MATH 2220

Logic and Set Theory

author
Dr. Paul Vrbik

based on the lecture notes of
Dr. Gregory H. Moore

latest edit
November 15, 2015

THE UNIVERSITY OF
NEWCASTLE
AUSTRALIA

Contents

1 Introduction

1.1 Logic

Our axioms for set theory will be expressed in a *formal language*. Intuitively, the symbol $\exists$ means "there exists", as in our first axiom:

$$\exists x(x = x).$$

Now we can define what we mean by a *formula* in our formal language. Any formula is built up out of our two relation symbols "$=$" and "$\in$", where "$\in$" is intended to mean "is a member of" or "is an element of." Likewise, we need variables, such as w, x, y, z, A, B, C, with or without subscripts. Thus "$x \in y$" means "x is a member of the set y."

Definition 1.1. For any variables x and y,

1. $x = y$ is a formula,
2. $x \in y$ is a formula,
3. If φ is a formula and ψ is a formula, then the following are also formulas:
   (a) $\varphi \vee \psi$,
   (b) $\varphi \wedge \psi$,
   (c) $\varphi \implies \psi$,
   (d) $\varphi \iff \psi$.
4. If ψ is a formula, then $\neg\psi$ is a formula.
5. If φ is a formula, then $\exists x(\varphi)$ is a formula.
6. If ψ is a formula, then $\forall x(\psi)$ is a formula.
7. ψ is a formula only if ψ can be obtained from clauses 1 to 6.

Example 1.2. Each of the following is a formula of set theory:

1. $x = z \vee x \in z$,
2. $\forall w(w \in x \implies \neg(w \in y))$,
3. $\forall z(z \in x \iff z \in y)$,
4. $\exists w(w \in x) \vee \forall z(z \in y)$.

Example 1.3. Each of the following are *not* formulas of set theory:

1. $(x = y) = z$,
2. $(x \in y) \in z$,
3. $(c \implies y) \in z$.

1.2 Axioms of Set Theory

We give a precise statement of each axiom in our formal language, and then give a rough, intuitive, equivalent in prose (i.e. plain language). Proofs depend on the formal language, *not* on the intuitive equivalents. (We list them here and revisit them individually in the following sections.)

Axiom 1 (Extensionality). If two sets have the same members, then the sets are identical.

$$\forall x \forall y \left[\forall z \left(z \in x \iff z \in y\right) \iff x = y\right].$$

Axiom 2 (Replacement). If the domain of a functional is a set, then its range is also a set.

$$\theta(x, y) \text{ is a functional} \implies \forall A \, \exists B \, \forall y \left[y \in B \iff \exists x \left[x \in A \wedge \theta(x, y)\right]\right].$$

Axiom 3 (Set Existence). There is at least one set:

$$\exists A \left[A = A\right].$$

Axiom 4 (Power Set). For each set A there is a set containing all the subsets of A.

$$\forall A \, \exists C \, \forall x \left[x \in C \iff x \subseteq A\right].$$

Axiom 5 (Union). If A is a set, then the union of A is a set.

$$\forall A\, \exists w\, \forall z\, [z \in w \iff \exists y\, [z \in y \wedge y \in A]].$$

Axiom 6 (Infinity). There is an inductive set. (See §?? for more details.)

$$\exists A\, [A \text{ is inductive}].$$

Axiom 7 (Choice). Every set has a choice function. (See §6.1 for more details.)

1.3 Subsets, the Empty Set, No Universal Set

Our first axiom gives us a condition which guarantees that two sets x and y are identical:

Axiom 1 (Extensionality). If two sets have the same members, then the sets are identical.

$$\forall x \forall y\, [\forall z\, (z \in x \iff z \in y) \implies x = y].$$

We next introduce the ideas of a *subset* and *proper subset*:

Definition 1.4. $A \subseteq B$ states that A "is a subset of" B.

$$A \subseteq B \overset{\text{defn.}}{\iff} \forall z\, [z \in A \implies z \in B].$$

Theorem 1.5. The subset operation is reflexive.

$$A \subseteq B \wedge B \subseteq A \iff A = B.$$

Proof.

$$\begin{aligned}
&A \subseteq B \wedge B \subseteq A \\
&\quad \iff \forall z\, [z \in A \implies z \in B] \wedge \forall z\, [z \in B \implies z \in A] && \text{Def. 1.4} \\
&\quad \iff \forall z\, [z \in A \implies z \in B \wedge z \in B \implies z \in A] \\
&\quad \iff \forall z\, [z \in A \iff z \in B] \\
&\quad \iff A = B. && \text{Extensionality}
\end{aligned}$$

∎

Theorem 1.6. The subset operation is transitive.

$$[A \subseteq B \land B \subseteq C] \implies A \subseteq C.$$

Proof. Let $x \in A$ be arbitrary

$$\begin{aligned}
&[A \subseteq B \land B \subseteq C] \\
&\quad \implies \forall x\,(x \in A \implies x \in B \land x \in B \implies x \in C) && \text{Def. 1.4} \\
&\quad \implies \forall x\,(x \in A \implies x \in C) && \text{Transitivity}
\end{aligned}$$

■

Definition 1.7. $A \subset B$ states that A "is a proper subset" of B.

$$A \subset B \overset{\text{defn.}}{\iff} [A \subseteq B \land \neg\,(B \subseteq A)]$$

Definition 1.8. Some extra notation for negation:

1. $A \neq B \overset{\text{defn.}}{\iff} \neg\,(A = B)$,
2. $A \notin B \overset{\text{defn.}}{\iff} \neg\,(A \in B)$.

Theorem 1.9. Proper subsets cannot be equal to the subset they are contained in.

$$A \subset B \iff (A \subseteq B \land A \neq B)\,.$$

Proof.

$$\begin{aligned}
&A \subset B \\
&\quad \iff A \subseteq B \land \neg(B \subseteq A) && \text{Def. 1.7} \\
&\quad \iff [A \subseteq B \land \neg(A \subseteq B)] \lor [A \subseteq B \land \neg(B \subseteq A)] \\
&\quad \iff A \subseteq B \land \neg(A \subseteq B \land B \subseteq A) \\
&\quad \iff A \subseteq B \land \neg(A = B) && \text{Thm. 1.5} \\
&\quad \iff A \subseteq B \land A \neq B && \text{Def. 1.8.1}
\end{aligned}$$

■

Exercise 1.10.

$$(A \subset B \land B \subseteq C \implies A \subset C) \land A \subseteq B \land B \subset C \implies A \subset C.$$

We wish to have a way to express that a formula is true for exactly one set y:

Definition 1.11. There exists exactly one y such that $\varphi(y)$:

$$\exists! y\ \varphi(y) \overset{\text{defn.}}{\iff} \exists y\,[\varphi(y) \wedge \forall z\,(\varphi(z) \implies y = z)]$$

where z does not occur in $\varphi(y)$.

In order to express our next axiom, we need the idea that a formula $\varphi(x, y)$ of set theory is a *functional*.

Definition 1.12 (Functional). $\varphi(x, y)$ is functional *if an only if*

$$\forall x\,\forall y\,\forall z\,[(\varphi(x, y) \wedge \varphi(x, z)) \implies y = z].$$

A functional, like a *function*, must satisfy the "vertical line test" $f(x) = a$ and $f(y) = a$ implies $x = y$.

Axiom 2 (Replacement). If the domain of a functional is a set, then its range is also a set.

$$\begin{aligned}&\theta(x, y) \text{ is a functional}\\ &\quad\implies \forall A\ \exists B\ \forall y\,[y \in B \iff \exists x\,[x \in A \wedge \theta(x, y)]].\end{aligned}$$

In order to get started, we need to assume that there is at least one set, and that is what our next axiom states:

Axiom 3 (Set Existence). There is at least one set:

$$\exists A\,[A = A].$$

Then we can prove that :

Theorem 1.13. There is exactly one set with no members:

$$\exists! B\ \forall y\,(y \notin B)$$

Proof of Existence. Let $\theta(x, y) \iff \bot$ and note that θ is a functional because

$$\theta(x, y) \wedge \theta(x, z) \equiv \bot \implies y = z$$

is a tautology. We have $\exists A\,(A = A)$ by the the Set Existence Axiom and the Axiom of Replacement implies

$$\begin{aligned}\exists B\,\forall y\,(y \in B &\iff \exists x\,(x \in A \wedge \bot))\\ &\implies \exists B\,\forall y\,(y \in B \iff \bot)\\ &\implies \exists B\,\forall y\,(y \notin B).\end{aligned}$$

Proof of Uniqueness. Suppose there are two sets, $A \neq B$ with no members:

$$\forall x\,(x \notin A \wedge x \notin B) \wedge A \neq B.$$

Notice though, that

$$\forall x\,(x \in A \iff x \in B) \equiv \forall x\,(\bot \iff \bot) \equiv \top.$$

So by the Axiom of Extensionality we have $A = B$ ↯.

This set B with no members is called the *empty set*, or the *null set*, and is written $\varnothing$.

> Distinguish carefully between the empty set $\varnothing$ and φ — an arbitrary formula of set theory.

Definition 1.14 (empty set)**.**

$$\varnothing = w \overset{\text{defn.}}{\iff} \forall y\,(y \notin w)$$

Theorem 1.15. 1. $\forall x\,(x \notin \varnothing)$,

2. $\forall x\,(\varnothing \subseteq x)$, and

3. $\forall x\,(x \subseteq \varnothing \implies x = \varnothing)$.

Proof of 1. Let $x = y$ and $B = \varnothing$ in Definition 1.14. We deduce

$$\begin{aligned} \varnothing = \varnothing &\iff \forall x\,(x \notin \varnothing) \\ &\implies \top \iff \forall x\,(x \notin \varnothing) && \text{Tautology} \\ &\implies \forall x\,(x \notin \varnothing). \end{aligned}$$

Proof of 2. Let x be an arbitrary set.

$$\begin{aligned} &\forall z\,(z \in \varnothing \implies z \in x) \iff \varnothing \subseteq x && \text{Def. 1.4} \\ &\implies \forall z\,(\bot \implies z \in x) \iff \varnothing \subseteq x && \text{Thm. 1.15} \\ &\implies \forall z\,(\top) \iff \varnothing \subseteq x && \text{Tautology} \\ &\implies \varnothing \subseteq x. \end{aligned}$$

Proof of 3. Let x be an arbitrary set

$$\begin{aligned}
x \subseteq \varnothing &\iff \forall z\,(z \in x \implies z \in \varnothing) && \text{Def. 1.4}\\
&\implies \forall z\,(z \in x \implies \bot) && \text{Thm. 1}\\
&\implies \forall z\,(\top \implies \neg(z \in x)) && \text{Contrapositive}\\
&\implies \forall z\,(z \notin x)\\
&\implies x = \varnothing && \text{Def. 1.14}
\end{aligned}$$

■

We might think that there is a "universal set" which contains every set as a member. But we can prove there is no such set of all:

Theorem 1.16 (Russel's Paradox)**.**

$$\neg\exists A \forall x\,(x \in A).$$

Proof. Suppose there is *universal set* U containing all sets

$$\exists U\,\forall x\,(x \in U).$$

Write U with *class abstraction* by

$$U = \{x : x \notin x\}$$

as $\forall x\,(x \notin x) \equiv \top$. However this derives contradiction because

$$U \in U \iff U \notin U.$$

Thus there is no universal set. ■

1.4 Class Abstraction, or $\{x : \varphi(x)\}$

Intuitively, $\{x : \varphi(x)\}$ is intended to be the set of all those sets x such that $\varphi(x)$ is true. But then $\{x : \varphi(x)\}$ could be "too big" to be a set. In particular, $\{x : x = x\}$ would be the set of *all* sets. But we know from Theorem 1.16 that there is no such set. So when $\{x : \varphi(x)\}$ would be too big to be a set, we define $\{x : \varphi(x)\}$ to be some fixed set; the only fixed set so far being the empty set.

Definition 1.17 (Class Abstraction)**.**

$$\{z : \varphi(z)\} = w \overset{\text{defn.}}{\iff}$$

$$\forall x\,[x \in w \iff \varphi(x)] \vee (\neg\exists A\,\forall x\,[x \in A \iff \varphi(x)] \wedge w = \varnothing).$$

(The second condition covers the case of w being empty.)

Theorem 1.18. $\{z : z \in x\} = x$.

Theorem 1.19.

$$\begin{aligned}\forall x\,[x \in \{z : \varphi(z)\} &\iff \varphi(x)]\\ &\vee (\neg\exists A\,\forall x\,[x \in A \iff \varphi(x)] \wedge \{z : \varphi(z)\} = \varnothing)\end{aligned}$$

That is to say,

$$\{x : \varphi(z)\} \neq \varnothing \implies [x \in \{z : \varphi(z)\} \iff \varphi(x)].$$

Proof. Let $w = \{z : \varphi(z)\}$ in Definition 1.17.

$$\begin{aligned}\{z : \varphi(z)\} = \{z : \varphi(z)\}&\\ \iff \forall x\,[x \in \{z : \varphi(z)\} &\iff \varphi(x)]\\ \vee (\neg\exists A\,\forall x\,[x \in A &\iff \varphi(x)] \wedge \{z : \varphi(z)\} = \varnothing)\end{aligned}$$

Thus, because $\{z : \varphi(z)\} = \{z : \varphi(z)\} \equiv \top$ the result follows. ∎

Given some predicate $\varphi(x)$ we can be sure that

$$\exists A x\,[x \in A \iff \varphi(x)]$$

provided there is some set C such that $\{x : \varphi(x)\} \subseteq C$.

Theorem 1.20.

$$\exists C\,\forall z\,[\varphi(z) \implies z \in C] \implies \exists! A\,\forall z\,[z \in A \iff \varphi(z)]$$

Proof. Bounty. ∎

From 1.19 and 1.20 if follows (easily) that From 1.19 and 1.20 if follows (easily) that

Theorem 1.21.

$$\exists C\,\forall z\,[\varphi(z) \implies z \in C] \implies \forall x\,[x \in \{z : \varphi(z)\} \iff \varphi(x)].$$

Proof. Bounty. ∎

1.5 The Power Set Axiom, Unordered

Thus far, our three axioms only guarantee the existence of one set: the empty set. For it might happen that this was the set given by the Set Existence Axiom.

So we next introduce an axiom which states that if A is a set then there is a set $\mathcal{P}(A)$ (called the power set of A) containing all the subsets of A.

Definition 1.22 (Power set)**.** The *power set*

$$\mathcal{P}(A) := \{B : B \subseteq A\}.$$

An alternate notation of $\mathcal{P}(A)$ is 2^A; hence "power set."

In order to be sure that the power set of A is *not* the empty set, we must introduce the *Power Set Axiom*:

Axiom 4 (Power Set)**.** For each set A there is a set containing all the subsets of A.

$$\forall A\, \exists C\, \forall x\, [x \in C \iff x \subseteq A].$$

Then we can prove the following:

Theorem 1.23. For every set A, z is in the power set of A only when z is a subset of A:

$$\forall A\, \forall z\, [z \in \mathcal{P}(A) \iff z \subseteq A]$$

Proof. Bounty. ∎

We next see that the power set operation is *monotonic*:

Theorem 1.24 (Monotonicity)**.**

$$A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

Proof. Homework. ∎

Then we obtain the following:

Theorem 1.25. For every set A

1. $\varnothing \in \mathcal{P}(A)$,
2. $A \in \mathcal{P}(A)$,

3. $\varnothing \neq \mathcal{P}(A)$, and
4. $z \in \mathcal{P}(\mathcal{P}(\varnothing)) \iff [z = \varnothing \vee z = \mathcal{P}(\varnothing)]$

Proof of 1. By Theorem 1.23 we have

$$\forall A \, \forall z \, [z \in \mathcal{P}(A) \iff z \subseteq A]$$

and since $\forall A \, (\varnothing \subseteq A)$ by Theorem 1.15 if follows that

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

from Theorem 1.23. ∎

Proof of 2.

$$\begin{aligned} A = A &\implies A \subseteq A \wedge A \subseteq A && \text{Thm. 1.5} \\ &\implies A \subseteq A \\ &\implies A \in \mathcal{P}(A) && \text{Thm. 1.23} \end{aligned}$$

∎

Proof of 3. Towards a contradiction assume $\exists A \, (\varnothing = \mathcal{P}(A))$ then

$$\begin{aligned} &\exists A \, (\varnothing = \mathcal{P}(A)) && \text{Assumption} \\ &\quad \implies \exists A \, \forall x \, (x \notin \mathcal{P}(A)) && \text{Def. 1.14} \\ &\quad \implies \exists A \, (\varnothing \notin \mathcal{P}(A)) \lightning && \text{Thm. 1.25.1} \end{aligned}$$

Thus $\neg \exists A \, (\varnothing = \mathcal{P}(A)) \equiv \forall A \, (\varnothing \neq \mathcal{P}(A))$ and the result follows. ∎

Proof of 4. By Definition 1.22 we have

$$\mathcal{P}(\varnothing) = \{B \, : \, B \subseteq \varnothing\}$$

which means, since $\forall x \, (x \subseteq \varnothing \implies x = \varnothing)$ by Theorem 1.14, we have $\mathcal{P}(\varnothing) = \{\varnothing\}$. Thereby

$$\begin{aligned} &\mathcal{P}(\mathcal{P}(\varnothing)) = \mathcal{P}(\{\varnothing\}) = \{B \, : \, B \subseteq \{\varnothing\}\} && \text{Def. 1.22} \\ &\quad \implies B = \varnothing \vee B = \{\varnothing\} && \text{Thm. 1.19} \\ &\quad \implies \mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\} = \{\varnothing, \{\mathcal{P}(\varnothing)\}\} \end{aligned}$$

Thus $z \in \{\varnothing, \mathcal{P}(\varnothing)\} \iff (z = \varnothing \vee z = \mathcal{P}(\varnothing))$ by Theorem 1.28. ∎

Note that we have *two* distinct sets, $\varnothing$ and $\mathcal{P}(\varnothing)$, we can use the *Axiom of Replacement* to ensure that the concept of *unordered pair* $\{x, y\}$ makes sense:

Definition 1.26 (Unordered Pair)**.**

$$\{x, y\} := \{z : z = x \vee z = y\}.$$

In particular, the Axiom of Replacement is needed to ensure that $\{x, y\}$ does not collapse to the empty set:

Theorem 1.27. $\forall x, y\,[\{x, y\} \neq \varnothing]$.

