show that if $(P, <)$ does not have any gaps, then it is complete. Suppose $(P, <)$ is not complete, that is, there is a nonempty set $S \subseteq P$ bounded from above, and S does not have a supremum. Let

$$A = \left\{x \in P \colon x \leqslant s \text{ for some } s \in S\right\},$$
$$B = \left\{x \in P \colon x > s \text{ for every } s \in S\right\}.$$

Then (A, B) is a gap: $A \neq \varnothing$ since $S \subseteq A$, and $B \neq \varnothing$ since S is bounded from above. Next, for every $p \in P$, if $p > s$ for all $s \in S$ then $p \in B$; if $p \leqslant s$ for some $s \in S$ then $p \in A$, i.e., $A \cup B = P$. Finally, $A \cap B = \varnothing$, and if $a \in A$ and $b \in B$ then there exists $s \in S$ such that $a \leqslant s < b$, i.e., $a < b$.

If A has a greatest element, or B has a least element, then A has a supremum, but which means that S has a supremum, too. To see this, let $\sup A = \gamma$. Then $\gamma \geqslant a$ for all $a \in A$, and if $\gamma' < \gamma$, there exists $\widetilde{a} \in A$ such that $\gamma' < \widetilde{a} \leqslant \gamma$. Since $S \subseteq A$, we get $s \leqslant \gamma$ for all $s \in S$. So we need only to prove that there exists $\widetilde{s} \in S$ such that $\gamma' < s \leqslant \gamma$. By definition, there exists $\widetilde{s} \in S$ such that $\widetilde{s} \geqslant \widetilde{a}$; therefore, $\gamma' < \widetilde{a} \leqslant \widetilde{s} \leqslant \gamma$ implies that $\gamma' < \widetilde{s} \leqslant \gamma$ since $<$ is transitive.

For the other direction, assume that $(P, <)$ has a gap (A, B). Then $\varnothing \neq A \subseteq P$, A is bounded from above (since any element of B is an upper bound of A). But A does not have a supremum; hence $(P, <)$ is not complete. □

► EXERCISE 135 (4.5.1). *Prove that there is no $x \in \mathbb{Q}$ for which $x^2 = 2$.*

PROOF. (See Rudin, 1976, for this exercise and Exercise 136.) If there were such a $x \in \mathbb{Q}$, we could write $x = m/n$, where m and n are integers that are not both even. Let us assume this is done. Then $x^2 = 2$ implies

$$m^2 = 2n^2. \tag{4.9}$$

This shows that m^2 is even. Hence m is even (if m were odd, then $m = 2k + 1$, $k \in \mathbb{Z}$, then $m^2 = 2\left(2k^2 + 2k\right) + 1$ is odd), and so m^2 is divisible by 4. It follows that the right side of (4.9) is divisible by 4, so that n^2 is even, which implies that n is even.

The assumption that $x^2 = 2$ holds thus leads to the conclusion that both m and n are even, contrary to our choice of m and n. Thus, $x^2 \neq 2$ for all $x \in \mathbb{Q}$. □

► EXERCISE 136 (4.5.2). *Show that (A, B), where*

$$A = \left\{x \in \mathbb{Q} : x \leqslant 0 \textit{ or } (x > 0 \textit{ and } x^2 < 2)\right\}, B = \left\{x \in \mathbb{Q} : x > 0 \textit{ and } x^2 > 2\right\},$$

is a gap in $(\mathbb{Q}, <)$.

PROOF. To show that (A, B) is a gap in $(\mathbb{Q}, <)$, we need to show (a)–(c) of the definition hold. Since (a) and (b) are clear [note that $\sqrt{2} \notin \mathbb{Q}$ by Exercise 135], we need only to verify (c); that is, A does not have a greatest element, and B does not have a least element.

More explicitly, for every $p \in A$ we can find a rational $q \in A$ such that $p < q$, and for every $p \in B$ such that $q < p$. To to this, we associate with each rational $p > 0$ the number

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}. \tag{4.10}$$

Then

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2}. \tag{4.11}$$

- If $p \in A$ then $p^2 - 2 < 0$, (4.10) shows that $q > p$, and (4.11) shows that $q^2 < 2$. Thus $q \in A$.

- If $p \in B$ then $p^2 - 2 > 0$, (4.10) shows that $0 < q < p$, and (4.11) shows that $q^2 > 2$. Thus $q \in B$. □

► EXERCISE 137 (4.5.3). *Let $0.a_1a_2a_3\cdots$ be an infinite, but not periodic, decimal expansion. Let*

$$A = \left\{x \in \mathbb{Q} \colon x \leqslant 0.a_1a_2\cdots a_k \text{ for some } k \in \mathbb{N} \smallsetminus \{0\}\right\},$$
$$B = \left\{x \in \mathbb{Q} \colon x \geqslant 0.a_1a_2\cdots a_k \text{ for all } k \in \mathbb{N} \smallsetminus \{0\}\right\}.$$

Show that (A, B) is a gap in $(\mathbb{Q}, <)$.

PROOF. It is easy to see that A and B are nonempty, disjoint, and $A \cup B = \mathbb{Q}$. Further, if $a \in A$ and $b \in B$, then there exists $k \in \mathbb{N} \smallsetminus \{0\}$ such that $a \leqslant 0.a_1a_2\cdots a_k < b$.