Proof.

$$\begin{aligned}
\{x, y\} = \varnothing &\implies \{z : z = x \vee z = y\} = \varnothing && \text{Def. 1.26}\\
&\implies \neg\exists z\,(z = x \vee z = y) && \text{Thm. 1.19}\\
&\implies \forall z\,(z \neq x \wedge z \neq y)\\
&\implies \forall z\,(z \neq x)\\
&\implies x \neq x \lightning
\end{aligned}$$

■

Theorem 1.28. $\forall x\,\forall y\,\forall z\,[z \in \{x, y\} \iff (z = x \vee z = y)]$.

Proof. Let $\varphi(z) \equiv (z = x \vee z = y)$ so that $\{x, y\} = \{z : \varphi(z)\}$ and recall $\{x, y\} \neq \varnothing$ by Theorem 1.27.

$$z \in \{x, y\} \iff \varphi(z) \iff z = x \vee z = y. \qquad \text{Thm. 1.19}$$

■

The main result about unordered pairs is the following theorem:

Theorem 1.29.

$$\{x, y\} = \{A, B\} \iff (x = A \wedge y = B) \vee (x = B \wedge y = A).$$

Proof. Bounty. ■

Thus, in an unordered pair, the elements occur in no particular order:

Exercise 1.30. $\{x, y\} = \{y, x\}$.

If $x = y$, it will be useful to define $\{x\}$ to be $\{x, x\}$ and to call $\{x\}$ a *singleton*.

Definition 1.31 (Singleton)**.**

$$\{x\} := \{x, x\}\,.$$

If follows that

Theorem 1.32. $\{A\} = \{B\} \iff A = B.$

Proof.

$$\begin{aligned}
&\{A\} = \{B\} \\
&\quad\iff \{A, A\} = \{B, B\} && \text{Def. 1.31} \\
&\quad\iff (A = B \wedge A = B) \vee (A = B \wedge A = B) && \text{Thm. 1.29} \\
&\quad\iff A = B
\end{aligned}$$

■

In order to have them available for examples, we define the first few natural numbers.

Definition 1.33 (Natural Numbers)**.**

$$\begin{aligned}
0 &:= \varnothing \\
1 &:= \mathcal{P}(\varnothing) \\
2 &:= \mathcal{P}(\mathcal{P}(\varnothing)) \\
&\vdots
\end{aligned}$$

In contrast to the unordered pair $\{x, y\}$, the *ordered pair* (x, y) depends on the x and y being in a particular oder: first z and then the y. There are many different ways in which we could defined a concept of ordered pair.

We use a definition invented by the Polish mathematician Kuratowski in 1921:

Definition 1.34 (Ordered Pair)**.**

$$(x, y) := \{\{x\}\,, \{x, y\}\}\,.$$

The key property of ordered pairs is expressed in the following theorem:

Theorem 1.35. $(x, y) = (A, B) \iff x = A \wedge y = B.$

Lemma 1.36. $(x = y) \implies [(x, y) = (A, B) \iff (x = A \wedge y = B)]$.

Proof. Homework. ∎

Proof. Assume $x \neq y$ then

$$\begin{aligned}
&(x, y) = (A, B) \\
&\quad \iff \{\{x\}, \{x, y\}\} = \{\{A\}, \{A, B\}\} && \text{Def. 1.34} \\
&\quad \iff (\{x\} = \{A\} \wedge \{x, y\} = \{A, B\}) \\
&\qquad \vee (\{x\} = \{A, B\} \wedge \{x, y\} = \{A\}) && \text{Thm. 1.29}
\end{aligned}$$

Dealing with each side of the disjunction individually we have

$$\begin{aligned}
&\{x\} = \{A\} \wedge \{x, y\} = \{A, B\} \\
&\quad \iff x = A \wedge \{x, y\} = \{A, B\} && \text{Thm. 1.32} \\
&\quad \iff x = A \wedge [(x = A \wedge y = B) \vee (x = B \wedge y = A)] && \text{Thm. 1.29} \\
&\quad \iff (x = A \wedge x = A \wedge y = B) \vee (x = A \wedge x = B \wedge y = A) \\
&\quad \iff (x = A \wedge y = B) \vee \bot && \text{Assumption} \\
&\quad \iff x = A \wedge y = B
\end{aligned}$$

or

$$\begin{aligned}
&\{x\} = \{A, B\} \wedge \{x, y\} = \{A\} \\
&\quad \iff \{x, x\} = \{A, B\} \wedge \{x, y\} = \{A, A\} && \text{Def. 1.31} \\
&\quad \iff (x = A \wedge x = B) \wedge (x = A \wedge y = A) \\
&\quad \iff \bot. && \text{Assumption}
\end{aligned}$$

Thus we have

$$x \neq y \implies [(x, y) = (A, B) \iff (x = A \wedge y = B)].$$

Combining this with Lemma 1.36 gives the result. ∎

Contrast Theorem 1.35 with Theorem 1.29 about unordered pairs.

1.6 Intersection, Set Difference, and Union

Most students are familiar with the concept of the intersection $A \cap B$ of the sets A and B:

Definition 1.37 (Intersection).

$$A \cap B := \{z : z \in A \wedge z \in B\}.$$

Theorem 1.38. $z \in x \cap y \iff z \in x \wedge z \in y$.

Exercise 1.39. Demonstrate the intersection operation is *commutative*, *associative*, and *idempotent*. Namely:

1. $x \cap y = y \cap x$,
2. $(x \cap y) \cap z = x \cap (y \cap z)$, and
3. $x \cap x = x$.

The next theorem states that $x \cap y$ is a *lower bound* for x and y with respect to $\subseteq$, and 1.41 states that, actually, $x \cap y$ is the *greatest lower bound* of x and y with respect to $\subseteq$:

Theorem 1.40. $(x \cap y \subseteq x) \wedge (x \cap y \subseteq y)$.

Proof.

$$\begin{aligned}
&\forall z\,(z \in x \cap y \implies z \in x \wedge z \in y) && \text{Thm. 1.38}\\
&\quad \implies \forall z\,(z \in x \cap y \implies z \in x) \wedge \forall z\,(z \in x \cap y \implies z \in y)\\
&\quad \implies (x \cap y \subseteq x) \wedge (x \cap y \subseteq y) && \text{Thm. 1.4}
\end{aligned}$$

■

Theorem 1.41. $z \subseteq x \wedge z \subseteq y \implies z \subseteq x \cap y$.

Proof.

$$\begin{aligned}
&z \subseteq x \wedge z \subseteq y\\
&\quad \implies \forall a\,[a \in z \implies a \in x] \wedge \forall a\,[a \in z \implies a \in y] && \text{Thm. 1.4}\\
&\quad \implies \forall a\,[a \in z \implies (a \in x \wedge a \in y)]\\
&\quad \implies \forall a\,[a \in z \implies a \in x \cap y] && \text{Thm. 1.38}\\
&\quad \implies z \subseteq x \cap y && \text{Thm. 1.4}
\end{aligned}$$

■

We next introduce $x \setminus y$, the *set difference* of x with y. Sometimes we say $x \setminus y$ as "x set minus y":

Definition 1.42 (Set Difference).

$$x \setminus y := \{z : z \in x \wedge z \notin y\}.$$

Theorem 1.43. $z \in x \setminus y \iff z \in x \wedge z \notin y$.

Proof. ∎

Two theorems that will be useful later are the following.

Theorem 1.44. $B = A \setminus (A \setminus B) \iff B \subseteq A$.

Proof of $\Longrightarrow$. Assume $B = A \setminus (A \setminus B)$.

$$\begin{aligned} x \in B &\implies x \in A \setminus (A \setminus B) && \text{Assumption} \\ &\implies x \in A \wedge x \notin A \setminus B && \text{Thm. 1.43} \\ &\implies x \in A \end{aligned}$$

and thus $\forall x\,(x \in B \implies x \in A)$ which means $B \subseteq A$ by Definition 1.4. ∎

Proof of $\Longleftarrow$. Assume $B \subseteq A$.

$$\begin{aligned} x \in B &\implies x \in B \wedge x \in B \\ &\implies x \in A \wedge x \in B && \text{Assumption} \\ &\implies \bot \vee (x \in A \wedge x \in B) \\ &\implies (x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B) \\ &\implies x \in A \wedge (x \notin A \vee x \in B) \\ &\implies x \in A \wedge \neg(x \in A \wedge x \notin B) \\ &\implies x \in A \wedge x \notin A \setminus B && \text{Thm. 1.43} \\ &\implies x \in A \setminus (A \setminus B) \end{aligned}$$

Thus $B \subseteq A \implies (x \in B \iff x \in A \setminus (A \setminus B))$. Or, using Axiom 1 to write it differently, $B \subseteq A \implies B = A \setminus (A \setminus B)$. ∎

Theorem 1.45. $(A \setminus B) \setminus C = (A \setminus B) \cap (A \setminus C)$.

Proof.

$$\begin{aligned} x \in (A \setminus B) \setminus C & \\ &\iff (x \in A \wedge x \notin B) \wedge x \notin C && \text{Thm. 1.43} \\ &\iff (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\ &\iff x \in A \setminus B \wedge x \in A \setminus C && \text{Thm. 1.43} \\ &\iff x \in (A \setminus B) \cap (A \setminus C) && \text{Thm. 1.38.} \end{aligned}$$

∎

Exercise 1.46. $x \setminus (x \cap y) = x \setminus y = x \cap (x \setminus y)$.

Proof.

$$\begin{aligned} a \in x \setminus (x \cap y) &\iff a \in x \wedge \neg(a \in x \wedge a \in y) && \text{Axiom 1} \\ &\iff a \in x \wedge (a \notin x \vee a \notin y) \\ &\iff a \in x \wedge a \notin y \end{aligned}$$

Notice that

$$a \in x \wedge a \notin y \iff a \in x \setminus y$$

by Theorem 1.43, and

$$\begin{aligned} a \in x \wedge a \notin y &\iff a \in x \wedge (a \in x \wedge a \notin y) \\ &\iff a \in x \wedge a \in x \setminus y && \text{Thm. 1.43} \\ &\iff a \in x \cap (x \setminus y). && \text{Thm. 1.38} \end{aligned}$$

Thus by Axiom 1 we have $x \setminus (x \cap y) = x \setminus y = x \cap (x \setminus y)$. ∎

So far, we have talked about the intersection of two sets. Now we introduce the *intersection* of *any* set A. If A has infinitely many members, then we have a new notion that goes beyond the intersection of two (and, by iteration, of a finite number of) sets; that is, the intersection of finitely many or infinitely many sets:

Definition 1.47.

$$\bigcap A := \{z : \forall y\,(y \in A \implies z \in y)\}.$$

Now $\bigcap \varphi$ would be "too big" to be a set without our convention that $\{z : \varphi(z)\}$ is $\varnothing$ in that case.

Theorem 1.48. $\bigcap \varnothing = \varnothing$.

Proof. Consider

$$\begin{aligned} \bigcap \varnothing &= \{z : \forall y\,(y \in \varnothing \implies z \in y)\} && \text{Def. 1.47} \\ &= \{z : \forall y\,(\bot \implies z \in y)\} \\ &= \{z : \top\} \\ &= \text{ Universal Set} = \varnothing. \end{aligned}$$

∎

Theorem 1.49.

$$A \neq \varnothing \implies \forall z\,[z \in \bigcap A \iff \forall y\,(y \in A \implies z \in y)].$$

Proof. Assume $A \neq \varnothing$.

$$\begin{aligned} z \in \bigcap A &\iff z \in \{z : \forall y\,(y \in A \implies z \in y)\} \\ &\iff \forall y\,(y \in A \implies z \in y) && \text{Thm. 1.19.} \end{aligned}$$

■

Exercise 1.50. 1. $\bigcap \{x\} = x$,

2. $\bigcap \{x, y\} = x \cap y$, and

3. $x \neq \varnothing \wedge x \subseteq y \implies \bigcap y \subseteq \bigcap x$.

The next two theorems will be applied later:

Theorem 1.51. $x \in A \implies \bigcap A \subseteq x$.

Proof. Suppose $x \in A$.

$$\begin{aligned} z \in \bigcap A &\implies \forall y\,(y \in A \implies z \in y) \\ &\implies (x \in A \implies z \in x) \\ &\implies (\top \implies z \in x) && \text{Assumption} \\ &\implies z \in x. \end{aligned}$$

Thus $\bigcap A \subseteq x$ by Definition 1.4. ■

Theorem 1.52. $[C \neq \varnothing \wedge \forall B\,(B \in C \implies A \subseteq B)] \implies A \subseteq \bigcap C$.

Proof. Homework. ■

We now come to $\bigcup A$, the union of the set A. The union of A is more general than the union of two sets, since A may be infinite. We will see later that $B \cup C$ is a special case of $\bigcup A$, since $B \cup C = \bigcup \{B, C\}$.

Definition 1.53.

$$\bigcup A := \{z : \exists y\,[z \in y \wedge y \in A]\}.$$

In order to ensure that $\bigcup A$ is not always the empty set, thus allowing us to build "bigger" sets through unions, we need a new axiom:

Axiom 5 (Union). If A is a set, then the union of A is a set.

$$\forall A\, \exists w\, \forall z\, [z \in w \iff \exists y\, (z \in y \land y \in A)].$$

Theorem 1.54. $z \in \bigcup A \iff \exists y\, [z \in y \land y \in A]$.

We now define "little union", that is, $B \cup C$, the union of the sets B and C.

Definition 1.55 (Little Union).

$$B \cup C := \bigcup \{B, C\}.$$

Theorem 1.56. $z \in B \cup C \iff (z \in B \lor z \in C)$.

Proof.

$$\begin{aligned} z \in B \cup C &\iff z \in \bigcup \{B, C\} \\ &\iff \exists y\, (z \in y \land y \in \{B, C\}) && \text{Thm. 1.54} \\ &\iff (z \in y \land y = B) \lor (z \in y \land y = C) \\ &\iff z \in B \lor z \in C. \end{aligned}$$

Theorem 1.57. $x \cup y = \{z : z \in x \lor z \in y\}$.

Proof.

$$\begin{aligned} z \in x \cup y &= \bigcup \{x, y\} && \text{Def. 1.57} \\ &= \{z : (z \in A \land A \in \{x, y\})\} && \text{Def. 1.53} \\ &= \{z : (z \in A \land A = x) \lor (z \in A \land A = y)\} \\ &= \{z : z \in x \lor z \in y\}. \end{aligned}$$

Exercise 1.58. Prove $x \cup y$ is commutative, associative, idempotent, and has $\varnothing$ as its *identity element*:

1. $x \cup y = y \cup x$,
2. $(x \cup y) \cup z = x \cup (y \cup z)$,
3. $x \cup x = x$, and
4. $x \cup \varnothing = x$.

Exercise 1.59. Prove

1. $x \subseteq x \cup y$,
2. $y \subseteq x \cup y$,
3. $x \subseteq z \wedge y \subseteq z \implies x \cup y \subseteq z$.

So $x \cup y$ is an *upper bound* of x and of y with respect to $\subseteq$. Moreover, $x \cup y$ is the *least upper bound* of x and y with respect to $\subseteq$.

Exercise 1.60. The following are equivalent:

1. $x \subseteq y$,
2. $x \cup y = y$,
3. $x \cap y = x$.

Proof. ∎

The various parts of the next theorem are often called *De Morgan's Laws*, after the English mathematician Augustus DeMorgan:

Theorem 1.61 (DeMorgan's Laws)**.**

1. $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$,
2. $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$,
3. $x \setminus (y \cap z) = (x \setminus y) \cup (x \setminus z)$,
4. $x \setminus (y \cup z) = (x \setminus y) \cap (x \setminus z)$.

Proof of 1.

$$
\begin{aligned}
& a \in x \cap (y \cup z) \\
& \quad \iff a \in x \wedge a \in (y \cup z) && \text{Def. 1.37} \\
& \quad \iff a \in x \wedge (a \in y \vee a \in z) && \text{Thm. ??} \\
& \quad \iff (a \in x \wedge a \in y) \vee (a \in x \wedge a \in z) \\
& \quad \iff a \in x \cap y \vee a \in x \cap z && \text{Def. 1.37} \\
& \quad \iff a \in (x \cap y) \cup (x \cap z). && \text{Thm. ??}
\end{aligned}
$$

∎

Proof of 3.

$$\begin{aligned}
& a \in x \setminus (y \cap z) \\
& \quad \iff a \in x \wedge \neg(a \in y \cap z) && \text{Thm. 1.43} \\
& \quad \iff a \in x \wedge \neg(a \in y \wedge a \in z) && \text{Thm. 1.38} \\
& \quad \iff a \in x \wedge (a \notin y \vee a \notin z) \\
& \quad \iff (a \in x \wedge a \notin y) \vee (a \in x \wedge a \notin z) \\
& \quad \iff (a \in x \setminus y) \vee (a \in x \setminus z) && \text{Thm. 1.50} \\
& \quad \iff a \in (x \setminus y) \cup (x \setminus z). && \text{Thm. ??}
\end{aligned}$$

■

We end his section with a few additional results on the union of an arbitrary set A of sets:

Theorem 1.62. 1. $\bigcup \varnothing = \varnothing$,

2. $x \in y \implies x \subseteq \bigcup y$.

Proof of 1.

$$\begin{aligned}
x \in \bigcup \varnothing & \iff \exists A\,(x \in y \wedge A \in \varnothing) && \text{Thm. 1.60} \\
& \iff \bot.
\end{aligned}$$

And thus $\bigcup \varnothing = \varnothing$. ■

Proof of 2. Assume $x \in y$.

$$\begin{aligned}
a \in x & \implies a \in x \wedge x \in y \\
& \implies \exists x\,(a \in x \wedge x \in y) \\
& \implies a \in \bigcup y. && \text{Thm. 1.60}
\end{aligned}$$

Thereby $x \in y \implies x \subseteq \bigcup y$. ■

Theorem 1.63. $\forall B\,[B \in C \implies B \subseteq A] \implies \bigcup C \subseteq A$.