If A has a greatest element α, then $\alpha = 0.a_1a_2\cdots a_k$ for some $k \in \mathbb{N} \smallsetminus \{0\}$. But $\alpha < 0.a_1a_2\cdots a_k1 \in A$. Similarly, B does not have a least element. □

► EXERCISE 138 (4.5.4). *Show that a dense linearly ordered set $(P, <)$ is complete iff every nonempty $S \subseteq P$ bounded from below has an infimum.*

PROOF. We first suppose $(P, <)$ is complete. Then by definition, every nonempty $S' \subseteq P$ bounded from above has a supremum. Now suppose $\varnothing \neq S \subseteq S$ is bounded from below. Let S' be the set of all lower bounds of S. Since S is bounded from below, $S' \neq \varnothing$, and since S' consists of exactly those $s' \in P$ which satisfy the inequality $s' \leqslant s$ for every $s \in S$, we see that every $s \in S$ is an upper bound of S'. Thus S' is bounded above and

$$\alpha = \sup S'$$

exists in P by definition of completion. We show that indeed $\alpha = \inf S$.

- If $\gamma < \alpha$ then γ is not an upper bound of S', hence $\gamma \notin S$. It follows that $\alpha \leqslant s$ for every $s \in S$ since s is an upper bound of S'. Thus α is an lower bound of S, i.e., $\alpha \in S'$.

- If $\alpha < \beta$ then $\beta \notin S'$, since α is an upper bound of S'.

We have shown that $\alpha \in S'$ but $\beta \notin S'$ if $\beta > \alpha$. In other words, α is a lower bound of S, but β is not if $\beta > \alpha$. This means that $\alpha = \inf S$.

With the same logic, we can prove the inverse direction. Suppose every nonempty $S \subseteq P$ bounded from below has an infimum. Let $\varnothing \neq S' \subseteq P$ is an arbitrary set bounded from above. We want to show that S' has a supremum. Let S be the set of all upper bounds of S'. Since S' is bounded above, $S \neq \varnothing$, and since S consists of exactly those $s \in P$ which satisfy the inequality $s \geqslant s'$ for every $s' \in S'$, we see that every $s' \in S'$ is an lower bound of S. Therefore, S is bounded from below and

$$\beta = \inf S$$

exists in P. We show that $\beta = \sup S'$, too.

- As before, we first show $\beta \in S$. If $\gamma > \beta$, then γ is not an lower bound of S, hence $\gamma \notin S'$. It follows that $s' \leqslant \beta$ for every $s' \in S'$; that is, β is an upper bound of S', so $\beta \in S$.

- If $\alpha < \beta$ then $\alpha \notin S$, since β is an upper bound of S'.

We have shown that $\beta \in S$ but $\alpha \notin S$ if $\alpha < \beta$. Therefore, $\beta = \sup S'$. □

► EXERCISE 139 (4.5.5). *Let D be dense in $(P, <)$, and let E be dense in $(D, <)$. Show that E is dense in $(P, <)$.*

PROOF. It seems that the definition of *denseness* in the Theorem 4.5.3(c) is wrong. We use the definition from Jech (2006):

DEFINITION 4.1. a. A linear ordering $(P, <)$ is *dense* if for all $a < b$ there exists a c such that $a < c < b$.

b. A set $D \subseteq P$ is a *dense subset* if for all $a < b$ in P there exists a $d \in D$ such that $a < d < b$.

Let $p_1, p_2 \in P$ and $p_1 < p_2$. Since D is dense in $(P, <)$, there exists $d_1 \in D$ such that

$$p_1 < d_1 < p_2. \tag{4.12}$$

Because $d_1 \in D \subseteq P$, we know there exists a $d_2 \in D$ such that

$$d_1 < d_2 < p_2. \tag{4.13}$$

Because E is dense in $(D, <)$, there exists $e \in E$ such that

$$d_1 < e < d_2. \tag{4.14}$$

Now combine (4.12)—(4.14) and adopt the fact that $<$ is linear, we conclude that for any $p_1 < p_2$, there exists $e \in E$ such that $p_1 < e < p_2$; that is, E is dense in $(P, <)$. □

► EXERCISE 140 (4.5.8). *Prove that the set $\mathbb{R} \smallsetminus \mathbb{Q}$ of all irrational numbers is dense in $\mathbb{R}$.*

PROOF. We want to show that for any $a, b \in \mathbb{R}$ and $a < b$, there is an $x \in \mathbb{R} \smallsetminus \mathbb{Q}$ such that $a < x < b$. We can chose such an x as follows:

$$x = \begin{cases} (a+b)/2 & \text{if } x \in \mathbb{R} \smallsetminus \mathbb{Q} \\ (a+b)/\sqrt{2} & \text{otherwise.} \end{cases}$$ □

4.6 Uncountable Sets

► Exercise 141 (4.6.1). *Use the diagonal argument to show that $\mathbb{N}^{\mathbb{N}}$ is uncountable.*

Proof. Consider any infinite sequence $\left\langle \boldsymbol{a}_n \in \mathbb{N}^{\mathbb{N}} : n \in \mathbb{N} \right\rangle$, we prove that there is some $\boldsymbol{d} \in \mathbb{N}^{\mathbb{N}}$, and $\boldsymbol{d} \neq \boldsymbol{a}_n$ for all $n \in \mathbb{N}$. This can be done by defining

$$\boldsymbol{d}(n) = \boldsymbol{a}_n(n) + 1.$$

Note that $\boldsymbol{a}_n(n) + 1 \in \mathbb{N}$, and $\boldsymbol{d} \neq \boldsymbol{a}_n$ for all $n \in \mathbb{N}$. □

► Exercise 142 (4.6.2). *Show that* $\left|\mathbb{N}^{\mathbb{N}}\right| = 2^{\aleph_0}$.