(Compare 1.63 with 1.52 on intersection.)

Exercise 1.64. 1. $x \subseteq \implies x \cap z \subseteq y \cap z$,

2. $x \subseteq y \wedge w \subseteq z \implies x \cap w \subseteq y \cap z$,

3. $x \subseteq y \implies x \cup z \subseteq y \cap z$, and

4. $x \subseteq y \wedge w \subseteq z \implies x \cap w \subseteq y \cap z$.

Theorem 1.65. The union operation is *monotonic*, in contrast with the intersection operation, which is not.

$$A \subseteq B \implies \bigcup A \subseteq \bigcup B.$$

Proof. Assume $A \subseteq B$.

$$\begin{aligned} x \in \bigcup A &\implies \exists y\,(x \in y \wedge y \in A) && \text{Thm. 1.54} \\ &\implies \exists y\,(x \in y \wedge y \in B) && \text{Assumption} \\ &\implies x \in \bigcup B. && \text{Thm. 1.54} \end{aligned}$$

■

The power set operation will also turn out to be monotonic. (See **??**.)

Exercise 1.66. Prove or refute that

$$\bigcup A = \bigcup B \implies A = B.$$

Answer. Refute. Notice.

$$\begin{aligned} \bigcup \{\varnothing\} &= \{z : \exists x\,(z \in x \wedge x \in \{\varnothing\})\} \\ &= \{z : z \in x \wedge x = \varnothing\} \\ &= \{z : z \in \varnothing\} \\ &= \{z : \bot\} \\ &= \varnothing \end{aligned}$$

and

$$\begin{aligned} \bigcup \varnothing &= \{z : \exists z\,(z \in x \wedge x \in \varnothing)\} \\ &= \{z : \exists x\,(z \in x \wedge \bot)\} \\ &= \{z : \bot\} \\ &= \varnothing. \end{aligned}$$

◆

Exercise 1.67. Prove or refute

$$\bigcap \bigcup A = \bigcup \bigcap A.$$

Answer. Refute. Notice

$$\bigcap\bigcup\{\varnothing,\{\varnothing\}\} = \bigcap\{\varnothing\} = \{\varnothing\}.$$

and

$$\bigcup\bigcap\{\varnothing,\{\varnothing\}\} = \bigcup\varnothing = \varnothing.$$

1.7 Terms and Class Abstraction

At this point it will be helpful to introduce the concept of a "term" and to extend our class abstraction to allow terms. A term $t(x_1, x_2)$ is just a set in which x_1 and x_2 occur as free variables. Thus $t(x_1, x_2)$ might be $x_1 \cup x_2$ or $x_1 \setminus x_2$ or (x_1, x_2) or $\{x_1, x_2\}$ or $\{(x_1, x_2), \bigcup x_1\}$, and so on.

The following is a definition schema of class abstraction using terms.

Definition 1.68. Suppose that $v_1, \ldots, v_n, w$ are distinct variables and that $t(v_1, \ldots, v_n)$ is a term in which no bound variable occurs and the free variables occurring in $t(v_1, \ldots, v_n)$ are exactly $v_1, \ldots, v_n$, and that w does not occur in the formula $\varphi(v_1, \ldots, v_n)$. Then

$$\begin{aligned}&\{t(v_1, \ldots, v_n) : \varphi(v_1, \ldots, v_n)\}\\ &\quad = \{w : \exists v_1 \cdots \exists v_n (w = t(v_1, \ldots, v_n) \wedge \varphi(v_1, \ldots, v_n)\}\end{aligned}$$

For example, we will use class abstraction with such terms in the next theorem, which states the generalized version of De Morgan's laws. We will fix a set C and look at the set $\{C \setminus x : x \in A\}$. By 1.68 this set is $\{w : \exists x\,[w = c \setminus x \wedge x \in A]\}$.

Theorem 1.69. Let $A \subseteq \mathcal{P}(C)$ and $A \neq \varnothing$. Then

1. $C \setminus \bigcup A = \bigcap\{C \setminus x : x \in A\}$,
2. $C \setminus \bigcap A = \bigcup\{C \setminus x : x \in A\}$,
3. $B = \{C \setminus x : x \in A\} \implies A = \{C \setminus y : y \in B\}$.

Solution to Exercises

2 Relations and Functions

Mathematics makes very extensive use of both relations and functions. For us, a relation is defined to be *any* set of ordered pairs, as in the next definition.

Definition 2.1 (Relation). B is a relation when B is a set of ordered pairs:

$$\forall z\,(z \in B \implies \exists x \exists y : z = (x, y)).$$

Theorem 2.2. $\varnothing$ is a relation.

Proof. Let $B = \varnothing$ then

$$\begin{aligned} &\forall z\,(z \in \varnothing \implies \exists x\,\exists y : z = (x, y)) \\ &\quad \iff \forall z\,(\bot \implies \exists x\,\exists y : z = (x, y)) && 1.14 \\ &\quad \iff \top. \end{aligned}$$

■

Theorem 2.3. If $A \subseteq B$ and B is a relation, then A is a relation.

Proof. Suppose $A \subseteq B$ and B is a relation. We have

$$\begin{aligned} &\forall z\,(z \in A \implies z \in B) && 1.4 \\ &\quad \implies \forall z\,(z \in A \implies \exists x\,\exists y : z = (x, y)) && \text{Ass and 2.1} \end{aligned}$$

And thus A is a relation by Definition 2.1. ■

Theorem 2.4. Let A and B be relations. Then $A \cap B$ is a relation, $A \setminus B$ is a relation, and $A \cup B$ is a relation.

Proof. Suppose A and B are relations. Recall $A \cap B \subseteq B$ and $A \setminus B \subseteq A$. Thereby Theorem 2.3 proves these sets are relations.

For $A \cup B$ we have

$$\begin{aligned} & z \in A \cup B \\ & \quad \implies z \in A \vee z \in B && 1.56 \\ & \quad \implies \exists x \, \exists y \, (z = (x, y)) \vee \exists x \, \exists y \, (z = (x, y)) && \text{Ass 2.1} \\ & \quad \implies \exists x \, \exists y \, (z = (x, y)) \end{aligned}$$

Thus $\forall z \, (z \in A \cup B \implies \exists x \, \exists y \, : \, z = (x, y))$ and thereby $A \cup B$ is a relation by Defintion 2.1. ■

A key idea connected to relations is that of $A \times B$, the *Cartesian product* of the sets A and B. We will define $A \times B$ to be the set of all ordered pairs (w, z) such that $w \in A$ and $z \in B$:

Definition 2.5 (Cartesian Product)**.**

$$A \times B = \{(a, b) \, : \, a \in A \wedge b \in B\} .$$

Theorem 2.6.

$$z \in A \times B \iff \exists C \, \exists D \, [C \in A \wedge D \in B \wedge z = (C, D)]$$

Theorem 2.7. $(C, D) \in A \times B \iff C \in A \wedge D \in B$.

Proof. Let $z = (C, D)$ in Theorem 2.6

$$\begin{aligned} & (C, D) \in A \times B \\ & \quad \iff \exists C \, \exists D \, : \, C \in A \wedge D \in B \wedge (C, D) = (C, D) && 2.6 \\ & \quad \iff C \in A \wedge D \in B. \end{aligned}$$

■

Theorem 2.8. $A \times B$ is a relation.

Proof.

$$\begin{aligned} & z \in A \times B \\ & \quad \implies \exists C \, \exists D \, (C \in A \wedge D \in B \wedge z = (C, D)) && 2.6 \\ & \quad \implies \exists C \, \exists D \, (z = (C, D)) \end{aligned}$$

and thus $A \times B$ is a relation by Definition 2.1. ■

Exercise 2.9. Prove.

1. $A \times B = \varnothing \iff (A = \varnothing \vee B = \varnothing)$,
2. $B \subseteq C \implies (A \times B \subseteq A \times C \wedge B \times A \subseteq C \times A)$,
3. $A \times B = B \times A \iff \{A = B \vee A = \varnothing \vee B = \varnothing\}$,
4. $(A \neq \varnothing \wedge A \times B \subseteq A \times C) \implies B \subseteq C$.

Exercise 2.10. Prove or refute. If you refute an inequality then prove or refute each of the corresponding inclusions.

1. $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$,
2. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$,
3. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$,
4. $(A \setminus B) \times (C \setminus D) = [(A \times C) \setminus (B \times C)] \setminus A \times D$,
5. $(A \setminus B) \times (C \setminus D) = (A \setminus C) \times (B \setminus D)$,
6. $(A \neq \varnothing \wedge B \neq \varnothing) \implies [(A \subseteq C \wedge B \neq \varnothing) \iff A \times B \subseteq C \times D]$.

Exercise 2.11. Prove.

1. $(\bigcup B) \cap A = \bigcup \{C \cap A : C \in B\}$,
2. $(\bigcap B) \cup A = \bigcap \{C \cup A : C \in B\}$,
3. $(\bigcup B) \cup A = \bigcup \{C \cup A : C \in B\}$,
4. $(\bigcap B) \cap A = \bigcap \{C \cap A : C \in B\}$.

2.1 Domain, Range, Field of a Relation

From now on, we let R, S, and T (with or without subscripts) stand for relations.

Definition 2.12.

$$xRy \overset{\text{defn.}}{\iff} (x, y) \in R.$$

The *domain* of R, or $\mathrm{dom}(R)$, and the *range* of R, or $\mathrm{rng}(R)$, are closely related to each other, and their union is the *field* of R, or $\mathrm{fld}(R)$.

Definition 2.13 (Domain)**.**

$$\mathrm{dom}(R) := \{x : \exists y\, (xRy)\}.$$

Definition 2.14 (Range).

$$\mathrm{rng}(R) := \{y \,:\, \exists x\,(xRy)\}\,.$$

Definition 2.15 (Field).

$$\mathrm{fld}(R) := \mathrm{dom}(R) \cup \mathrm{rng}(R).$$

It follows that.

Theorem 2.16. 1. $x \in \mathrm{dom}(R) \iff \exists y\,(xRy)$,

2. $y \in \mathrm{rng}(R) \iff \exists x\,(xRy)$,

3. $z \in \mathrm{fld}(R) \iff \exists w\,(wRz \vee zRw)$.

Proof. Exercise. ∎

The operations of domain, range, and field are monotonic.

Theorem 2.17. 1. $R \subseteq S \implies \mathrm{dom}(R) \subseteq \mathrm{dom}(S)$,

2. $R \subseteq S \implies \mathrm{rng}(R) \subseteq \mathrm{rng}(S)$,

3. $R \subseteq S \implies \mathrm{fld}(R) \subseteq \mathrm{fld}(S)$.

Proof of 1. Assume $R \subseteq S$.

$$\begin{aligned}
z \in \mathrm{dom}(R) &\implies \exists y\,[zRy] && \text{2.15}\\
&\implies \exists y\,[(z,y) \in R] && \text{2.12}\\
&\implies \exists y\,[(z,y) \in S] && \text{Ass}\\
&\implies \exists y\,[zSy] &&\\
&\implies z \in \mathrm{dom}(S). && \text{2.15}
\end{aligned}$$

Thus $\mathrm{dom}(R) \subseteq \mathrm{dom}(S)$. ∎

Proof of 2. Assume $R \subseteq S$.

$$\begin{aligned}
z \in \mathrm{rng}(R) &\subseteq \mathrm{rng}(S)\\
&\implies \exists x\,[xRz] && \text{2.15}\\
&\implies \exists x\,[(x,z) \in R] && \text{2.12}\\
&\implies \exists x\,[(x,z) \in S] && \text{Ass}\\
&\implies \exists x\,[xSz] && \text{2.12}\\
&\implies z \in \mathrm{rng}(S).
\end{aligned}$$

Thus $\mathrm{dom}(R) \subseteq \mathrm{dom}(S)$. ∎

Proof of 3. Exercise. ∎

We next introduce $R|A$, the *restriction* of the relation R to A:

Definition 2.18 (Restriction)**.**

$$R|A := R \cap (A \times \mathrm{rng}(R)) .$$

Theorem 2.19. Restriction is monotonic:

1. $A \subseteq B \implies R|A \subseteq R|B$,
2. $R \subseteq S \implies R|A \subseteq S|A$.

Proof of 1. Assume $A \subseteq B$.

$$\begin{aligned}
& z \in R|A \\
& \quad \implies z \in R \cap (A \times \mathrm{rng}(R)) && \text{2.18} \\
& \quad \implies z \in R \wedge \exists x\, \exists y\, [x \in A \wedge y \in \mathrm{rng}(R) \wedge z = (x,y)] && \text{2.6} \\
& \quad \implies z \in R \wedge \exists x\, \exists y\, [x \in B \wedge y \in \mathrm{rng}(R) \wedge z = (x,y)] && \text{Ass} \\
& \quad \implies z \in R|B. && \text{2.18}
\end{aligned}$$

Thus $R|A \subseteq R|B$ by Theorem 1.4. ∎

Proof of 2. Assume $R \subseteq S$.

$$\begin{aligned}
& z \in R|A \\
& \quad \implies z \in R \cap A \times \mathrm{rng}(R) && \text{2.18} \\
& \quad \implies z \in S \cap A \times \mathrm{rng}(R) && \text{Ass} \\
& \quad \implies z \in S \wedge z \in A \times \mathrm{rng}(R) && \text{1.38} \\
& \quad \implies z \in S \\
& \qquad \wedge \exists x\, \exists y\, [x \in a \wedge y \in \mathrm{rng}(R) \wedge z = (x,y)] && \text{2.6} \\
& \quad \implies z \in S \\
& \qquad \wedge \exists x\, \exists y\, [x \in a \wedge y \in \mathrm{rng}(S) \wedge z = (x,y)] && \text{Ass, **??**} \\
& \quad \implies z \in S|A. && \text{2.18}
\end{aligned}$$

Thus $R|A \subseteq S|A$ by Theorem 1.4. ∎

Theorem 2.20. $R|A$ is a relation.

Proof.

$$z \in R|A$$

$$\begin{aligned} &\implies z \in R \wedge z \in A \times \mathrm{rng}(R) && 2.18 \\ &\implies \exists x\, \exists y\, [z = (x, y)] \wedge z \in A \times \mathrm{rng}(R) && 2.1 \\ &\implies \exists x\, \exists y\, [z = (x, y)]. \end{aligned}$$

Thus $R|A$ is a relation by Definition 2.1. ∎

Closely related with the range of a relation R is $R[A]$, the *image* of A under R:

Definition 2.21 (Image)**.**

$$R[A] := \mathrm{rng}(R|A)$$

Theorem 2.22.

$$y \in R[A] \iff \exists x\, [x \in A \wedge xRy].$$

Proof. Exercise. ∎

Theorem 2.23. The operation of image is monotonic.

$$A \subseteq B \implies R[A] \subseteq R[B].$$

Proof. Assume $A \subseteq B$.

$$\begin{aligned} &z \in R[A] \\ &\quad \implies \exists x\, [xRz \wedge x \in A] && 2.22 \\ &\quad \implies \exists x\, [xRz \wedge x \in B] && \text{Ass} \\ &\quad \implies z \in R[B]. && 2.22 \end{aligned}$$

Thus $R[A] \subseteq R[B]$ by Theorem 1.4. ∎

Theorem 2.24. Image is preserved by union:

1. $R[A \cup B] = R[A] \cup R[B]$,
2. $R[\bigcup A] = \bigcup \{R[C] \in A\}$,
3. $R[A \cap B] \subseteq R[A] \cap R[B]$,
4. $R[A] \setminus R[B] \subseteq R[A \setminus B]$.

Proof. Exercise. ∎

Exercise 2.25. Prove or refute

1. $R[A] \cap R[B] \subseteq R[A \cap B]$,

2. $R[A \setminus B] \subseteq R[A] \setminus R[B]$.

Theorem 2.26. $R = S \iff \forall x \forall y \, [xRy \iff xSy]$.

Proof of $\Longrightarrow$. Assume $R = S$.

$$\begin{aligned} xRy &\iff (x,y) \in R && 2.1 \\ &\iff (x,y) \in S && \text{Ass} \\ &\iff xSy. && 2.1 \end{aligned}$$

■

Proof of $\Longleftarrow$.

$$\begin{aligned} &\forall x \forall y \, [xRy \iff xSy] \\ &\quad \Longrightarrow \forall x \forall y \, [(x,y) \in R \iff (x,y) \in S] && 2.12 \\ &\quad \Longrightarrow R = S. && \text{Axiom 1} \end{aligned}$$

■

Exercise 2.27. Prove or refute

$$R = A \iff \forall x \, \forall y \, [(x,y) \in R \iff (x,y) \in A].$$

2.2 Converse and Relative Product

We next define $\breve{R}$, the converse of the relation R. The converse of a relation is a generalization of the inverse of a function. To define $\breve{R}$, we use Definition 1.68 with the term $t(x,y)$ equal to the ordered pair (x,y).

Definition 2.28 (Converse)**.**

$$\breve{R} := \{(x,y) \, : \, yRx\} \, .$$

Theorem 2.29. 1. $x\breve{R}y \iff yRx$,

2. $\breve{R}$ is a relation.

Proof. Exercise. ■

The *relative product* of R/S of the relations R and S is a generalization of the composition of two functions. Please note that in the relative product R/S, the slash / is at an angle, *not* vertical.

Definition 2.30 (Relative Product)**.**

$$R/S := \{(x,y) : \exists z\,[xRz \wedge zSy]\}.$$

Here Definition 1.68 was used once more with $t(x,y)$ as the ordered pair (x,y).

Theorem 2.31.

$$xR/Sy \iff \exists z\,[xRz \wedge zSy].$$

Exercise 2.32. R/S is a relation.

Theorem 2.33. 1. $\mathrm{dom}(R/S) \subseteq \mathrm{dom}(R)$,

2. $\mathrm{rng}(R/S) \subseteq \mathrm{rng}(S)$.