Proof. We first show that $\mathbb{N}^{\mathbb{N}} \subseteq \mathcal{P}(\mathbb{N} \times \mathbb{N})$. A generic element of $\mathbb{N}^{\mathbb{N}}$ can be written as $\{(1, a_1), (2, a_2), (3, a_3), \ldots\}$. Since $(n, a_n) \in \mathbb{N} \times \mathbb{N}$ for all $n \in \mathbb{N}$, we have $\{(1, a_1), (2, a_2), \ldots\} \subseteq \mathbb{N} \times \mathbb{N}$; that is, $\{(1, a_1), (2, a_2), \ldots\} \in \mathcal{P}(\mathbb{N} \times \mathbb{N})$. Therefore,

$$2^{\mathbb{N}} \subseteq \mathbb{N}^{\mathbb{N}} \subseteq \mathcal{P}(\mathbb{N} \times \mathbb{N}).$$

Because $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, we have $|\mathcal{P}(\mathbb{N} \times \mathbb{N})| = |\mathcal{P}(\mathbb{N})|$ (by Exercise 143); furthermore, $\left|2^{\mathbb{N}}\right| = |\mathcal{P}(\mathbb{N})|$, so $\left|2^{\mathbb{N}}\right| = |\mathcal{P}(\mathbb{N} \times \mathbb{N})|$. It follows from Cantor-Bernstein Theorem that $\left|\mathbb{N}^{\mathbb{N}}\right| = 2^{\aleph_0} = \mathfrak{c}$. □

► Exercise 143 (4.6.3). *Show that* $|A| = |B|$ *implies* $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.

Proof. Let $f : A \to B$ be a bijection. For every subset $a \subseteq A$, we define a function $g : \mathcal{P}(A) \to \mathcal{P}(B)$ as follows:

$$g(a) = f[a],$$

where $f[a]$ is the image of a under f. Then it is easy to see that g is bijective. Hence, $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. □

5

CARDINAL NUMBERS

5.1 Cardinal Arithmetic

► Exercise 144 (5.1.1). *Prove properties (a)–(n) of cardinal arithmetic stated in the text of this section.*

a. $\kappa + \lambda = \lambda + \kappa$.

b. $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$.

c. $\kappa \leqslant \kappa + \lambda$.

d. *If* $\kappa_1 \leqslant \kappa_2$ *and* $\lambda_1 \leqslant \lambda_2$, *then* $\kappa_1 + \lambda_1 \leqslant \kappa_2 + \lambda_2$.

e. $\kappa \cdot \lambda = \lambda \cdot \kappa$.

f. $\kappa \cdot \big(\lambda \cdot \mu\big) = (\kappa \cdot \lambda) \cdot \mu$.

g. $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

h. $\kappa \leqslant \kappa \cdot \lambda$ *if* $\lambda > 0$.

i. *If* $\kappa_1 \leqslant \kappa_2$ *and* $\lambda_1 \leqslant \lambda_2$, *then* $\kappa_1 \cdot \lambda_1 \leqslant \kappa_2 \cdot \lambda_2$.

j. $\kappa + \kappa = 2 \cdot \kappa$.

k. $\kappa + \kappa \leqslant \kappa \cdot \kappa$, *whenever* $\kappa \geqslant 2$.

l. $\kappa \leqslant \kappa^{\lambda}$ *if* $\lambda > 0$.

m. $\lambda \leqslant \kappa^{\lambda}$ *if* $\kappa > 1$.

n. *If* $\kappa_1 \leqslant \kappa_2$ *and* $\lambda_1 \leqslant \lambda_2$, *then* $\kappa_1^{\lambda_1} \leqslant \kappa_2^{\lambda_2}$.

Proof. We let $|A| = \kappa, |B| = \lambda$, and $|C| = \mu$ throughout this exercise.

(a & b) $A \cup B = B \cup A$, and $A \cup (B \cup C) = (A \cup B) \cup C$.

(c) Let $A \cap B = \varnothing$. Then $\kappa + \lambda = |A \cup B|$. Considering the embedding $\mathrm{Id}_A \colon A \to A \cup B$. Then $|A| \leqslant |A \cup B|$, i.e., $\kappa \leqslant \kappa + \lambda$.

(d) Let $|A_1| = \kappa_1, |A_2| = \kappa_2, |B_1| = \lambda_1, |B_2| = \lambda_2$, $A_1 \cap B_1 = \varnothing = A_2 \cap B_2$, $|A_1| \leqslant |A_2|$, and $|B_1| \leqslant |B_2|$. Let $f\colon A_1 \to A_2$ and $g\colon B_1 \to B_2$ be two injections. Define $h\colon A_1 \cup B_1 \to A_2 \cup B_2$ by letting

$$h(x) = \begin{cases} f(x) & \text{if } x \in A_1 \\ g(x) & \text{if } x \in B_1. \end{cases}$$

Then h is an injection, and so $\kappa_1 + \lambda_1 \leqslant \kappa_2 + \lambda_2$.

(e) Let $f\colon A \times B \to B \times A$ with $f((a,b)) = (b,a)$ for all $(a,b) \in A \times B$. Then f is bijective, and so $|A \times B| = |B \times A|$, i.e., $\kappa \cdot \lambda = \lambda \cdot \kappa$.

(f) By letting $f\colon (a,(b,c)) \mapsto ((a,b),c)$ for all $(a,(b,c)) \in A \times (B \times C)$, we see that $|A \times (B \times C)| = |(A \times B) \times C|$; hence, $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$.

(g) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(h) Pick $b \in B$ (since $\lambda > 0$). Define $f\colon A \to A \times \{b\}$ by letting for all $a \in A$:

$$f(a) = (a,b).$$

Then f is bijective. Since $A \times \{b\} \subseteq A \times B$, we have (h).

(i) Let $|A_1| = \kappa_1, |A_2| = \kappa_2, |B_1| = \lambda_1, |B_2| = \lambda_2$, $\kappa_1 \leqslant \kappa_2$, and $\lambda_1 \leqslant \lambda_2$. Let $f\colon A_1 \to A_2$ and $g\colon B_1 \to B_2$ be two injections. By defining $h\colon A_1 \times B_1 \to A_2 \times B_2$ with

$$h(a,b) = (f(a), g(b)),$$

we see that h is injective. Therefore, $\kappa_1 \cdot \lambda_1 \leqslant \kappa_2 \cdot \lambda_2$.

(j) In the book.

(k) $\kappa + \kappa \leqslant 2 \cdot \kappa \leqslant \kappa \cdot \kappa$ if $\kappa \geqslant 2$, by part (j) and (i).

(l) For every $a \in A$, let $f_a \in A^B$ be defined as $f_a(b) \equiv a$ for all $b \in B$. Then we define a function $F\colon A \to A^B$ by letting $F(a) = f_a$. Then F is injective and so $\kappa \leqslant \kappa^\lambda$ if $\lambda > 0$.

(m) Take $a_1, a_2 \in A$ (since $\kappa > 1$). For every $b \in B$, we define a function $f_b\colon B \to A$ by letting

$$f_b(x) = \begin{cases} a_1 & \text{if } x = b \\ a_2 & \text{if } x \neq b. \end{cases}$$

Then define a function $F\colon B \to A^B$ as $F(b) = f_b$. This function F is injective, and so $|B| \leqslant \left|A^B\right|$.

(n) Let $|A_1| = \kappa_1, |A_2| = \kappa_2, |B_1| = \lambda_1, |B_2| = \lambda_2$, $\kappa_1 \leqslant \kappa_2$, and $\lambda_1 \leqslant \lambda_2$. Let $f\colon A_1 \to A_2$ and $g\colon B_1 \to B_2$ be two injections. For any $k \in A_1^{B_1}$, we can pick a $h_k \in A_2^{B_2}$ such that

$$h_k(x) = \begin{cases} (f \circ k \circ g^{-1})(x) & \text{if } x \in g[B_1] \\ \widehat{b}_2 & \text{if } x \in A_2 \smallsetminus g[B_1], \end{cases}$$

where $\widehat{b}_2 \in B_2$. Then the function $F\colon A_1^{B_1} \to A_2^{B_2}$ defined by $f(k) = h_k$ is injective, and so $\kappa_1^{\lambda_1} \leqslant \kappa_2^{\lambda_2}$. □

► EXERCISE 145 (5.1.2). *Show that $\kappa^0 = 1$ and $\kappa^1 = \kappa$ for all κ.*

PROOF. $\kappa^0 = 1$ because $A^{\varnothing} = \langle\,\rangle$ for all A.

Let $|A| = \kappa$ and $B = \{b\}$. Then $A^{\{b\}} = \{b\} \times A$; that is, $\left|A^{\{b\}}\right| = |A|$. □

► EXERCISE 146 (5.1.3). *Show that $1^\kappa = 1$ for all κ and $0^\kappa = 0$ for all $\kappa > 0$.*

PROOF. Let $A = \{a\}$ and $|B| = \kappa$. In this case, $\{a\}^B = \{f : B \to \{a\} \colon f(b) = a \text{ for all } b \in B\}$; that is, $\left|\{a\}^B\right| = 1 = \left|\{a\}\right|$.

Since $\varnothing^B = \varnothing$ for all B, we have $\left|\varnothing^B\right| = 0 = |\varnothing|$. □

► EXERCISE 147 (5.1.4). *Prove that $\kappa^\kappa \leqslant 2^{\kappa\cdot\kappa}$.*

PROOF. Let $|A| = \kappa$. We look for an injection $F\colon A^A \to \{0,1\}^{A\times A}$. For every element $f \in A^A$, let $F(f)\colon A \times A \to \{0,1\}$ be defined as

$$F(f)(a,b) = \begin{cases} 0 & \text{if } b \neq f(a) \\ 1 & \text{if } b = f(a). \end{cases}$$

To verify F is injective, take arbitrary $f, f' \in A^A$ with $f \neq f'$. Then there exists $a \in A$ such that $f(a) \neq f'(a)$. For the pair $(a, f(a)) \in A \times A$,

$$F(f)(a, f(a)) = 1 \neq 0 = F(f')(a, f(a)).$$

Hence, $F(f) \neq F(f')$ whenever $f \neq f'$. Thus, $\kappa^\kappa \leqslant 2^{\kappa\cdot\kappa}$. □

► EXERCISE 148 (5.1.5). *If $|A| \leqslant |B|$ and if $A \neq \varnothing$, then there is a mapping of B onto A.*

PROOF. Let $f\colon A \to B$ be an injection, and let $a \in A$. Define $g\colon B \to A$ as

$$g(b) = \begin{cases} f^{-1}(b) & \text{if } b \in f[A] \\ a & \text{if } b \in B \smallsetminus f[A]. \end{cases}$$

It is evident that g is surjective. □

► EXERCISE 149 (5.1.6). *If there is a mapping of B onto A, then $2^{|A|} \leqslant 2^{|B|}$.*