Proof of 1.

$$\begin{aligned} & x \in \mathrm{dom}(R/S) \\ & \quad \Longrightarrow \exists y\,(xR/Sy) && 2.16 \\ & \quad \Longrightarrow \exists y\,\exists z\,(xRz \wedge zSy) && 2.31 \\ & \quad \Longrightarrow \exists z\,(xRz) \\ & \quad \Longrightarrow x \in \mathrm{dom}(R) && 2.16 \end{aligned}$$

Thus $\mathrm{dom}(R/S) \subseteq \mathrm{dom}(R)$ by 1.4. ∎

Proof of 2.

$$\begin{aligned} & y \in \mathrm{rng}(R/S) \\ & \quad \Longrightarrow \exists x\,(xR/Sy) && 2.16 \\ & \quad \Longrightarrow \exists x\,\exists z\,(xRz \wedge zSy) && 2.31 \\ & \quad \Longrightarrow \exists z\,(zSy) \\ & \quad \Longrightarrow y \in \mathrm{rng}(S) && 2.16 \end{aligned}$$

Thus $\mathrm{rng}(R/S) \subseteq \mathrm{rng}(S)$ by 1.4. ∎

The relative product is associative:

Theorem 2.34. $(R/S)/T = R/(S/T)$.

Proof.

$$\begin{aligned} & (x,y) \in (R/S)/T \\ & \quad \iff x\,(R/S)/T\,y && 2.12 \end{aligned}$$

$$\begin{aligned}
&\iff \exists z_0\,(xR/Sz_0 \wedge z_0Ty) && 2.31\\
&\iff \exists z_0\,\exists z_1\,(xRz_1 \wedge z_1Sz_0 \wedge z_0Ty) && 2.31\\
&\iff \exists z_1\,(xRz_1 \wedge z_1S/Ty) && 2.31\\
&\iff xR/(S/T)y && 2.31\\
&\iff (x,y) \in R/(S/T). && 2.12
\end{aligned}$$

Thus $(R/S)/T = R/(S/T)$ by Axiom 1. ∎

Theorem 2.35. $R\breve{/}S = \breve{S}/\breve{R}$.

Proof.

$$\begin{aligned}
(x,y) \in R\breve{/}S &\iff xR\breve{/}Sy && 2.12\\
&\iff xR/Sx && 2.29\\
&\iff \exists z\,(yRz \wedge zSx) && 2.31\\
&\iff \exists z\,(x\breve{S}z \wedge z\breve{R}y) && 2.31\\
&\iff (x,y) \in \breve{S}/\breve{R} && 2.12.
\end{aligned}$$

By Axiom 1 $R\breve{/}S = \breve{S}/\breve{R}$. ∎

Theorem 2.36. $\breve{\breve{R}} = R$

Proof.

$$\begin{aligned}
(x,y) \in \breve{\breve{R}} &\iff x\breve{\breve{R}}y && 2.12\\
&\iff y\breve{R}x && 2.29\\
&\iff xRy && 2.29\\
&\iff (x,y) \in R. && 2.12
\end{aligned}$$

∎

Theorem 2.37. 1. $\mathrm{dom}(\breve{R}) = \mathrm{rng}(R)$,

2. $\mathrm{rng}(\breve{R}) = \mathrm{dom}(R)$.

Proof of 1.

$$\begin{aligned}
y \in \mathrm{dom}(\breve{R}) &\iff \exists x\,(y\breve{R}x) && 2.16\\
&\iff \exists x\,(xRy) && 2.29\\
&\iff y \in \mathrm{rng}(R). && 2.16
\end{aligned}$$

Thus $\mathrm{dom}(\breve{R}) = \mathrm{rng}(R)$ by Axiom 1. ∎

Proof of 2.

$$\begin{aligned} x \in \mathrm{rng}(\breve{R}) &\iff \exists y\,(y\breve{R}x) && 2.16\\ &\iff \exists y\,(xRy) && 2.29\\ &\iff x \in \mathrm{dom}(R). && 2.16 \end{aligned}$$

Thus $\mathrm{rng}(\breve{R}) = \mathrm{dom}(R)$ by Axiom 1. ∎

Theorem 2.38. $\mathrm{rng}(R) = \mathrm{dom}(S) \implies \mathrm{dom}(R) = \mathrm{dom}(R/S)$

Proof. Assume $\mathrm{rng}(R) = \mathrm{dom}(S)$ which implies

$$\forall z\,(\exists x\,(xRz) \iff \exists y\,(zSy)).$$

We have from 2.17 that $\mathrm{dom}(R/S) \subseteq \mathrm{dom}(R)$ so it suffices to show $\mathrm{dom}(R) \subseteq \mathrm{dom}(R/S)$ to get equality.

$$\begin{aligned} & x \in \mathrm{dom}(R)\\ &\implies \exists z\,(xRz) && 2.16\\ &\implies \exists z\,\exists x\,(xRz)\\ &\implies \exists z\,\exists y\,(zSy) \end{aligned}$$

∎

Theorem 2.39. $\mathrm{rng}(R) = \mathrm{dom}(S) \implies \mathrm{rng}(S) = \mathrm{rng}(R/S)$

Proof. ∎

Theorem 2.40.

$$A \subseteq \mathrm{dom}(R) \implies A \subseteq \breve{R}[R[A]].$$

Proof. Assume $A \subseteq \mathrm{dom}(R)$.

$$\begin{aligned} x \in A &\implies x \in A \wedge x \in \mathrm{dom}(R) && \text{Ass}\\ &\implies x \in A \wedge \exists y\,(xRy) && 2.16\\ &\implies \exists y\,(x \in A \wedge xRy)\\ &\implies \exists y\,\exists a\,(a \in A \wedge aRy \wedge xRy)\\ &\implies \exists y\,(y \in R[A] \wedge y\breve{R}x) && 2.29,\ 2.22\\ &\implies x \in \breve{R}[R[A]]. && 2.29 \end{aligned}$$

∎

2.3 One-to-One Relations and Functions

A relation R may be one-one, written 1-1, even if R is *not* a function:

Definition 2.41 (1-1). R is 1-1 when

$$\forall x\, \forall y\, \forall z\, [xRz \wedge yRz \implies x = y].$$

Theorem 2.42.

$$(R \text{ is 1-1} \wedge S \subseteq R) \implies S \text{ is 1-1}.$$

Theorem 2.43. Let R be 1-1 and S be 1-1, then

1. $R \cap S$ is 1-1,
2. $R \setminus S$ is 1-1,
3. R/S is 1-1,

Theorem 2.44. $\mathrm{rng}(R) \cap \mathrm{rng}(S) = \varnothing \implies R \cup S$ is 1-1.

Proof. Assume the premise and, towards a contradiction, that $R \cup S$ is *not* 1-1.

$$\begin{aligned} &\exists z\, (xRz \wedge ySz \wedge x \neq y) && 2.41 \\ &\implies \exists z\, (z \in \mathrm{rng}(R) \wedge z \in \mathrm{rng}(S)) && 2.16 \\ &\implies \mathrm{rng}(R) \cap \mathrm{rng}(S) \neq \varnothing \lightning && 1.38 \end{aligned}$$

■

Exercise 2.45. Find R and S such that R is 1-1 and S is 1-1 but $\mathrm{rng}(R) \cap \mathrm{rng}(S) \neq \varnothing$ and $R \cup S$ is *not* 1-1.

Answer. Let $R = \{(x,z)\}$ and $S = \{(y,z)\}$. Notice $\mathrm{rng}(R) = \{z\} = \mathrm{rng}(S)$ so $\mathrm{rng}(R) \neq \mathrm{rng}(S)$ but $R \cup S = \{(x,y),(y,z)\}$ is *not* 1-1 because $x \neq y \wedge xRz \wedge yRz$. ◆

Theorem 2.46.

$$R \text{ is 1-1} \iff \forall A\, (\check{R}[R[A]] \subseteq A).$$

Proof of $\implies$. Assume R is 1-1 and let A be arbitrary

$$\begin{aligned} z \in \check{R}[R[A]] &\implies \exists y\, (y \in R[A] \wedge y\check{R}z) && 2.22 \\ &\implies \exists x\, \exists y\, (x \in A \wedge xRy \wedge zRy) && 2.22,\ 2.29 \\ &\implies \exists y\, (z \in A \wedge zRy) \end{aligned}$$

$$\implies z \in A.$$

Thus $\check{R}[R[A]] \subseteq A$ by 1.4. ■

Proof of $\Longleftarrow$. Exercise. ■

Theorem 2.47.

$$R \text{ is 1-1} \iff \forall A\, \forall B\, (R[A] \cap R[B] \subseteq R[A \cap B]).$$

Proof of $\Longrightarrow$. Assume R is 1-1 and let A and B be arbitrary.

$$\begin{aligned}
& z \in R[A] \cap R[B] \\
& \quad \implies \exists a\, (a \in A \wedge aRz) \wedge \exists b\, (b \in B \wedge bRz) && 1.38 \\
& \quad \implies \exists a\, \exists b\, (a \in A \wedge aRz \wedge b \in B \wedge bRz) \\
& \quad aRz \wedge bRz \implies a = b \text{ by assumption} \\
& \quad \implies \exists a\, (a \in A \wedge a \in B \wedge aRz) \\
& \quad \implies \exists a\, (a \in A \cap B \wedge aRz) && 1.38 \\
& \quad \implies z \in R[A \cap B]. && 2.22
\end{aligned}$$

Thus $R[A] \cap R[B] \subseteq R[A \cap B]$. ■

Proof of $\Longleftarrow$. Exercise. ■

Theorem 2.48.

$$A \subseteq \operatorname{dom}(R) \wedge R \text{ is 1-1} \implies \check{R}[R[A]] = A.$$

Proof of $\subseteq$. Assume the premise.

$$\begin{aligned}
z \in \check{R}[R[A]] & \implies \exists y\, (y \in R[A] \wedge y\check{R}z) && 2.22 \\
& \implies \exists x\, \exists y\, (x \in A \wedge xRy \wedge zRy) && 2.22,\ 2.29 \\
& \quad xRy \wedge zRy \implies x = z \text{ by assumption} \\
& \quad \exists y\, (z \in A \wedge zRy) \\
& \quad \implies z \in A.
\end{aligned}$$

Thus $\check{R}[R[A]] \subseteq A$ by 1.4. ■

Proof of $\supseteq$. Assume the premise.

$$\begin{aligned}
z \in A & \implies z \in \operatorname{dom}(R) \wedge z \in A \\
& \implies \exists y\, (xRy \wedge z \in A) && 2.16
\end{aligned}$$

$$\begin{aligned}
&\implies \exists x\,\exists y\,(x \in A \wedge xRy \wedge zRy) \\
&\implies \exists y\,(y \in R[A] \wedge y\check{R}z) && \text{2.22, 2.29} \\
&\implies z \in \check{R}[R[A]] && \text{2.22}
\end{aligned}$$

Thus $A \subseteq \check{R}[R[A]]$ by 1.4. ∎

Theorem 2.49.

$$R \text{ is 1-1} \implies R[A \cap B] = R[A] \cap R[B].$$

Proof. Assume R is 1-1.

$$\begin{aligned}
z \in R[A \cap B] &\iff \exists y\,(y \in A \cap B \wedge yRz) && \text{2.22} \\
&\iff \exists y\,(y \in A \wedge y \in B \wedge yRz \wedge yRz) && \text{1.38} \\
&\iff z \in R[A] \wedge z \in R[B] && \text{2.22} \\
&\iff z \in R[A] \cap R[B] && \text{1.38}
\end{aligned}$$

Thus $R[A \cap B] = R[A] \cap R[B]$ by Axiom 1. ∎

Theorem 2.50.

$$R \text{ is 1-1} \implies R[A] \setminus R[B] = R[A \setminus B].$$

Proof of $\subseteq$. Assume R is 1-1.

$$\begin{aligned}
&z \in R[A] \setminus R[B] \\
&\quad\implies z \in R[A] \wedge z \notin R[B] && \text{1.43} \\
&\quad\implies \exists a\,(a \in A \wedge aRz) \wedge \neg\exists b\,(b \in B \wedge bRz) && \text{2.22} \\
&\quad\implies \exists a\,(a \in A \wedge aRz) \wedge \forall b\,(b \notin B \vee \neg bRz) \\
&\quad\implies \exists a\,(a \in A \wedge aRz) \wedge \forall b\,(b \in B \implies \neg bRz) \\
&\quad\implies \exists a\,(a \in A \wedge a \notin B \wedge aRz) \\
&\quad\implies \exists a\,(a \in A \setminus B \wedge aRz) && \text{1.43} \\
&\quad\implies z \in R[A \setminus B]. && \text{2.22}
\end{aligned}$$

Thus $R[A] \setminus R[B] \subseteq R[A \setminus B]$ by 1.4. ∎

Proof of $\supseteq$. Bounty. ∎

Next we define the usual functional notation $y = f(x)$, but we do it more generally for any relation R: $y = R(x)$. Notice that whenever

$\exists y\, \exists z\, [xRy \wedge xRz \wedge y \neq z]$, then $R(x)$ collapses to the empty set. Likewise, if $\neg\exists y\, [xRy]$, then $R(x)$ collapses to the empty set. We need such a collapse to ensure that $R(x)$ is well-defined for every x.

Definition 2.51.

$$y = R(x) \overset{\text{defn.}}{\iff} (\exists!z\, [xRz] \wedge xRy) \vee (\neg\exists!z\, [xRz] \wedge y = \varnothing)\,.$$

We define a *function* to be a relation R such that $\breve{R}$ is 1-1.

Definition 2.52.

$$R \text{ is a function} \overset{\text{defn.}}{\iff} \breve{R} \text{ is 1-1.}$$

From Definition 2.52 of function, we easily derive the following more familiar description of what it means to be a *function*:

Theorem 2.53. R is a function *if and only if*

$$\forall x\, \forall y\, \forall z\, (xRy \wedge xRz \implies y = z).$$

Proof of $\implies$. Let x, y, and z be arbitrary.

$$\begin{aligned} & xRy \wedge xRz \\ & \quad \implies y\breve{R}x \wedge z\breve{R}x && \text{2.29} \\ & \quad \implies y = z. && \text{Ass, 2.41} \end{aligned}$$

■

Proof of $\impliedby$. ■

We then prove:

Theorem 2.54. R is a function *if and only if*

$$\forall x\, \forall y\, (xRy \implies y = R(x)).$$

Theorem 2.55.

$$R \text{ is a function} \wedge S \subseteq R \iff S \text{ is a function.}$$

From now on, we let f, g, h and F, G, H (with or without subscripts) stand for functions.

Theorem 2.56. The following are functions

1. $F \cap G$,
2. $F \setminus G$,
3. F/G,
4. $F|A$.

Theorem 2.57.

$$\mathrm{dom}(F) \cap \mathrm{dom}(G) = \varnothing \implies F \cup G \text{ is a function.}$$

Proof. Assume $F \cup G$ is *not* a function. There exists x, y, z such that

$$\begin{aligned}
& y \neq z \wedge xF \cup Gy \wedge xF \cup Gz && 2.53 \\
& \quad \implies y \neq z \wedge (xFy \vee xGy) \wedge (xFz \vee xGz) \\
& \quad \implies (y \neq z \wedge xFy \wedge xFz) \\
& \qquad \vee (y \neq z \wedge xFy \wedge xGz) \\
& \qquad \vee (y \neq z \wedge xGy \wedge xFz) \\
& \qquad \vee (y \neq z \wedge xGy \wedge xGz) \\
& \quad \implies \bot \vee (y \neq z \wedge xFy \wedge xGz) \\
& \qquad \vee (y \neq z \wedge xGy \wedge xFz) \vee \bot && 2.53 \\
& \quad \implies (x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G)) \\
& \qquad \vee (x \in \mathrm{dom}(G) \wedge x \in \mathrm{dom}(F)) && 2.16 \\
& \quad \implies x \in \mathrm{dom}(F) \cap \mathrm{dom}(G) \lightning && 1.38
\end{aligned}$$

Thus

$$\neg(F \cup G \text{ a function}) \implies \neg(\mathrm{dom}(F) \cap \mathrm{dom}(G) = \varnothing)$$

and the result follows from the contraposition. ∎

Theorem 2.58.

$$\check{f}[A \cap B] = \check{f}[A] \cap \check{f}[B].$$

Proof of $\subseteq$.

$$\begin{aligned}
& z \in \check{f}[A \cap B] \\
& \quad \implies \exists y\, (y \in A \cap B \wedge z\check{f}y) && 2.22 \\
& \quad \implies \exists y\, (y \in A \wedge y \in B \wedge z\check{f}y) && 1.38 \\
& \quad \implies \exists y\, (y \in A \wedge z\check{f}y \wedge y \in B \wedge z\check{f}y) \\
& \quad \implies z \in \check{f}[A] \wedge z \in \check{f}[B] && 2.22
\end{aligned}$$

$$\implies z \in \breve{f}[A] \cap \breve{f}[B]. \qquad 1.38$$

Thus $\breve{f}[A \cap B] \subseteq \breve{f}[A] \cap \breve{f}[B]$ by 1.4. ∎

Proof of $\supseteq$.

$$\begin{aligned}
& z \in \breve{f}[A] \cap \breve{f}[B] \\
& \quad \implies z \in \breve{f}[A] \wedge z \in \breve{f}[B] && 1.38 \\
& \quad \implies \exists y_0 \, (y_0 \in A \wedge y_0 \breve{f} z) \wedge \exists y_1 \, (y_1 \in B \wedge y_1 \breve{f} z) && 2.22 \\
& \quad \implies \exists y_0 \, \exists y_1 \, (y_0 \in A \wedge y_1 \in B \wedge y_0 \breve{f} z \wedge y_1 \breve{f} z) \\
& \quad \breve{f} \text{ is 1-1 by assumption implying } y_0 = y_1 = y \\
& \quad \implies \exists y \, (y \in A \cap B \wedge y \breve{f} z) && 1.38 \\
& \quad \implies z \in \breve{f}[A \cap B] && 2.22
\end{aligned}$$

Thus $\breve{f}[A] \cap \breve{f}[B] \subseteq \breve{f}[A \cap B]$ by 1.4. ∎

Theorem 2.59.

$$\breve{f}[A] \setminus \breve{f}[B] = \breve{f}[A \setminus B].$$

Exercise 2.60. Prove or refute

1. $f[\bigcup A] = \bigcup f[A]$,
2. $f[\bigcap A] = \bigcap \{f[B] : B \in A\}$,
3. $f[A \cap B] = f[A] \cap f[B]$,
4. $f[A] \setminus f[B] = f[A \setminus B]$,
5. $\breve{f}[\bigcap A] = \bigcap \left\{ \breve{f}[B] : B \in A \right\}$.