PROOF. Let $g\colon B \to A$ be surjective. Define $f\colon \wp(A) \to \wp(B)$ as $f(X) = g^{-1}[X]$. Then f is injective and so $2^{|A|} = |\wp(A)| \leqslant |\wp|\,(B) = 2^{|B|}$. □

► EXERCISE 150 (5.1.7). *Use Cantor's Theorem to show that the "set of all sets" does not exist.*

PROOF. Suppose $\mathcal{U}$ is the "set of all sets". Then $Y = \wp(\bigcup \mathcal{U}) \subseteq \bigcup \mathcal{U}$, and so $|Y| \leqslant \left|\bigcup \mathcal{U}\right|$. But Cantors' Theorem says that $|Y| > \left|\bigcup \mathcal{U}\right|$. A contradiction. □

▶ Exercise 151 (5.1.8). *Let X be a set and let f be a one-to-one mapping of X into itself such that $f[X] \subset X$. Then X is infinite.*

Proof. $f : X \to f[X]$ is bijective, and so $|X| = |f[X]|$. If X is finite, it contradicts Lemma 4.2.2. □

▶ Exercise 152 (5.1.9). *Every countable set is Dedekind infinite.*

Proof. It suffices to consider $\mathbb{N}$. Let $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ be defined as $f(n) = n+1$. Thus, $\mathbb{N}$ is Dedekind infinite. □

▶ Exercise 153 (5.1.10). *If X contains a countable subset, then X is Dedekind infinite.*

Proof. Let $A \subseteq X$ be countable. Then there is an bijection $f : \mathbb{N} \to A$. Define a function $g : X \to X$ by

$$\begin{aligned} g(f(n)) &= f(n+1) && \text{for } n \in \mathbb{N} \\ g(x) &= x && \text{for } x \in X \setminus A \end{aligned}$$

(see Figure 5.1). By this construction, $g : X \to X \setminus \{g(0)\}$ is bijective.

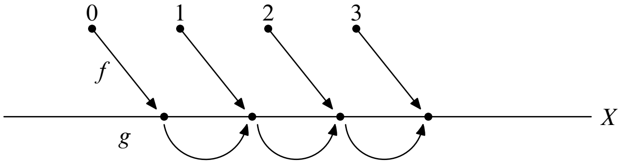

Figure 5.1. $f(0)$ is not in $\Re_g$.

□

▶ Exercise 154 (5.1.11). *If X is Dedekind infinite, then it contains a countable subset.*

Proof. Let X be Dedekind infinite. Then there exists a bijection $f : X \to Y$, where $Y \subset X$. Pick $x \in X \setminus Y$. Let

$$x_0 = x, x_1 = f(x_0), \dots, x_{n+1} = f(x_n), \dots.$$

Then the set $\{x_n : n \in \mathbb{N}\}$ is countable. □

▶ Exercise 155 (5.1.12). *If A and B are Dedekind finite, then $A \cup B$ is Dedekind finite.*

Proof. If A and B are Dedekind finite, then A and B does not contain a countable subset; hence, $A \cup B$ does not contain a countable subset, and so $A \cup B$ is Dedekind finite. □

► EXERCISE 156 (5.1.13). *If A and B are Dedekind finite, then $A \times B$ is Dedekind finite.*

PROOF. If A and B are Dedekind finite, then A and B does not contain a countable subset; hence, $A \times B$ does not contain a countable subset, and so $A \times B$ is Dedekind finite. □

► EXERCISE 157 (5.1.14). *If A is infinite, then $\mathcal{P}(\mathcal{P}(A))$ is Dedekind infinite.*

PROOF. For each $n \in \mathbb{N}$, let

$$S_n = \left\{X \subset A \colon |X| = n\right\}.$$

The set $\{S_n \colon n \in \mathbb{N}\}$ is a countable subset of $\mathcal{P}(\mathcal{P}(A))$, and hence $\mathcal{P}(\mathcal{P}(A))$ is Dedekind infinite. □

5.2 The Cardinality of the Continuum

► EXERCISE 158 (5.2.1). *Prove that the set of all finite sets of reals has cardinality $\mathfrak{c}$.*

PROOF. Every finite set of reals can be written as a finite union of open intervals with rational endpoints. For example, we can write $\{a, b, c\}$ as $(a, b) \cup (b, c)$. Thus, the cardinality of the set of all finite sets of reals is $\mathfrak{c}$. □

► EXERCISE 159 (5.2.2). *A real number x is* algebraic *if it is a solution of some equation*

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \tag{$*$}$$

where $a_0, \dots, a_n$ are integers. If x is not algebraic, it is called transcendental. *Show that the set of all algebraic numbers is countable and hence the set of all transcendental numbers has cardinality $\mathfrak{c}$.*

PROOF. Let $\mathcal{A}_n$ denote the set of algebraic numbers that satisfy polynomials of the form $a_kx^k + \cdots + a_1x + a_0$ where $k < n$ and $\max\{|a_j|\} < n$. Note that there are at most n^n polynomials of this form, and each one has at most n roots. Hence, $\mathcal{A}_n$ is a finite set having at most $n^{n+1} < \aleph_0$ elements. Let $\mathcal{A}$ denote the set of all algebraic numbers. Then $|\mathcal{A}| = \left|\bigcup_{n\in\mathbb{N}} \mathcal{A}_n\right| \leqslant \aleph_0 \cdot \aleph_0 = \aleph_0$.