Theorem 2.61.

$$f[\breve{f}[B]] \subseteq B.$$

Proof.

$$\begin{aligned}
z \in f[\breve{f}[B]] & \implies \exists y \, (y \in \breve{f}[B] \wedge y f z) && 2.22 \\
& \implies \exists y \, \exists b \, (b \in B \wedge b \breve{f} y \wedge y f z) && 2.22 \\
& \implies \exists y \, \exists b \, (b \in B \wedge b \breve{f} y \wedge z \breve{f} y) && 2.29 \\
& \quad f \text{ is 1-1 implies } z = b \\
& \implies \exists y \, (z \in B \wedge z f y) \\
& \implies z \in B.
\end{aligned}$$

Thus $f[\breve{f}[B]] \subseteq B$ by 1.4. ∎

Theorem 2.62.

$$\breve{f}[B] = \{x : f(x) \in B \wedge x \in \mathrm{dom}(f)\}.$$

Theorem 2.63. If f is 1-1, then $\breve{f}$ is a 1-1 function.

We will find it useful to have the notation $f : A \to B$ when $\mathrm{dom}(f) = A$ and $\mathrm{rng}(f) \subseteq B$.

Definition 2.64.

$$f : A \to B \overset{\text{defn.}}{\iff} [\mathrm{dom}(f) = A \wedge \mathrm{rng}(f) \subseteq B].$$

Definition 2.65. Suppose that $f : A \to B$.

1. f is said to be *surjective*, or to be *onto* B, if $\mathrm{rng}(f) = B$,
2. f is *injective* if f is 1-1,
3. f is *bijective* if f is both injective and surjective.

Theorem 2.66. If $f : A \to B$ is bijective, then $\breve{f} : B \to A$ is bijective.

Proof. Assume that $f : A \to B$ is bijective. We have $\breve{f}$ is 1-1 by virtue of the fact f is a function.

$$\begin{aligned} z \in \mathrm{rng}(\breve{f}) &\iff \exists y\,(y \breve{f} z) && 2.16 \\ &\iff \exists y\,(z f y) && 2.29 \\ &\iff z \in \mathrm{dom}(f) && 2.16 \\ &\iff z \in A. \end{aligned}$$

Thus $\mathrm{rng}(\breve{f}) = A$ and thereby $\breve{f} : B \to A$ is bijective by 2.65. ∎

The *composite function* $f \circ g$ is obtained by applying first the function g and then the function f. Notice that the order of the functional notation $f \circ g$ is reversed from that of the relative product g/f of f and g:

Definition 2.67.

$$f \circ g = g/f.$$

Theorem 2.68.

$$f \circ g \text{ is a function.}$$

Proof. Suppose, towards a contradiction, that $f \breve{\circ} g$ is *not* 1-1, then there is x, y, and z

$$\begin{aligned}
& x \, f \breve{\circ} g \, z \wedge y \, f \breve{\circ} g \, z \wedge x \neq y && 2.41 \\
& \quad \Longrightarrow \; x g \breve{/} f z \wedge y g \breve{/} f z \wedge x \neq y && 2.67 \\
& \quad \Longrightarrow \; x \breve{f} / \breve{g} z \wedge y \breve{f} / \breve{g} z \wedge x \neq y && 2.35 \\
& \quad \Longrightarrow \; \exists a \, (x \breve{f} a \wedge a \breve{g} z) \wedge \exists b \, (y \breve{f} b \wedge b \breve{g} z) \wedge x \neq y \\
& \quad \Longrightarrow \; \exists a \, \exists b \, (x \breve{f} a \wedge y \breve{f} b \wedge a \breve{g} z \wedge b \breve{g} z \wedge x \neq y) \\
& \quad \text{Notice } a \breve{g} z \wedge b \breve{g} z \implies a = b \text{ as } \breve{g} \text{ is 1-1.} \\
& \quad \Longrightarrow \; \exists a \, (x \breve{f} a \wedge y \breve{f} a \wedge x \neq y) \\
& \quad \Longrightarrow \; (x = y) \wedge (x \neq y) \lightning .
\end{aligned}$$

Therefore $f \breve{\circ} g$ is 1-1 $\implies$ $f \circ g$ is a function. ∎

Theorem 2.69.

$$x \in \operatorname{dom}(f \circ g) \implies f \circ g(x) = f(g(x)).$$

Theorem 2.70.

1. If f is 1-1 and g is 1-1, then $f \circ g$ is 1-1.
2. If $g : A \to B$ is surjective and $f : B \to C$ is surjective, then $f \circ g : A \to C$ is surjective.
3. If $g : A \to B$ is bijective and $f : B \to C$ is bijective, then $f \circ g : A \to C$ is bijective.

Proof of 1. Suppose the premise and, towards a contradiction, that $\exists x \exists y \exists z$ such that

$$\begin{aligned}
& x f \circ g z \wedge y f \circ g z \wedge x \neq y \\
& \quad \Longrightarrow \; \exists a \exists b : (x g a \wedge a f z) \wedge (y g b \wedge b f z) \\
& \quad f \text{ is injective} \implies a = b \\
& \quad \Longrightarrow \; \exists a : x g a \wedge a f z \wedge y g a \wedge a f z \\
& \quad g \text{ is injective} \implies x = y \\
& \quad \Longrightarrow \; x = y \wedge x \neq y \lightning
\end{aligned}$$

∎

Proof of 2. Exercise. ∎

Proof of 3. By part 1 and 2 we have $f \circ g$ is injective and surjective (respectively). Thus, by Definition **??**, is bijective. ∎

We next define the identity relation on A, and write it as Id_A:

Definition 2.71.

$$\mathrm{Id}_A := \{(a,a) \,:\, a \in A\}.$$

Theorem 2.72. Let $f : A \to B$ and $g : B \to A$.

1. $g \circ f = \mathrm{Id}_A \implies f$ is injective,
2. $f \circ g = \mathrm{Id}_B \implies f$ is surjective.

Proof of 1. Suppose $a_0, a_1 \in \mathrm{dom}(f)$ and

$$\begin{aligned} & a_0 f z \wedge a_1 f z \\ & \quad \implies z g a_0 \wedge z g a_1 && \text{Lemma} \\ & \quad \implies a_0 = a_1 && g \text{ is a function.} \end{aligned}$$

Lemma 2.73. $afz \implies zga$.

Notice

$$a \in \mathrm{dom}(f) = A \implies \exists b \in \mathrm{rng}(f) = B \,:\, afb$$

and

$$b \in \mathrm{rng}(f) \subseteq B \implies b \in \mathrm{dom}(g) \implies \exists a' \in A \,:\, bga.$$

Thus

$$\begin{aligned} a \in \mathrm{dom}(f) & \implies \exists b \in b \exists a' \in A \,:\, afb \wedge bga' \\ & \implies (a, a') \in g \circ f = \mathrm{Id}_A \\ & \implies a = a'. \end{aligned}$$

Therefore $afb \implies bga$. ∎

Proof of 2. Exericse. ∎

To conclude this section, we introduce ${}^B A$, the set of all functions f with $f : B \to A$.

Definition 2.74 (Set of all functions)**.**

$${}^B A := \{f \,:\, \mathrm{dom}\, f = B \wedge \mathrm{rng}\, f \subseteq A\}.$$

Theorem 2.75.

$$f \in {}^B A \iff (f : B \to A).$$

Theorem 2.76.

$$A \subseteq B \implies {}^{C}A \subseteq {}^{C}B.$$

Proof. Assume $A \subseteq B$.

$$\begin{aligned} f \in {}^{C}Aq &\implies \operatorname{dom} f = C \wedge \operatorname{rng} f \subseteq A \\ &\implies \operatorname{dom} f = C \wedge \operatorname{rng} f \subseteq B \qquad \text{Assumption} \\ &\implies f \in {}^{C}B. \end{aligned}$$

Thus ${}^{C}B \subseteq {}^{C}A$. ∎

Theorem 2.77. 1. ${}^{\varnothing}A = \{\varnothing\}$,

2. $A \neq \varnothing \implies {}^{A}\varnothing = \varnothing$,

3. ${}^{B}A = \varnothing \iff (A = \varnothing \wedge B \neq \varnothing)$.

Proof of 1. $f \in {}^{\varnothing}A \iff f \subseteq \varnothing \times A \iff f \subseteq \varnothing \iff f = \varnothing$. ∎

Proof of 2. $f \in {}^{A}\varnothing \implies \operatorname{dom}(f) = A \neq \varnothing \wedge \operatorname{rng}(f) = \varnothing$ and thereby

$$\begin{aligned} \operatorname{dom}(f) \neq \varnothing &\implies \exists x \in \operatorname{dom}(f) \\ &\implies \exists y : xRy \\ &\implies y \in \operatorname{rng}(f) = \varnothing \lightning \end{aligned}$$

Thus $\forall f\,(f \notin {}^{A}\varnothing) \implies {}^{A}\varnothing = \varnothing$ ∎

Proof of 3. Exercise. ∎

2.4 Partial Orders and Strict Partial Orders

We wish to draw the reader's attention to the certain particularly useful kinds of relations. To do so, we first need to introduce various properties of relations:

Definition 2.78 (Reflexive)**.** R is *reflexive* when

$$\forall x\,[x \in \operatorname{fld}(R) \implies xRx].$$

Definition 2.79 (Irreflexive)**.** R is *irreflexive* when

$$\forall x\,[x \in \operatorname{fld}(R) \implies \neg(xRx)].$$

Definition 2.80 (Transitive). R is *transitive* when

$$\forall x \forall y \forall z [(x, y, z \in \text{fld}(R) \land xRy \land yRz) \implies xRz].$$

Definition 2.81 (Symmetric). R is *symmetric* when

$$\forall x \forall y [(x, y \in \text{fld}(R) \land xRy) \implies yRx].$$

Definition 2.82 (Asymmetric). R is *asymmetric* when

$$\forall x \forall y [(x, y \in \text{fld}(R) \land xRy) \implies \neg(yRx)].$$

Definition 2.83 (Antisymmetric). R is *antisymmetric* when

$$\forall x \forall y [(x, y \in \text{fld}(R) \land xRy \land yRx) \implies x = y].$$

Now we can define "partial order" and "strict partial order":

Definition 2.84 (Partial Order). R is a *partial order* when R is antisymmetric, reflexive, *and* transitive.

Definition 2.85 (Strict Partial Order). R is a *strict partial order* when R is irreflexive and transitive.

Theorem 2.86. R is a strict partial order when R is asymmetric and transitive.

$\Longleftarrow$. Is trivial as asymmetry implies irreflexivity:

$$(xRy \implies \neg yRx) \implies (xRx \implies \neg xRx) \implies (\neg xRx).$$

■

$\Longrightarrow$. Assume R is irreflexive and transitive. For any x and y we have

$$xRy \land yRx \implies xRx \implies \bot.$$

Thus $\forall x \forall y (\neg xRy \lor \neg yRx)$ or equivalently

$$xRy \implies \neg yRx$$

implying R is asymmetric. ■

The usual $\leq$ relation on the real numbers is a partial order, and so is the usual $\geq$. The usual $<$ on the real numbers is a strict partial order, and so is the usual $>$.

We now give examples in terms of $\subseteq$, $\subset$, and $\in$.

Definition 2.87. 1. $\subseteq_A := \{(x,y) : x,y \in A \wedge x \subseteq y\}$,

2. $\subset_A := \{(x,y) : x,y \in A \wedge x \subset y\}$,

3. $\in_A := \{(x,y) : x,y \in A \wedge x \in y\}$.

Definition 2.88. 1. R is a partial order on A when $R \cap (A \times A)$ is a partial order,

2. R is a strict partial order on A when $R \cap (A \times A)$ is a strict partial order.

Theorem 2.89. 1. $\subseteq_A$ is a partial order on A,

2. $\subset_A$ is a strict partial order on A.

Proof of 1. We need to show $\subseteq_A$ is antisymmetric, reflexive and transitive.
Antisymetric:

$$x \subseteq_A y \wedge y \subseteq_A x \implies x,y \in A \wedge x \subseteq y \wedge y \subseteq x \implies x = y.$$

Reflexive:

$$x \in A \wedge x = x \implies x \in A \wedge x \subseteq x \implies x \subseteq_A x.$$

Transitive:

$$x \subseteq y \wedge y \subseteq z \implies x \subseteq z \implies x \subseteq_A z.$$

The result follows. ∎

Proof of 2. Exercise. ∎

Exercise 2.90. 1. $\subseteq$ is not a relation,

2. $\subset$ is not a relation,

3. $\in$ is not a relation.

Theorem 2.91. 1. If R is a strict partial order on A, then $R \cup \mathrm{Id}_A$ is a partial order on A,

2. If R is a partial order on A, then $R \setminus \mathrm{Id}_A$ is a strict partial order on A.

Proof of 1. By assumption R is irreflexive and transitive. We need to show $R \cup \mathrm{Id}_A$ is reflexive, transitive, and antisymmetric.
Reflexive:

$$a \in A \implies (a,a) \in \mathrm{Id}_A \implies (a,a) \in R \cup \mathrm{Id}_A.$$

Transitive:

$$\begin{aligned} & xR \cup \mathrm{Id}_A y \wedge yR \cup \mathrm{Id}_A z \\ & \quad \implies (xRy \vee x\mathrm{Id}_A y) \wedge (yRz \vee y\mathrm{Id}_A z) \\ & \quad \implies (xRy \wedge yRz) \vee (x\mathrm{Id}_A y \wedge y\mathrm{Id}_A z) \\ & \qquad \vee (xRy \wedge y\mathrm{Id}_A z) \vee (x\mathrm{Id}_A y \wedge yRz) \\ & \quad \implies (xRz) \vee (x = z) && \text{Assumption} \\ & \quad \implies xR \cup \mathrm{Id}_A z. \end{aligned}$$

Antisymmetric: Towards a contradiction suppose

$$\begin{aligned} & xR \cup \mathrm{Id}_A y \wedge yR \cup \mathrm{Id}_A x \wedge x \neq y \\ & \quad \implies (xRy \wedge yRx) \vee (xRy \wedge y\mathrm{Id}_A x) \\ & \qquad \vee (x\mathrm{Id}_A y \wedge yRx) \vee (x\mathrm{Id}_A y \wedge y\mathrm{Id}_A x) \\ & \quad \implies xRy \wedge yRx \\ & \quad \implies xRx && \text{Assumption} \end{aligned}$$

■

Proof of 2. Exercise. ■

It will be useful to have the concept of "smallest" or "least" element of a set A in regard to a relation R:

Definition 2.92 (R-smallest)**.** x is an *R-smallest element* (or *R-first element*, or *R-least element*) of A when

$$x \in A \wedge \forall y\,(y \in A \implies (xRy \vee x = y)).$$

Because $\in$ is not a relation, we cannot use $\in$ in place of R in Definition . So we need the following Definition:

Definition 2.93 ($\in$-smallest)**.** x is an *$\in$-smallest* (or *$\in$-least*) element of A *if and only if* x is an $\in_A$-least element of A.

We need one last property of relations, namely *connectedness* in order to define what we mean by an *order* and a *well-order*.

Definition 2.94 (Connected). R is *connected* when

$$\forall x \forall y \, [x, y \in \mathrm{fld}(R) \implies (xRy \vee yRx \vee x = y)].$$

Definition 2.95 (Order). R is an *order* (or an *ordering*) *if and only if* R is a partial order and R is connected.

Definition 2.96 (Strict Order). R is a *strict order if and only if* R is a strict partial order and R is connected.

Definition 2.97 (Well-order). R is a well-order (or a *well-ordering*) *if and only if* R is a strict order *and*

$$\forall B \, [B \subseteq \mathrm{fld}(R) \wedge B \neq \varnothing \implies \exists x \, (x \text{ is an } R\text{-least element of} B)].$$

Once more, because $\in$ is *not* a relation, we cannot use $\in$ in place of R in Definition 2.97 and 2.98. Se we need the following definition:

Definition 2.98 ($\in$ Well-orders). $\in$ *well-orders* A when $\in_A$ well-orders A.

We now introduce the *natural numbers* as sets which are well-ordered by $\in$.

3 The Natural Numbers

The natural numbers 0, 1, 2, ... are usually axiomized, and characterized, by the following five axioms. They are called the *Peano Postulates*, after the Italian mathematician Giuseppe Peano who invtented them about 1890:

P1 0 is a natural number,

P2 the successor of a natural number is a natural number,

P3 if the successor of x equals the successor of y, then $x = y$,

P4 there is no natural number x such that 0 is the successor of x,

P5 if 0 has the property ψ and, for any natural number x, if x has ψ, then the successor of x has ψ, then every natural number has ψ.

Since set theory is the foundation for mathematics, we wish to construct a set, to be called ω or *omega* (the last letter in the Greek alphabet), that satisfies the Peano Postulates.

Definition 3.1 (Sucessor). $\mathrm{suc}(A)$ is the *successor* of the set A when

$$\mathrm{suc}(A) := A \cup \{A\}.$$

Definition 3.2 (Inductive). A is *inductive* when it contains the empty set and is closed under the operation of successor:

$$\varnothing \in A \wedge \forall y\,(y \in A \implies \mathrm{suc}(y) \in A).$$

We are now in a position to define the concept of *natural number*.

Definition 3.3 (Natural Number). Let ω denote the set of natural numbers, then

$$\omega = \{x : \forall B\,(B \text{ is inductive} \implies x \in B)\}.$$

Definition 3.4. Let the following serve a short-hands for natural numbers:

$$\begin{aligned} 0 &= \varnothing \\ 1 &= \mathrm{suc}(0) \\ 2 &= \mathrm{suc}(1) \\ &\vdots \end{aligned}$$

> From now on, we let k, m, n (with and without subscripts) stand for natural numbers.

Let us now show that our *natural numbers* satisfy the Peano Postulates.