On the other hand, consider the following set of algebraic numbers:

$$\mathcal{A}' = \{x \in \mathbb{R} \colon a_0 + x = 0, a_0 \in \mathbb{Z}\}.$$

Obviously, $|\mathcal{A}'| = |\mathbb{Z}|$ and so $|\mathcal{A}| \geqslant |\mathbb{Z}| = \aleph_0$. It follows from Cantor-Benstein Theorem that $|\mathcal{A}| = \aleph_0$. □

► EXERCISE 160 (5.2.4). *The set of all closed subsets of reals has cardinality $\mathfrak{c}$.*

Proof. Let $\mathscr{C}$ be the set of closed sets in $\mathbb{R}$, and $\mathscr{O}$ the set of open sets in $\mathbb{R}$. A set $E \in \mathscr{C}$ iff $\mathbb{R} \smallsetminus E \in \mathscr{O}$; that is, there exists a bijection $f\colon \mathscr{C} \to \mathscr{O}$ defined by $f(E) = \mathbb{R} \smallsetminus E$. Thus, $|\mathscr{C}| = |\mathscr{O}| = \mathfrak{c}$ by Theorem 5.2.6(b). □

► Exercise 161 (5.2.5). *Show that, for* $n > 0$*,* $n \cdot 2^{\mathfrak{c}} = \aleph_0 \cdot 2^{\mathfrak{c}} = \mathfrak{c} \cdot 2^{\mathfrak{c}} = 2^{\mathfrak{c}} \cdot 2^{\mathfrak{c}} = (2^{\mathfrak{c}})^n = (2^{\mathfrak{c}})^{\aleph_0} = (2^{\mathfrak{c}})^{\mathfrak{c}} = 2^{\mathfrak{c}}$*.*

Proof. We have

$$2^{\mathfrak{c}} \leqslant n \cdot 2^{\mathfrak{c}} \leqslant \aleph_0 \cdot 2^{\mathfrak{c}} \leqslant \mathfrak{c} \cdot 2^{\mathfrak{c}} \leqslant 2^{\mathfrak{c}} \cdot 2^{\mathfrak{c}} = 2^{\mathfrak{c}+\mathfrak{c}} = 2^{\mathfrak{c}},$$

$$2^{\mathfrak{c}} \leqslant (2^{\mathfrak{c}})^n \leqslant (2^{\mathfrak{c}})^{\aleph_0} \leqslant (2^{\mathfrak{c}})^{\mathfrak{c}} \leqslant= 2^{\mathfrak{c}^2} = 2^{\mathfrak{c}},$$

and

$$2^{\mathfrak{c}} \leqslant n^{\mathfrak{c}} \leqslant \aleph_0^{\mathfrak{c}} \leqslant (2^{\aleph_0})^{\mathfrak{c}} = 2^{\aleph_0 \cdot \mathfrak{c}} = 2^{\mathfrak{c}}.$$

Thus, by the Cantor-Bernstein Theorem, we get the result. □

► Exercise 162 (5.2.6). *The cardinality of the set of all discontinuous functions is* $2^{\mathfrak{c}}$*.*

Proof. Let $\mathscr{C}$ denote the set of all continuous functions, and $\mathscr{D}$ the set of all discontinuous functions. Suppose that $|\mathscr{D}| = \kappa < 2^{\mathfrak{c}}$. Then by Cantor's Theorem,

$$\left|\mathbb{R}^{\mathbb{R}}\right| = |\mathscr{D}| + |\mathscr{C}| = \kappa + \mathfrak{c} < 2^{\kappa+\mathfrak{c}} \leqslant 2^{2^{\mathfrak{c}}+\mathfrak{c}}.$$

Since

$$2^{\mathfrak{c}} + \mathfrak{c} \leqslant 2^{\mathfrak{c}} + 2^{\mathfrak{c}} = 2 \cdot 2^{\mathfrak{c}} = 2^{\mathfrak{c}}$$

by Exercise 161, we have

$$\left|\mathbb{R}^{\mathbb{R}}\right| < 2^{\mathfrak{c}} = \left|\mathbb{R}^{\mathbb{R}}\right|.$$

A contradiction. □

► Exercise 163 (5.2.7). *Construct a one-to-one mapping of* $\mathbb{R} \times \mathbb{R}$ *onto* $\mathbb{R}$*.*

Proof. Using the hints. □

6

ORDINAL NUMBERS

6.1 Well-Ordered Sets

► Exercise 164 (6.1.1). *Give an example of a linearly ordered set* $(L, <)$ *and an initial segment* S *of* L *which is not of the form* $\{x : x < a\}$*, for any* $a \in L$*.*

Proof. We know from Lemma 6.1.2 that if L is a well-ordered set, then every initial segment is of the form $L[a]$ for some $a \in L$. Hence, we have to find a linear ordered set which is *not* well-ordered. We also know from Lemma 4.4.2 that every linear ordering on a finite set is a well-ordering. Therefore, our fist task is to find an infinite linear ordered $(L, <)$ which is not well-ordered.

As an example, let $L = \mathbb{R}$ and $S = (-\infty, 0]$. Then $(\mathbb{R}, <)$ is a linear ordered set, and S is an initial segment of L, but $S \neq \mathbb{R}[a]$ for any $a \in \mathbb{R}$. □

► Exercise 165 (6.1.2). $\omega + 1$ *is not isomorphic to* ω *(in the well-ordering by* $\in$*).*

Proof. We first show that $\omega = \mathbb{N}$ is an initial segment of $\omega + 1$. By definition, $\omega + 1 = \omega \cup \{\omega\}$, so $\omega \subset \omega + 1$. Choose any $\alpha \in \omega$, and let $\beta \in \alpha$. Both α and β are natural numbers, and so $\beta \in \omega$. Then, by Corollary 6.1.5 (a), $\omega + 1$ is not isomorphic to ω since $\omega + 1$ is a well-ordered sets. □

► Exercise 166 (6.1.3). *There exist* $2^{\aleph_0}$ *well-orderings of the set of all natural numbers.*

Proof. There are $\aleph_0^{\aleph_0} = \mathfrak{c}$ well-orderings on $\mathbb{N}$. □

► Exercise 167 (6.1.4). *For every infinite subset* A *of* $\mathbb{N}$*,* $(A, <)$ *is isomorphic to* $(\mathbb{N}, <)$.