Theorem 3.5 (P1)**.** o is a natural number.

$$0 \in \omega.$$

Proof. By definition every inductive set contains the empty set $\varnothing$. Thus, also by definition, $\varnothing = 0$ is a natural number. ∎

Theorem 3.6 (P2)**.** If x is a natural number then its successor is a natural number

$$x \in \omega \implies \mathrm{suc}(x) \in \omega.$$

Proof. If x is a natural number this means $x \in A$ for every inductive set A. By definition then, $\mathrm{suc}(x) \in A$ for every inductive set A. ∎

We defer P3 until later and turn to considering P4:

Theorem 3.7 (P4)**.** There is no natural number x such that $0 = \mathrm{suc}(x)$.

Proof. Suppose *towards a contradiction* that $\exists x : 0 = \mathrm{suc}(x)$. Then

$$\begin{aligned} 0 = \mathrm{suc}(x) &\implies \varnothing = x \cup \{x\} \\ &\implies x \notin x \cup \{x\} \\ &\implies x \neq x. \lightning \end{aligned}$$

∎

On the basis of our axioms thus far, there might not exist any inductive set. In that case, *every* set would be a natural number, and P5 would be false for natural numbers. So our next step is to assume the existence of an inductive set:

Axiom 6 (Infinity). $\exists A\,(A \text{ is inductive}).$

This assumption is called the Axiom of Infinity because it gives us a set A that will turn out to be infinite. Using only the axioms assumed before A6, we cannot prove that there exists an infinite set. Of course, we have not yet defined precisely what we mean by an infinite (or a finite) set, but we will do so soon.

Definition 3.8.

$$\omega := \{x : x \in \omega\}.$$

Our next goal is to prove that ω, or "omega", is not the empty set.

Theorem 3.9.

$$x \in \omega \iff x \in \mathbb{N}.$$

We now show ω satisfies P5.

Theorem 3.10. Let $B \subseteq \omega$ then

$$[0 \in B \wedge \forall n\,(n \in B \implies \text{suc}(n) \in B)] \implies B = \omega.$$

Theorem 3.11 (The Principle of Mathematical Induction). Let $\psi(x)$ be any formula of set theory, then

$$[\psi(0) \wedge \forall n\,(\psi(n) \implies \psi(\text{suc}(n)))] \implies \forall n\,[\psi(n)].$$

Our next development is oriented toward showing that ω satisfies P3:

Definition 3.12 ($\in$-transitive). B is $\in$-transitive when

$$\forall x\,(x \in B \implies x \subseteq B).$$

Theorem 3.13. $\forall n \in \omega$; n is $\in$-transitive.

Proof. Let $\psi(x) \iff x$ is $\in$-transitive.

Base:

$$\begin{aligned}
\psi(0) &\iff 0 \text{ is } \in\text{-transitive} \\
&\iff \forall x\,(x \in \varnothing \implies x \subseteq \varnothing) \\
&\iff \forall x\,(\bot \implies x \subseteq \varnothing) \\
&\iff \top.
\end{aligned}$$

Induction hypothesis: Assume n is $\in$-transitive.

Notice $x \in \text{suc}(n) \implies x \in n \cup \{n\} \implies x \in n \vee x = n$ and $x \in n \overset{\text{IH}}{\implies} x \subseteq n$ and $x = n \implies x \subseteq n \cup \{n\}$. Thus, by the principle of mathematical induction the result follows. ∎

Theorem 3.14. $\forall n \in \omega;\, n \notin n$.

Theorem 3.15.

$$\forall n \,[B \subseteq n \wedge B \neq \varnothing \implies \exists x \,(x \text{ is an } \in\text{-least element of } B)].$$

Proof. Let $\Phi(B, x) \iff x$ is the $\in_B$-least element of B and

$$\psi(n) \iff \forall n \,(B \subseteq n \wedge B \neq \varnothing \implies \exists x \,\Phi(B, x)).$$

Base:

$$\begin{aligned}\psi(0) &\iff \forall n \,(B \subseteq \varnothing \wedge B \neq \varnothing \implies \exists x \,\Phi(B, x)) \\ &\iff \forall n \,(\bot \implies \exists x \,\Phi(B, x)) \\ &\iff \top.\end{aligned}$$

Induction hypothesis: Assume $\psi(n) \equiv \top$.

Notice

$$\begin{aligned}B \subseteq \text{suc}(n) &\implies B \subseteq n \cup \{n\} \\ &\implies \forall a \,(a \in B \implies a \in n \vee a \in \{n\}) \\ &\implies \forall a \,(a \in B \implies a \in n \vee a = n).\end{aligned}$$

However, $n \notin n$ by Theorem 3.14 so $\neg(a \in \wedge\ a = n)$. Thus $B \subseteq n$ or (exclusively) $B = \{n\}$.

When $B \subseteq n$ we have

$$\psi(n) \implies [B \subseteq n \wedge B \neq \varnothing \overset{\text{IH}}{\implies} \exists x \,\Phi(B, x)]$$

and when $B = \{n\}$ we have

$$\begin{aligned}\Phi(B, x) &\iff x \in \{n\} \wedge \forall y \,(y \in \{n\} \implies x \in_B y \vee x = y) \\ &\iff n \in_B n \vee n = n \\ &\iff \top.\end{aligned}$$

Thus $\psi(n) \implies \psi(\text{suc}(n))$ and the result follows from the principle of mathematical induction. ∎

Theorem 3.16 (ω satisfies P3)**.**

$$\text{suc}(m) = \text{suc}(n) \implies m = n.$$

Proof. Assume $\text{suc}(m) = \text{suc}(n)$, then

$$\begin{aligned}
&(a \in \text{suc}(m) \iff a \in \text{suc}(n)) \\
&\quad\iff (a \in m \cup \{m\} \iff a \in n \cup \{n\}) \\
&\quad\iff (a \in m \vee a = m \iff a \in n \vee a = n) \\
&\quad\iff (a \in m \iff a \in n) \vee (a \in m \iff a = n) \\
&\qquad\vee (a = m \iff a \in n) \vee (a = m \iff a = n) \\
&\quad\iff (m = n) \vee (m = \{n\}) \vee (n = \{m\}) \vee (m = n).
\end{aligned}$$

Note

$$\begin{aligned}
m = \{n\} &\implies \text{suc}(\{n\}) = \text{suc}(n) \\
n = \{m\} &\implies \text{suc}(\{m\}) = \text{suc}(m)
\end{aligned}$$

both contradict our assumption.

Thus we can conclude

$$\text{suc}(m) = \text{suc}(n) \implies m = n$$

and the result follows by the principle of mathematical induction. ∎

Theorem 3.17.

$$n = 0 \vee \exists m\, \{n = \text{suc}(m)\}.$$

Proof. Let $\psi(n) \iff n = 0 \vee \exists m\, \{n = \text{suc}(m)\}$.

Base:

$$\psi(0) \iff 0 = 0 \vee \exists m\, \{n = \text{suc}(m)\} \iff \top.$$

Induction hypothesis: Assume $\psi(n) \equiv \top$.

$$\begin{aligned}
\psi(n) &\overset{\text{IH}}{\implies} \exists m\, \{n = \text{suc}(m) \vee n = 0\} \\
&\implies \exists m\, \{\text{suc}(n) = \text{suc}(\text{suc}(m))\} \\
&\implies \exists m'\, \{m' = \text{suc}(m) \wedge \text{suc}(n) = \text{suc}(m')\} \\
&\implies \psi(\text{suc}(n)).
\end{aligned}$$

Thus, by the principle of mathematical induction, the result follows. ∎

Theorem 3.18. 1. Every member of a natural number is a natural number,

2. ω is $\in$-transitive.

Definition 3.19. 1. $m < n \iff m \in n$,

2. $m \leq n \iff (m < n \vee m = n)$.

Theorem 3.20. $0 \leq n$.

Proof. Towards a contradiction

$$\exists n\,(0 > n) \implies \exists n\,(n \in \varnothing) \implies \exists n\,(n \in \varnothing)\lightning.$$

■

Theorem 3.21. $m < n \implies \mathrm{suc}(m) \leq n$.

Proof. Assume $m < n$ and, towards a contradiction, that $n < \mathrm{suc}(m)$.

$$\begin{aligned} & m < n \wedge n < \mathrm{suc}(m) \\ & \quad \implies m \in n \wedge n \in \mathrm{suc}(m) \\ & \quad \implies m \in n \wedge n \in m \cup \{m\} \\ & \quad \implies m \in n \wedge (n \in m \vee n = m) \\ & \quad \implies (m \in n \wedge n \in m) \vee (m \in n \wedge n = m). \end{aligned}$$

Breaking the disjunction into two cases:

$$\begin{aligned} & m \in n \wedge n \in m \\ & \quad \implies m \subseteq n \wedge n \subseteq m \wedge n \in m \qquad \in\text{-transitivity} \\ & \quad \implies n = m \wedge n \in m \\ & \quad \implies n \in m\lightning \end{aligned}$$

and $m \in n \wedge n = m \implies n \in n\lightning$. ■

Theorem 3.22. $m < n \vee m = n \vee n < m$.

Theorem 3.23. $\in$ well-orders n.

Theorem 3.24.

$$\exists n\,[\varphi(n)] \implies \exists m\,[m \text{ is the } \in\text{-least natural number } k \text{ such that } \varphi(k)].$$

Theorem 3.25. $\in$ well-orders ω.

Next we give an extremely important theorem, the *Recursion Theorem* for natural numbers, which justifies definition by *recursion*:

3.1 Recursion

Theorem 3.26 (Recursion Theorem, first form)**.** Let H be a function. Then there is a unique function F such that

1. $\mathrm{dom}(F) = \omega$, and
2. $\forall n\,[F(n) = H(F|n)]$.

Theorem 3.27 (Recursion Theorem, second form)**.** Let $a \in A$ and $G : A \times \omega \to A$. Then there is a unique function $h : \omega \to A$ such that

1. $h(0) = a$,
2. $\forall n\,[h(\mathrm{suc}(n) = G(h(n), n)]$.

Our first application of the Recursion Theorem is to show that the Peano Postulates P1–P5 characterize the natural numbers as given by the structure $(\omega, \mathrm{suc}\,|\omega, 0)$. To do so, we first need to define the concept of ordered triple, then the type of the structure $(\omega, \mathrm{suc}\,|\omega, 0)$, and then the concept of isomorphism.

Definition 3.28. $(A, B, C) := (A, (B, C))$.

Definition 3.29. (A, f, a) has the structural type of $(\omega, \mathrm{suc}\,|\omega, 0)$ if $a \in A$ and $f : A \to A$.

Definition 3.30. (A, f, a) and (B, g, b) are *isomorphic* when

1. (A, f, a) and (B, g, b) have the structural type of $(\omega, \mathrm{suc}\,|\omega, D)$,
2. there is a bijection $H : A \to B$ such that $H(a) = b$, and
3. $\forall x \in A\,[H(f(x)) = g(H(x))]$.

Theorem 3.31 (Isomorphism Theorem for ω)**.** If (A, f, a) has the structural type of $(w, \mathrm{suc}\,|\omega, 0)$ and (A, f, a) satisfies P1–P5, then $(\omega, \mathrm{suc}\,|\omega, 0)$ is isomorphic to (A, f, a).

We now use the Recursion Theorem to define addition, multiplication, and exponentiation on natural numbers:

3.1.1 Addition

Definition 3.32 (Addition)**.** For each m, let $A = \omega$ and let $a = m$ and let $G : \omega \times \omega \to \omega$ be such that $G(n, k) = \mathrm{suc}(n)$ for all n and k. Define F_m to be the unique function F given by . Define, for each m and n,

$$m + n := F_m(n).$$

Theorem 3.33. $\forall m\,[m + 0] = m$.

Proof. There $\exists! h_m : h_m(0) = m \wedge h_m(\mathrm{suc}(n)) = \mathrm{suc}(h(n))$. By definition we have

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

■

Theorem 3.34. $\forall m\,\forall n\,(m + \mathrm{suc}(n) = \mathrm{suc}(m + n))$.

Proof. Let m be arbitrary and

$$\psi(n) \iff (m + \mathrm{suc}(n) = \mathrm{suc}(m + n))$$

further let h_m be the unique function such that $m + n = h_m(n)$.
Base:

$$m + \mathrm{suc}(0) = h_m(\mathrm{suc}(0)) = \mathrm{suc}(h_m(0)) = \mathrm{suc}(m) = \mathrm{suc}(m + 0)$$

Induction hypothesis: $m + \mathrm{suc}(n) = \mathrm{suc}(m + n)$.

Now we need show $m + \mathrm{suc}(\mathrm{suc}(m)) = \mathrm{suc}(m + \mathrm{suc}(n))$. So, by induction hypothesis,

$$\begin{aligned}
&\mathrm{suc}(m + \mathrm{suc}(n)) \\
&\quad = \mathrm{suc}(\mathrm{suc}(m + n)) \\
&\quad = \mathrm{suc}(\mathrm{suc}(h_m(n)) \\
&\quad = \mathrm{suc}(h_m(\mathrm{suc}(n))) \\
&\quad = h_m(\mathrm{suc}(\mathrm{suc}(n))) \\
&\quad = m + \mathrm{suc}(\mathrm{suc}(n))
\end{aligned}$$

The result follows from the principle of mathematical induction. ■

3.1.2 Multiplication

Definition 3.35 (Multiplication). For each m, let $A = \omega$ and let $a = 0$ and let $G : \omega \times \omega \to \omega$ be such that $G(n, k) = n + m$ for all n and all k. Define F_m to be the unique function F then given by 3.32. Define, for each m and n,

$$m \cdot n := F_m(n).$$

Theorem 3.36. $\forall m\,[m \cdot 0 = 0]$

Proof. Let $h_m^{\times}$ be the unique function such that $h_m^{\times}(0) = 0$ and $m \cdot n = h_m^{\times}(n)$, then by definition

$$m \cdot 0 = h_m^{\times}(0) = 0.$$

■

Theorem 3.37. $\forall m \forall n \, [m \cdot \mathrm{suc}(n) = m \cdot n + m]$.

3.1.3 Exponentiation

Definition 3.38 (Exponentiation)**.** For each m, let $A = \omega$ and let $a = 1$ and let $G : \omega \times \omega$ be such that $G(n, k) = n \cdot m$ for all n and all k. Define F_m to be the unique function F then determined by 3.32. Define $m^n = F_m(n)$ for each m and n.

Theorem 3.39. $\forall m \, [m^0 = 1]$.

Proof. Let $h_m^{\wedge}$ be the unique function satisfying $m^n = h_m^{\wedge}(n)$, then by definition

$$m^0 = h_m^{\wedge}(0) = 1.$$

■

Theorem 3.40. $\forall m \forall n \, [m^{\mathrm{suc}(n)} = m^n \cdot m]$.

Exercise 3.41. Prove

1. $\forall m \forall n \, [m + n = n + m]$,
2. $\forall m \forall n \forall k \, [(m + n) + k = m + (n + k)]$,
3. $\forall m \forall n \, [m \cdot n = n \cdot m]$,
4. $\forall m \forall n \forall k \, [(m \cdot n) \cdot k = m \cdot (n \cdot k)]$,
5. $\forall m \forall n \forall k \, [(m^n)^k = m^{n \cdot k}]$.

3.2 The Set of Integers

We wish to define a set which we can use as the *integers* (at this point we only have natural numbers). First, we define what will serve as the *negative integers*.

Definition 3.42 (Negative Integer)**.**

$$\forall n \, [n \neq 0 \implies -n = (0, n)].$$

Definition 3.43 (Negative Integers).

$$\mathbb{Z}^- := \{-n : n \in \omega \setminus \{0\}\}.$$

Theorem 3.44. $\omega \cap \mathbb{Z}^- = \varnothing$.

Proof. Towards a contradiction assume $a \in \omega \cap \mathbb{Z}^-$.

$$\begin{aligned} & a \in \omega \cap \mathbb{Z}^- \\ & \quad \implies a \in \omega \wedge a \in \mathbb{Z}^- \\ & \quad \implies \varnothing \in a \wedge a \in \mathbb{Z}^- \\ & \quad \implies \exists b : a = (0, b) \wedge \varnothing \in (0, b) \\ & \quad \implies \varnothing \in \{\{0\}, \{0, b\}\} \\ & \quad \implies \varnothing = \{0\} \vee \varnothing = \{0, b\} \lightning \end{aligned}$$

■

Definition 3.45 (Integers).

$$\mathbb{Z} := \omega \cup \mathbb{Z}^-.$$

This set $\mathbb{Z}$ will be the integers for us. We wish to extend the relation $<$, defined on ω at 3.19, to all of $\mathbb{Z}$. To avoid confusion here, we rename the $<$ defined at 3.19, as $<_\omega$.

Definition 3.46.

$$<_{\mathbb{Z}} := <_\omega \cup \{(-m, -n) : n \in m\} \cup \{(-m, n) : m \neq 0\}.$$

Theorem 3.47.

1. $<_\omega \cap \{(-m, -n) : n \in m\} = \varnothing$,
2. $<_\omega \cap \{(-m, m) : m \neq 0\} = \varnothing$,
3. $\{(-m, -n) : n \in m\} \cap \{(-m, n) : m \neq 0\} = \varnothing$.

Proof of 1. Towards a contradiction assume $a \in <_\omega \cap \{(-m, -n) : n \in m\}$.

$$\begin{aligned} & \exists m, n : (m, n) = (-m, -n) \wedge m < n \\ & \quad \implies \exists m, n : m = -m \wedge n = -n \wedge m < n \\ & \quad \implies \exists m, n : m = (0, m) \wedge n = (0, n) \wedge m < n \\ & \quad \implies \varnothing \in (0, m) \\ & \quad \implies \varnothing = \{0\} \vee \varnothing = \{0, m\} \lightning \end{aligned}$$

Proof of 2.

Proof of 3.

3.3 Homomorphisms of Relations

We next wish to investigate functions $f : A \to B$, where $A = \text{fld}(R)$ and $B = \text{fld}(S)$, that are "*structure-preserving*". Such functions are called "*homomorphisms*":

Definition 3.48. Let $f : A \to B$ and $A = \text{fld}(R)$ and $B = \text{fld}(S)$.