Proof. Let $A \subseteq \mathbb{N}$ be infinite. Notice that $(A, <)$ is a well-ordered set, and A is not an initial segment of $\mathbb{N}$; for otherwise, $A = \mathbb{N}[n]$ for some $n \in \mathbb{N}$ and so A is finite.

A cannot be isomorphic to $\mathbb{N}[n]$ for all $n \in \mathbb{N}$ since $\mathbb{N}[n]$ is finite; similarly, $A[n]$ cannot be isomorphic to $\mathbb{N}$. Hence, by Theorem 6.1.3, A is isomorphic to $\mathbb{N}$. □

▶ EXERCISE 168 (6.1.5). *Let $(W_1, <_1)$ and $(W_2, <_2)$ be disjoint well-ordered sets, each isomorphic to $(\mathbb{N}, <)$. Show that the sum of the two linearly ordered sets is a well-ordering, and is isomorphic to the ordinal number $\omega + \omega = \{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2, \dots\}$.*

PROOF. Let $(W, \prec)$ be the sum of $(W_1, <_1)$ and $(W_2, <_2)$. We have known that $(W, \prec)$ is a linearly ordered set. To see $(W, \prec)$ is well-ordered, take an arbitrary nonempty set $X \subset W$. Then $X = (W_1 \cap X) \cap (W_2 \cap X)$, and $(W_1 \cap X) \cap (W_2 \cap X) = \varnothing$. For $i = 1, 2$, if $W_i \cap X \neq \varnothing$, then it has a least element α_i. Let $\alpha = \min\{\alpha_1, \alpha_2\}$. Then α is the least element of X.

Let $f_i \colon W_i \to \mathbb{N}$, $i = 1, 2$, be two isomorphisms. To see $(W, \prec) \cong (\omega + \omega, <)$, let $f \colon W_1 \cup W_2 \to \omega + \omega$ be defined as

$$f(w) = \begin{cases} f_1(w) & \text{if } w \in W_1 \\ \omega + f_2(w) & \text{if } w \in W_2. \end{cases}$$

It is clear that f is an isomorphism and so $(W, <) \cong (\omega + \omega, <)$. □

▶ EXERCISE 169 (6.1.6). *Show that the lexicographic product $(\mathbb{N} \times \mathbb{N}, <)$ is isomorphic to $\omega \cdot \omega$.*

PROOF. Define a function $f \colon \mathbb{N} \times \mathbb{N} \to \omega \cdot \omega$ as follows: for an arbitrary $(m, n) \in \mathbb{N} \times \mathbb{N}$,

$$f(m, n) = \omega \cdot m + n.$$

Clearly, f is bijective. To see f is an isomorphism, let $(m, n) < (p, q)$. Then either $m < p$ or $m = p$ and $n < q$. For every case, $\omega \cdot m + n < \omega \cdot p + q$. □

▶ EXERCISE 170 (6.1.7). *Let $(W, <)$ be a well-ordered set, and let $a \notin W$. Extend $<$ to $W' = W \cup \{a\}$ by making a greater than all $x \in W$. Then W has smaller order type than W'.*

PROOF. We have $W'[a] = W$. Define a bijection $f \colon W \to W'[a]$ as $f(x) = x$ for all $x \in W$. Then f is an isomorphism. □

▶ EXERCISE 171 (6.1.8). *The sets $W = \mathbb{N} \times \{0, 1\}$ and $W' = \{0, 1\} \times \mathbb{N}$, ordered lexicographically, are nonisomorphic well-ordered sets.*

PROOF. See Figures 6.1 and 6.2. The first ordering is isomorphic to $(\omega, <)$, but the second ordering is isomorphic to $(\omega + \omega, <)$. Since $\omega + \omega$ is not isomorphic to ω (by Exercise 165, we get the result.

6.2 ORDINAL NUMBERS

REMARK. Let A be a nonempty set of ordinals. Take $\alpha \in A$, and consider the set $\alpha \cap A$.

$$\begin{tikzcd}
(0,1) \arrow[dr] & (1,1) \arrow[dr] & (2,1) \arrow[dr] & (3,1) & \cdots \\
(0,0) \arrow[u] & (1,0) \arrow[u] & (2,0) \arrow[u] & (3,0) \arrow[u] & \cdots
\end{tikzcd}$$

FIGURE 6.1. The lexicographic ordering on $\mathbb{N} \times \{0, 1\}$.

$$\begin{tikzcd}
(1,0) \arrow[r] & (1,1) \arrow[r] & (1,2) \arrow[r] & (1,3) \arrow[r] & \cdots \\
(0,0) \arrow[r] & (0,1) \arrow[r] & (0,2) \arrow[r] & (0,3) \arrow[r] & \cdots \arrow[to=1-1, rounded corners]
\end{tikzcd}$$

FIGURE 6.2. The lexicographic ordering on $\{0, 1\} \times \mathbb{N}$.

□

a. If $\alpha \cap A = \varnothing$, then α is the least element of A.

b. If $\alpha \cap A \neq \varnothing$, then γ, where γ is the least element of $\alpha \cap A$, is the least element of A.

PROOF. (a) If $\alpha \cap A = \varnothing$, then $\beta \notin \alpha$ for every $\beta \in A$. It follows from Theorem 6.2.6(c) that $\alpha \leqslant \beta$ for all $\beta \in A$. Hence, α is the least element of A.

(b) For every $\beta \in A$, if $\beta \notin \alpha$, then $\alpha \leqslant \beta$; if $\beta \in \alpha$, then $\beta < \alpha$. If $\alpha \cap A \neq \varnothing$, it has a least element γ in the ordering $\in_\alpha$; that is $\gamma \leqslant \beta$ for any $\beta \in \alpha \cap A$. Further, since $\gamma \in \alpha \cap A \subseteq \alpha$, we have $\gamma < \alpha$ and $\gamma \in A$. In sum,

$$\begin{cases} \gamma < \alpha \leqslant \beta & \text{if } \beta \in A \smallsetminus \alpha \\ \gamma \leqslant \beta & \text{if } \beta \in A \cap \alpha. \end{cases}$$

Hence, γ is the least element of A. □

► EXERCISE 172 (6.2.1). *A set X is transitive if and only if $X \subseteq \mathcal{P}(X)$.*

PROOF. Take an arbitrary $x \in X$. If X is transitive, then $x \subseteq X$, and so $x \in \mathcal{P}(X)$, i.e., $X \subseteq \mathcal{P}(X)$. On the other hand, if $X \subseteq \mathcal{P}(X)$, then $x \in X$ implies that $x \in \mathcal{P}(X)$, which is equivalent to $x \subseteq X$; hence X is transitive. □

► EXERCISE 173 (6.2.2). *A set X is transitive if and only if $\bigcup X \subseteq X$.*

PROOF. Take any $x \in \bigcup X$, then there exists $x_i \in X$ such that $x \in x_i$, that is, $x \in x_i \in X$; therefore, $x \in X$ if X is transitive and so $\bigcup X \subseteq X$. To see the converse direction, let $\bigcup X \subseteq X$. Take any $x \in \bigcup X$. There exists $x_i \in X$ such that $x \in x_i$; but $x \in X$ since $\bigcup X \subseteq X$, so X is transitive. □

► EXERCISE 174 (6.2.3). *Are the following sets transitive?*

a. $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$,

b. $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$,

c. $\{\varnothing, \{\{\varnothing\}\}\}$.

Proof. (a) and (b) are transitive. However, (c) is not since $\{\varnothing\} \in \{\{\varnothing\}\}$, but $\{\varnothing\} \notin \{\varnothing, \{\{\varnothing\}\}\}$. □

► Exercise 175 (6.2.4). *Which of the following statements are true?*

a. *If X and Y are transitive, the $X \cup Y$ is transitive.*

b. *If X and Y are transitive, the $X \cap Y$ is transitive.*

c. *If $X \in Y$ and Y is transitive, then X is transitive.*

d. *If $X \subseteq Y$ and Y is transitive, then X is transitive.*

e. *If Y is transitive and $S \subseteq \mathcal{P}(Y)$, then $Y \cup S$ is transitive.*

Proof. (a), (b), and (e) are correct. □

► Exercise 176 (6.2.5). *If every $X \in S$ is transitive, then $\bigcup S$ is transitive.*

Proof. Let $u \in v \in \bigcup S$. Then there exists $X \in S$ such that $u \in v \in X$ and so $u \in X$ since X is transitive. Therefore, $u \in \bigcup S$, i.e., $\bigcup S$ is transitive. □

► Exercise 177 (6.2.7). *If a set of ordinals X does not have a greatest element, then* $\sup X$ *is a limit ordinal.*

Proof. If X does not have a greatest element, then $\sup X > \alpha$ for all $\alpha \in X$, and $\sup X$ is the least such ordinal. If there were β such that $\sup X = \beta + 1$, then β would be the greatest element of X. A contradiction. □

► Exercise 178 (6.2.8). *If X is a nonempty set of ordinals, then $\bigcap X$ is an ordinal. Moreover, $\bigcap X$ is the least element of X.*

Proof. If $u \in v \in \bigcap X$, then $u \in v \in \alpha$ for all $\alpha \in X$, and so $u \in \alpha$ for all $\alpha \in X$, i.e., $u \in \bigcap X$. Hence, $\bigcap X$ is transitive. It is evident to see that $\bigcap X$ is well-ordered. Thus, $\bigcap X$ is an ordinal. For every $\alpha \in X$, we have $\bigcap X \subseteq \alpha$; hence, $\bigcap X \leqslant \alpha$ for all $\alpha \in X$.

We finally show that $\bigcap X \in X$. If not, then $\bigcap X < \gamma$, where γ is the least element of X. It is impossible. □

References

[1] Apostol, Tom M. (1974) *Mathematical Analysis*: Pearson Education, 2nd edition. [58]

[2] Hrbacek, Karel and Thomas Jech (1999) *Introduction to Set Theory*, **220** of Pure and Applied Mathematics: A Series of Monographs and Textbooks, New York: Taylor & Francis Group, LLC, 3rd edition. [i]

[3] Jech, Thomas (2006) *Set Theory*, Springer Monographs in Mathematics, Berlin: Springer-Verlag, the third millennium edition. [67]

[4] Rudin, Walter (1976) *Principles of Mathematical Analysis*, New York: McGraw-Hill Companies, Inc. 3rd edition. [65]