1. f is a homomorphism $\iff \forall x \forall y \, (xRy \iff f(x)Sf(y))$,
2. f is an embedding of R *into* S (or: of A into B) $\iff$ f is 1-1 $\wedge$ f is a homomorphism,
3. f is an isomorphism $\iff$ f is bijective $\wedge$ f is a homomorphism,
4. f is an automorphism $\iff$ f is an isomorphism $\wedge$ $A = B$.

Assume that we have extended our addition $+$ from ω to our integers $\mathbb{Z}$. Then do the following exercise:

Exercise 3.49. Find all the:

1. automorphisms of $<_\omega$,
2. automorphisms of $<_\mathbb{Z}$,
3. embeddings of $<_\omega$ in $<_\mathbb{Z}$,
4. embeddings of $<_\mathbb{Z}$ in $<_\omega$,
5. embeddings of $<_\omega$ in $<_\omega$,
6. embeddings of $<_\mathbb{Z}$ in $<_\mathbb{Z}$.

Answer.

1. The only automorphism is the identity.
2. All linear shifts $f(n) \mapsto n + m$ for fixem m.

Theorem 3.50. $<_{\mathbb{Z}}$ is a strict order and is not a well-ordering.

To develop further our ideas about $\mathbb{Z}$, we need some new definitions:

Definition 3.51 (R-predecessor)**.** x is an *R-predecessor* of y *if and only if*

$$xRy \wedge x \neq y.$$

Definition 3.52 (R-immediate predecessor)**.** x is an *R-immediate predecessor* of y *if and only if*

1. x is an R-predecessor of y, *and*
2. $\forall z\,[xRz \implies (z \text{ is not an } R\text{-predecessor of } y) \vee x = z]$

Definition 3.53 (R-successor)**.** y is an *R-successor* of x *if and only if*

$$x \text{ is an } R\text{-predecessor of } y.$$

Definition 3.54 (R-immediate successor)**.** y is an *R-immediate successor* of x *if and only if*

$$x \text{ is an } R\text{-immediate predecessor of } y.$$

Theorem 3.55.

1. Every member of ω has $<_\omega$-immediate successor,
2. every member of $\omega \setminus \{0\}$ has an $<_\omega$-immediate predecessor,
3. every member of $\mathbb{Z}$ has $<_{\mathbb{Z}}$-immediate predecessor and an $<_{\mathbb{Z}}$-immediate successor.

Proof of 1. $\mathrm{suc}(m)$ is the $<_\omega$-immediate successor of $n \iff n$ is the $<_\omega$-immediate predecessor of $\mathrm{suc}(n)$.

Notice n is the $<_\omega$-predecessor of $\mathrm{suc}(n)$,

$$\begin{aligned} n <_\omega \mathrm{suc}(n) \wedge n \neq \mathrm{suc}(n) &\iff n <_\omega \mathrm{suc}(n) \\ &\iff n \subseteq n \cup \{n\} \\ &\iff \top. \end{aligned}$$

and

$$n <_\omega \ell \wedge \ell <_\omega \mathrm{suc}(n)$$

$$\begin{aligned} &\implies n \in \ell \wedge \ell \in n \cup \{n\} \\ &\implies (n \subseteq \ell) \wedge (\ell \subseteq n \vee \ell = n) \\ &\implies \ell = n. \end{aligned}$$

■

3.4 Finite and Infinite Sets

We next wish to introduce the idea that two sets A and B have the *same cardinal number* or are *equipotent*.

Definition 3.56.

$$A \approx_f B \iff (\mathrm{dom}(f) = A \wedge \mathrm{rng}(f) = B \wedge f \text{ is injective})$$

Now $A \approx_f B$ is read "A is *equipotent* to B under f". We will write $A \approx B$, to be read "A is equipotent to B".

Definition 3.57. $A \approx B \iff \exists f\,[A \approx_f B]$.

The next theorem is an easy consequence of these two definitions:

Theorem 3.58.

1. $A \approx A$,
2. $A \approx B \implies B \approx A$,
3. $A \approx B \wedge B \approx C \implies A \approx C$,
4. $(A \approx_f B \wedge C \subseteq A) \implies C \approx f[C]$.

Proof of 1. Let $f = \mathrm{Id}_A$. Then $\mathrm{dom}(f) = A \wedge \mathrm{rng}(f) = A \wedge f$ injective. Thus $A \approx A$. ■

Proof of 2. $A \approx B \implies \exists f : \mathrm{dom}(f) = A \wedge \mathrm{rng}(f) = B \wedge f$ injective. Note we have (by definition) that $\breve{f}$ is injective because f is a function and $\breve{f}$ is a function because f is injective. ■

Proof of 3. $A \approx B \wedge B \approx C \implies \exists f, g : A \approx_f B \wedge B \approx_g C$ where $f : A \to B$ and $g : B \to C$ are injective. Notice $g \circ f : A \to C$ and $g \circ f$ injective and thus $A \approx_{g\circ f} C \implies A \approx C$. ■

Proof of 4. Assume $A \approx_f B$ and $C \subseteq A$. This means

$$\mathrm{dom}(f) = A \wedge rng(f) = B \wedge f \text{ injective} \wedge C \subseteq A.$$

Let $g : C \to f[C] = \{c : \exists x\,(xfc)\}$ be given by

$$g = \{(c, b) : c \in C \wedge cfb\}.$$

Thus $\mathrm{dom}(g) = C \wedge \mathrm{rng}(g) = f[C] \wedge g$ injective which means $C \approx_g f[C] \implies C \approx f[C]$. ∎

Unfortunately, $\approx$ is too big to be a relation:

Theorem 3.59. $\approx$ is not a relation.

Sketch of Proof. We have $\forall A\,(A \approx A)$ so

$$\{(A, A) : A \text{ a set}\} \subseteq \approx.$$

This means $\approx$ contains the universal set and thus is not a set. ∎

We next define $A \preccurlyeq B$, read "A is less than or equipotent to B":

Definition 3.60. $A \preccurlyeq B \iff \exists C\,[A \approx C \wedge C \subseteq B]$.

The next theorem gives some easy consequences of this definition:

Theorem 3.61.

1. $A \approx B \implies A \preccurlyeq B$,
2. $A \subseteq B \implies A \preccurlyeq B$,
3. $A \preccurlyeq A$,
4. $A \preccurlyeq B \wedge B \preccurlyeq C \implies A \preccurlyeq C$.

Proof of 1. $A \approx B \implies \exists C = B : A \approx C \wedge C \subseteq B \implies A \preccurlyeq B$. ∎

Proof of 2. $A \subseteq B \implies A \approx A \wedge A \subseteq B \implies A \preccurlyeq B$. ∎

Proof of 3. $A \approx A \wedge A \subseteq A \implies A \preccurlyeq A$. ∎

Proof of 4.

$$\begin{aligned}
&A \preccurlyeq B \wedge B \preccurlyeq C \\
&\quad \implies \exists D_0, D_1 : A \approx D_0 \wedge D_0 \subseteq B \wedge B \approx D_1 \wedge D_1 \subseteq C \\
&\quad \implies \exists D_0, D_1, f, g : A \approx_f D_0 \wedge D_0 \subseteq B \wedge B \approx_g D_1 \wedge D_1 \subseteq C \\
&\quad \text{Note: } f[A] \subseteq B \wedge g[B] \subseteq C \implies g[f[A]] \subseteq C. \\
&\quad \implies A \approx_{g \circ f} g[f[A]] \wedge g[f[A]] \subseteq C \\
&\quad \implies A \preccurlyeq C.
\end{aligned}$$

∎

Now we define $A \prec B$, read "A is less potent than B""

Definition 3.62. $A \prec B \iff [A \preccurlyeq B \wedge \neg (B \preccurlyeq A)]$.

Here are some easy consequences:

Theorem 3.63.

1. $\neg (A \prec A)$,
2. $(A \prec B \wedge B \prec C) \implies A \prec C$,
3. $(A \prec B) \implies \neg (B \prec A)$,
4. $(A \prec B \wedge B \preccurlyeq C) \implies A \prec C$.

Proof of 1. $A \prec A \iff A \preccurlyeq A \wedge \neg (A \preccurlyeq A) \iff \bot$. ■

Proof of 2.

$$
\begin{aligned}
& A \prec B \wedge B \prec C \\
& \quad \implies A \preccurlyeq B \wedge \neg (B \preccurlyeq A) \wedge B \preccurlyeq C \wedge \neg (C \preccurlyeq B) \\
& \quad \implies (A \preccurlyeq B \wedge B \preccurlyeq C) \wedge \neg (C \preccurlyeq B \wedge B \preccurlyeq A) \\
& \quad \text{Note that } (\neg p \wedge \neg q) \implies \neg (p \wedge q) \\
& \quad \implies A \preccurlyeq C \wedge \neg (C \preccurlyeq A) \\
& \quad \implies A \prec C.
\end{aligned}
$$

■

Exercise 3.64. $\mathrm{dom}(f) \approx f$.

Answer. Let $g : \mathrm{dom}(f) \to f$ be given by

$$g = \{(a, f(a)) \,:\, a \in \mathrm{dom}(f)\}$$

then $\exists g \,:\, \mathrm{dom}(g) = \mathrm{dom}(f) \wedge \mathrm{rng}(g) = f \wedge g$ injective $\implies \mathrm{dom}(f) \approx_g f \implies \mathrm{dom}(f) \approx f$. ◆

We can now define what we mean by a set being "finite" or "infinite."

Definition 3.65.

1. A is finite $\iff \exists n \, [A \approx n]$,
2. A is infinite $\iff \neg (A \text{ is finite})$.

Now we give some simple theorems about finite and infinite sets:

Theorem 3.66. A is infinite $\implies \forall n\,(n \prec A)$.

Proof. Assume A infinite and proceed with the PMI, letting

$$\psi(n) \iff n \preccurlyeq A.$$

Base: $\psi(0) \iff \varnothing \preccurlyeq A \iff \exists \varnothing \subseteq A : \varnothing \approx \varnothing \iff \top$.

Induction hypothesis: $n \preccurlyeq A$.

We $\psi(n) \implies \exists A' \subseteq A : n \approx A' \implies \exists A' \exists f : A' \subseteq A \wedge n \approx_f A'$ which decomposes into two cases

1. $A' = A \implies n \approx A \implies A$ is finite. $\lightning$
2. $A' \subset A \implies \exists a \in A \setminus A'$.

Consider $g = f \cup \{(n, a)\}$ — this is a function satisfying

$$\begin{aligned} \operatorname{dom}(g) &= \operatorname{dom}(f) \cup \{n\} = n \cup \{n\} = \operatorname{suc}(n), \\ \operatorname{rng}(g) &= A' \cup \{a\} \subseteq A, \end{aligned}$$

and g injective (not proved but trivial).

Thus $n \approx_g A' \cup \{a\} \implies n \preccurlyeq A$. By PMI $\forall n$; $n \preccurlyeq A$. ∎

Theorem 3.67. $\forall m\,(m \text{ is finite})$

Proof. $m \approx m \implies m \preccurlyeq m \implies \exists m\,(m \preccurlyeq m) \implies m$ is finite. ∎

Theorem 3.68. $(A \text{ is finite} \wedge A \approx B) \implies B$ is finite.

Proof. $\exists n\,(A \approx n \wedge A \approx B) \implies \exists n\,(B \approx n) \implies B$ is finite. ∎

Theorem 3.69. A is finite $\implies A \cup \{y\}$ is finite.

Proof. $\exists n\,(A \approx n) \implies \exists n \exists f\,(A \approx_f n)$ where $\operatorname{dom}(f) = A \wedge \operatorname{rng}(g) = n \cup \{n\} \wedge f$ injective. This means

$$\exists g\,(\operatorname{dom}(g) = A \cup \{y\} \wedge \operatorname{rng}(g) = n \cup \{n\} \wedge f \text{ injective})$$

where $g = f \cup \{y, \operatorname{suc}(n)\}$. Thus $A \cup \{y\} \approx_g \operatorname{suc}(n) \implies A \cup \{y\}$ finite. ∎

Theorem 3.70. $A \subseteq n \implies A$ is finite.

Proof. Let A be arbitrary and

$$\psi(n) \iff (A \subseteq n \implies A \text{ is finite}).$$

Base: $\psi(0) \iff (A \subseteq \varnothing \implies A \text{ is finite}) \iff \varnothing \text{ is finite} \iff \top$.
Induction hypothesis: $A \subseteq n \implies A$ is finite.

Suppose $A \subseteq \text{suc}(n) = n \cup \{n\}$. Notice $A \subseteq n \implies A$ is finite by induction hypothesis so suppose $A \not\subseteq n$.

$A \not\subseteq n \implies n \in A$ so let $A^- = A \setminus \{n\}$. A^- is finite by the induction hypothesis because $A^0 \subseteq n$. This means $A^- \cup \{n\}$ is finite by Theorem **??**. Thus A is finite. ∎

Theorem 3.71. $(A \text{ is finite} \wedge B \subseteq A) \implies A$ is finite.

Proof. A is finite $\wedge\, B \subseteq A \implies \exists n\,(A \approx n \wedge B \subseteq A) \implies \exists f\,(\text{dom}(f) = A \wedge \text{rng}(f) = n \wedge f \text{ injective})$.

Consider $g : B \to f[B]$ where $B \subseteq A \wedge f[B] \subseteq n$, it follows that $f[B] \subseteq n \implies f[B]$ is finite by Theorem 3.35. Letting $m \approx f[B]$, this means $g = f \cap B \times \text{rng}(f)$ is a function satisfying

$$\text{dom}(g) = B \wedge \text{rng}(g) \approx m \wedge g \text{ injective}$$

which implies $B \approx_g m \implies B \approx m \implies B$ is finite. ∎

Theorem 3.72. $(A \text{ is finite} \wedge B \preccurlyeq A) \implies B$ is finite

Proof. We have A is finite $\implies \exists n : A \approx n$ and $B \preccurlyeq A \implies \exists A' \subseteq A : B \approx A'$. Thus there is injective f and g such that

1. $\text{dom}(f) = A \wedge \text{rng}(f) = n$, and
2. $\text{dom}(g) = B \wedge \text{rng}(g) = A' \subseteq A$.

It follows

$$f \circ g : B \to n' \subseteq n$$

is injective and thus

$$\exists m : B \approx n' \wedge n' \approx m \implies B \approx m \implies B \text{ is finite.}$$

∎

Theorem 3.73. $(A \text{ is infinite} \wedge A \subseteq B) \implies B$ is infinite.

Theorem 3.74. $(A \text{ is infinite} \wedge A \preccurlyeq B) \implies B$ is infinite.

Theorem 3.75. A is finite $\implies$ $A \setminus B$ is finite.

Theorem 3.76. (A is finite $\vee$ B is finite) $\implies$ $A \cap B$ is finite.

Proof. Without loss of generality assume A is finite, then we have, for any B

$$(A \cap B \subseteq A) \wedge A \text{ is finite} \implies A \cap B \text{ is finite.}$$

■

Theorem 3.77. (A is finite $\wedge$ B is finite) $\implies$ $A \cup B$ is finite.

Theorem 3.78.

$$(C \text{ is finite} \wedge \forall c\,[c \in C \implies C \text{ is finite}]) \implies \bigcup C \text{ is finite.}$$

Theorem 3.79. $A \approx A \times \{y\}$.

Theorem 3.80. (A is finite $\wedge$ B is finite) $\implies$ $A \times B$ is finite.

Dedekind.

Theorem 3.81 (Dedekind-infinite). A is a *Dedekind-infinite* (or D-infinite) when there is some function $f : A \to A$ which is an injection but not a surjection:

$$A \text{ is D-infinite} \iff \exists f : A \to A\,(f \text{ injective} \wedge f \text{ not surjective})$$

Moreover, A is *Dedekind-finite* (or D-finite) when A is not D-infinite.

Theorem 3.82. $\forall n\,(n \text{ is D-finite})$

Proof. Towards a contradiction assume $\exists n$ is D-infinite. This implies

$$\exists f : n \to n' \;:\; f \text{ injective } \wedge\, n' \subset n.$$

Note:

- $\mathrm{dom}(f) = n \implies \mathrm{rng}(\breve{f}) = n$, and
- f a function $\implies$ $\breve{f}$ is injective.

and thus $\breve{f} : n' \to n$ is a bijection.

Consider $g : n \to n$ a *bijection* given by $(g \circ \breve{f})(n) = n$, namely

$$g = \left\{(\breve{f}(m), m) \;:\; m \in \mathrm{dom}(\breve{f})\right\} \cup \left\{(m, n) \;:\; m \in n \setminus \mathrm{dom}(\breve{f})\right\}.$$

Let $h = g \circ \breve{f}$ and thus

$$\begin{aligned} h = \mathrm{Id} : n' &\to n \\ \implies \breve{h} : \mathrm{Id} : n &\to n' \\ \implies \breve{h}[n] &\subseteq n' \\ \implies n &\subseteq n'. \lightning \end{aligned}$$

■

Theorem 3.83. A is finite $\implies$ A is D-finite.

Proof. Towards a contradiction suppose A is finite $\wedge$ A is D-infinite. We have $\exists m : A \approx m \wedge A$ is D-finite $\implies m$ is D-infinite. $\lightning$. ■

Theorem 3.84. A is D-infinite $\implies$ A is infinite.

Theorem 3.85. ω is D-infinite.

Proof. Let $f : \omega \to \omega$ be given by $f = \{(n, \mathrm{suc}(n)) : n \in \omega\}$. Clearly $\varnothing \notin \mathrm{rng}(f)$ and f-injective. Thus ω is D-infinite by definition. ■

Theorem 3.86. $m < n \implies \neg(m \approx n)$.

Theorem 3.87. $m \approx n \implies m = n$.

Theorem 3.88 (Dirichlet's Pigeonhole Principle)**.** If $m < n$ and $f : n \to m$, then for some $k < m$ and some $n_1, n_2 < n$, we have $n_1 \neq n_2$ and $f(n_1) = f(n_2) = k$:

$$\begin{aligned} &(m < n \wedge f : n \to m) \implies \\ &\quad \exists k, n_1, n_2 \, (k < m \wedge n_1 < n \wedge n_2 < n \wedge f(n_1) = f(n_2) = k.) \end{aligned}$$

Theorem 3.89. There is no surjective function $f : n \to \mathrm{suc}(n)$:

$$\neg \exists f : n \to \mathrm{suc}(n) \wedge f \text{ surjective.}$$

Proof. Let $\psi(n) \iff \neg \exists f : n \to \mathrm{suc}(n) \wedge f$ surjective.
Base: $\mathrm{dom}(f) = \varnothing \implies \mathrm{rng}(f) = \varnothing \neq \mathrm{suc}(\varnothing)$. Thus $\psi(0)$.
Induction Hypothesis: Suppose $\neg \exists f : n \to \mathrm{suc}(n) \wedge f$ surjective.

Towards a contradiction let f be a surjective function on $\mathrm{suc}(n) \times \mathrm{suc}(\mathrm{suc}(n))$. There are two cases:

$$\begin{aligned} &\underline{f(\mathrm{suc}(n)) = \mathrm{suc}(\mathrm{suc}(n))} \\ &\quad \implies f = f' \cup \{(\mathrm{suc}(n), \mathrm{suc}(\mathrm{suc}(n)))\} \end{aligned}$$

$$\implies f' : n \to \mathrm{suc}(n) \wedge f' \text{ surjective}$$

This contradicts $\psi(n)$. $\lightning$

$$\begin{aligned} &\underline{f(\mathrm{suc}(n)) \neq \mathrm{suc}(\mathrm{suc}(n))} \\ &\quad \implies \exists a, b \,:\, f = f' \cup \{(a, \mathrm{suc}(\mathrm{suc}(n))), (\mathrm{suc}(n), b)\} \\ &\quad \implies f' \cup \{(a,b)\} : n \to \mathrm{suc}(n) \wedge f' \text{ surjective} \end{aligned}$$

This also contradicts $\psi(n)$. $\lightning$. ∎

Theorem 3.90. If $f : A \to A$ and A is finite, then f is injective iff and only if f is surjective.

$$(f : A \to A \wedge A \text{ is finite}) \implies (f \text{ is injective} \iff f \text{ is surjective}).$$

Proof of $\implies$. Assume A finite and $f : A \to A$ and towards a contradiction suppose f is injective and *not* surjective. By definition A is D-infinite and therefore P-infinite. $\lightning$. ∎

Proof of $\impliedby$. Let

$$\psi(n) \iff A \approx n \wedge \forall f \,(f \text{ surjective} \implies f \text{ injective})$$

and proceed with induction.
Base: The only function on $\varnothing \times \varnothing$ is both injective and surjective. Thereby $\psi(0)$.
Induction hypothesis: $A \approx n \wedge \forall f \,(f \text{ surjective} \implies f \text{ injective})$.

Towards a contradiction assume

$$A \approx \mathrm{suc}(n) \wedge f \text{ surjective } \wedge f \text{ not injective.}$$

which implies $\exists a \neq b \,:\, f(a) = f(b)$.

Consider $g : A \setminus \{b\} \to A$ given by

$$g = f|A \setminus \{b\} = \{(a, f(a)) \,:\, a \in A \setminus \{b\}\}.$$

This function g defines a surjective function satisfying

$$g : A \setminus \{b\} \approx n \to A \approx \mathrm{suc}(n)$$

which itself gives another surjective function

$$g' : n \to \mathrm{suc}(n)$$

contradicting Theorem 3.89. ■

Theorem 3.91. A is finite $\implies \mathcal{P}(A)$ is finite.

Theorem 3.92. (A is finite $\wedge$ B is finite) $\implies {}^{B}A$ is finite.

Proof. A, B is finite $\implies$ $B \times A$ is finite by 3.80 and thus $\mathcal{P}(B \times A)$ is finite by 3.91. Notice $f \in {}^{B}A \implies f : B \to A \implies f \subseteq B \times A \implies f \in \mathcal{P}(B \times A)$ and thereby ${}^{B}A \subseteq \mathcal{P}(B \times A)$ is finite. ■

Theorem 3.93. A is finite $\implies f[A]$ is finite.

Theorem 3.94. A is D-infinite $\iff \omega \preccurlyeq A$.

Proof of $\implies$. Assume A is D-infinite. We have then,

$$\exists f\ (f : A \to A \text{ injective and } \textit{not} \text{ onto})$$

which means $\exists a \in A : a \notin \operatorname{rng}(f)$.

By Recursion Theorem, second form, there is *unique* $h : w \to A$ satisfying

$$\begin{aligned} h(0) &= 0 \\ h(\operatorname{suc}(n)) &= G(h(n), n) = f(h(n)). \end{aligned}$$

Thus we have shown there is a function $h : \omega \to A$; it remains to show h is injective.

Claim. h is injective.

Let $\psi(n) \iff h[n] \approx n$.

Base: $\psi(0) \iff h[\varnothing] \approx \varnothing \iff \varnothing \approx \varnothing$.

Towards a contradiction suppose it is *not* the case that $h[\operatorname{suc}(n)] \approx \operatorname{suc}(n)$ then there is $\ell, m : \ell < m \wedge h(\ell) = h(m)$. Let $\ell = \operatorname{suc}(k)$ and $m = \operatorname{suc}(p)$ and notice

$$h(\ell) = h(\operatorname{suc}(k)) = f(h(k)) \quad \text{and} \quad h(m) = h(\operatorname{suc}(p)) = f(h(p)).$$

so $f(h(k)) = f(h(p)) \implies h(k) = h(p)$ because f is injective.

We have $0 < k < p \leq \operatorname{suc}(n)$ because $h(0) = a \notin \operatorname{rng}(f)$ and p, $k < \operatorname{suc}(n)$. It follows that there is an *injection* $h : \omega \to A$. This contradicts the induction hypothesis $\psi(n)$ and proves h is injective.

It follows that there is injective $h : \omega \to A \implies \omega \preccurlyeq A$. ■

$\Longleftarrow$. Assume $\omega \preccurlyeq A$ (and show A is D-infinite).
Let $\omega \preccurlyeq A \implies \exists f : \omega \approx_f B \wedge B \subseteq A \wedge f$ bijectivel Define

$$g(x) \begin{cases} x & x \in A \setminus B \\ f(\mathrm{suc}(\check{f}(x))) & x \in B \end{cases}.$$

Then g is injective since f is a bijection. But g is *not surjective* because $\neg\exists x \in B : \mathrm{suc}(\check{f}(x)) = 0$. Thereby $f(0) \notin \mathrm{rng}(g)$ with $f(0) \in B$. The result follows. ∎

Theorem 3.95. $(A$ is D-infinite $\wedge\ A \preccurlyeq B) \implies B$ is D-infinite.

Proof. By 3.36, 3.61, 3.94, respectively, $\omega \preccurlyeq A$, ωB, and B is D-finite. ∎

Theorem 3.96. $(A$ is D-finite $\wedge\ B \preccurlyeq A) \implies B$ is D-finite.

Proof. Assume B is B is D-infinite, by 3.95 A is D-infinite. ↯ ∎

It would be natural, at this point, to prove that a set A is infinite if and only if A is Dedekind-infinite. But to show that if A is infinite, then A is Dedekind-infinite requires a new Axiom, the *Axiom of Choice*, to which we return later.

Theorem 3.97. A is infinite $\implies \mathcal{P}(\mathcal{P}(A))$ is D-infinite.

3.5 Partial Orders and Upper Bounds

We introduce some terminology that will be useful for us, both for dealing with natural numbers and more generally:

Definition 3.98 (Supremum and Infimum)**.** Let R be a *partial order* or a *strict partial order*. Let $B \neq \varnothing$.

R-***upper bound*** of B

$$z \in \mathrm{UB}_R(B) \iff \forall y\,(y \in B \implies (yRz \vee y = z)).$$

R-***supremum*** (or equivalently R-least upper bound) of B

$$x = \sup_R(B) \iff x \in \mathrm{UB}_R(B) \wedge (y \in \mathrm{UB}_R(B) \implies xRy \vee x = y)$$

R-***greatest*** (or equivalently R-largest or R-last) element of B

$$x = \max_R(B) \iff x \in B \wedge \forall y\,(y \in B \implies [yRx \vee y = x]).$$

*R-**lower bound*** of B

$$x \in \text{LB}_R(B) \iff x \in \text{LB}_{\check{R}}(B)$$

*R-**infimum*** (or equivalently R-greatest lower bound) of B

$$x = \inf_R(B) \iff x = \sup_{\check{R}}(B)$$

Theorem 3.99. Let R be a partial or a strict partial order.

$$x = \max_R(B) \implies x = \sup_R(B)$$

Proof.

$$\begin{aligned} x = \max_R(B) &\implies x \in B \wedge (z \in B \implies z \preccurlyeq x) \\ &\implies x \in \text{UB}_R(B) \wedge (z \in B \implies z \preccurlyeq x) \\ &\implies x = \sup_R(B). \end{aligned}$$

■

Theorem 3.100. Let $B \subseteq \omega$ and $B \neq \varnothing$. B has an $<_\omega$-upper bound if and only if B is finite.

$\implies$. Assume $B \subseteq \omega \wedge B \neq \varnothing \wedge \exists m \in \text{UB}{<_\omega}(B)$.

$$\begin{aligned} k \in B &\implies k <_\omega m \vee k = m \\ &\implies k \in m \vee k = m \\ &\implies k \in \text{suc}(m) \end{aligned}$$

Thereby $B \subseteq \text{suc}(m) \implies B$ is finite by 3.70. ■

$\impliedby$. By the PMI with

$$\psi(n) \iff (B \approx n \implies \exists m \in \text{UB}_{<_\omega}(B)).$$

For the base notice $\psi(0) \iff (B \approx 0 \implies \exists m \in \text{UB}_{<_\omega}(B) \iff \top)$.

Let $x \in B \implies \exists m \in \text{UB}_{<_\omega}(n)$ by $\psi(n)$. Thus $\max(x, m) \in \text{UB}_{<_\omega}(B)$

■

Theorem 3.101. Let $B \subseteq \omega$ and $B \neq \varnothing$. B has no $<_\omega$-upper bound if and only if $B \approx \omega$. That is,

$$\text{UB}_{<_\omega}(B) = \varnothing \iff B \approx \omega.$$

$\Longrightarrow$. Assume $B \approx \omega$ and, towards a contradiction, $\exists k \in \text{UB}_{<_\omega}(B)$.

$$\begin{aligned}(y \in B \implies (y <_\omega k \vee y = k)) \\ \implies (y \in B \implies y \in k \vee y = k) \\ \implies B \subseteq k \cup \{k\} = \text{suc}(k) \\ \implies B \text{ is finite} \wedge B \approx \omega \lightning\end{aligned}$$

$\Longleftarrow$. Assume $B \subseteq \omega \wedge B \neq \varnothing \wedge \text{UB}_{<_\omega}(B) = \varnothing$.

For $R \subseteq \omega \times \omega$ let

$$H(R) = \begin{cases} \max_{<_\omega}(B \setminus \text{rng}(R)) & \text{if } B \setminus \text{rng}(R) \neq \varnothing \\ 0 \end{cases}$$

Recursion Theorem First Form gives unique $h : \omega \to B$ such that

$$h(n) = H(h[n]) = \min_{<_\omega}(B \setminus h[n]).$$

B is infinite by **??** and $h[n]$ is finite $\implies B \setminus h[n] \neq \varnothing$.

Towards a contradiction assume h is *not* onto. This implies $B \setminus \text{rng}(h) \neq \varnothing$ so let

$$\begin{aligned} m &= \min_{<_\omega}(B \setminus \text{rng}(h)), \text{ and} \\ n &= \min_{<_\omega}(n : m < h(n)). \end{aligned}$$

We have $k < n \implies \neg(m < h(k)) \implies h(k) < m \vee m = h(k) \implies h(k) < m \vee \bot \implies m = h(k)$.

So we have

$$\min_{<_\omega}(B \setminus \text{rng}(h[n])) = m = h(n)$$

which gives $h(n) = m \wedge m < h(n)$ $\lightning$ Thus $h(n)$ is *onto*.

It is left as an exercise to show h is injective.

We conclude that h is an bijection from $\omega \to B$ which means $\omega \approx B$ as desired.

From 3.100 and 3.101, if follows immediately that

Theorem 3.102. $B \subseteq \omega \implies (B \text{ is finite} \vee B \approx \omega)$.

3.6 Countable Sets

The simplest infinite set, in a certain sense, is ω, the set of all natural numbers. We call a set "*denumerable*" if it is equipotent to ω.

Definition 3.103. A is denumerable $\iff A \approx \omega$.

Closely related to the idea of being denumerable are the two ideas of being "countable and "uncountable."

Definition 3.104 (Countable)**.** C is *countable* when

$$C \text{ is finite} \vee C \text{ is denumerable}$$

and *uncountable* otherwise.

Theorem 3.105. A is finite $\iff A \prec \omega$.

$\implies$. A is finite $\implies \exists n : A \approx n$. Since $n \preccurlyeq \omega$ this implies $A \preccurlyeq \omega$. Suppose $\omega \preccurlyeq A \implies \omega$ is finite by 3.72 $\lightning$.

Thus $\neg(\omega \preccurlyeq A) \implies A \prec \omega$. ∎

$\impliedby$. Assume $A \prec \omega \implies A \preccurlyeq \omega \implies \exists B \subseteq \omega : A \approx B$. By 3.102, B finite or $B \approx \omega$.

If B finite there is nothing to prove so suppose $B \approx \omega$:

$$B \approx \omega \wedge A \approx B \implies w \approx A \implies \omega \preccurlyeq A.$$

However, by assumption, $A \prec \omega \implies \neg(w \preccurlyeq A)$ $\lightning$.

Thus B-finite $\implies A$ finite. ∎

We would like to use this theorem, and 3.103 to show that A is countable if and only if $A \preccurlyeq \omega$. One direction is easy to prove:

Theorem 3.106. A is countable $\implies A \preccurlyeq \omega$.

Proof. A is countable $\implies A$ is finite $\vee$ A is denumerable $\implies \exists n \in \omega : A \approx n \vee A \approx \omega \implies \exists n \subseteq \omega : A \approx n \vee \exists w \subseteq w : A \approx \omega \implies A \preccurlyeq \omega$. ∎

But the other direction involves a difficulty: One step requires that, from $A \preccurlyeq \omega$ and $\omega \preccurlyeq A$ we show $A \approx \omega$. But similar problems will arise elsewhere, and so we wish to prove that

$$A \preccurlyeq B \wedge B \preccurlyeq A \implies A \approx B.$$

This is known as the *Cantor-Berstein Theorem*, and we now prepare to prove it.

A very useful tool in proving the Cantor-Bernstein Theorem is what is called the *Fixed-Point Theorem for Monotonic Functions*. We first need a couple of definitions:

Definition 3.107 (Fixed Point)**.**

$$y \text{ is a fixed point of } f \iff y = f(y).$$

Definition 3.108 (Monotonic)**.** Let $F : \mathcal{P}(A) \to \mathcal{P}(A)$. Then F is *monotonic* if and only if

$$\forall X \subseteq A \, \forall Y \subseteq A \, (X \subseteq Y \implies F(X) \subseteq F(Y)).$$

Theorem 3.109 (Fixed-Point Theorem on Monotonic Functions)**.**

$$F : \mathcal{P}(A) \to \mathcal{P}(A) \text{ is monotonic} \implies \exists x \, (x \text{ is a fixed point of } F).$$

Proof by magic. Let $E = \{B \subseteq A : B \subseteq F(B)\}$ so that

1. $x \in \bigcup E \implies \exists y \in E : x \in y$,
2. $y \subseteq \bigcup E \implies F(y) \subseteq F(\bigcup E)$,
3. $y \in E \implies y \subseteq F(y)$.

Thereby

$$(x \in y \wedge y \subseteq F(y) \wedge F(y) \subseteq F(\bigcup E)) \implies x \in F(\bigcup E)$$

and $x \in \bigcup E \implies x \in F(\bigcup E)) \implies \bigcup E \subseteq F(\bigcup E)$.

Notice

$$\begin{aligned} &\bigcup E \subseteq F(\bigcup E) \\ &\quad \implies F(\bigcup E) \subseteq F(F(\bigcup E)) \\ &\quad \implies F(\bigcup E) \in E \\ &\quad \implies F(\bigcup E) \subseteq \bigcup E \end{aligned}$$

and thereby $F(\bigcup E) \subseteq \bigcup E \wedge \bigcup E \subseteq F(\bigcup E) \implies F(\bigcup E) = \bigcup E \implies \bigcup E$ is a fixed point of F. ∎

We then prove a special case of Cantor-Bernstein Theorem:

Theorem 3.110. $(C \subseteq B \wedge B \subseteq A \wedge A \approx C) \implies (A \approx B)$.

Theorem 3.111 (Cantor-Bernstein)**.**

$$A \preccurlyeq B \land B \preccurlyeq A \implies A \approx B.$$

Proof. Notice, by definition,

$$\begin{aligned} A \preccurlyeq B &\implies \exists f : A \to B \text{ injective} \\ B \preccurlyeq A &\implies \exists g : B \to A \text{ injective} . \end{aligned}$$

and let

$$\begin{aligned} \Phi : \mathcal{P}(A) &\to \mathcal{P}(A) \\ x &\mapsto g[B \setminus f[A \setminus x]]. \end{aligned}$$

Claim. Φ is monotonic.

Notice

$$\begin{aligned} x \subseteq y &\implies A \setminus y \subseteq A \setminus x \\ &\implies f[A \setminus y] \subseteq f[A \setminus x] \\ &\implies g[B \setminus f[A \setminus x]] \subseteq g[B \setminus f[A \setminus y]] \end{aligned}$$

so we have $x \subseteq y \implies \Phi(x) \subseteq \Phi(y)$ and thereby Φ is monotonic $\implies \exists x : \Phi(x) = x$. $\square$

Notice

$$\begin{aligned} A &= x \cup (A \setminus x) \\ B &= (B \setminus f[A \setminus x]) \cup f[A \setminus x] \end{aligned}$$

We can use g to "induce a bijection" by defining a function from g *onto* $\operatorname{rng}(g)$.

$$g' : (B \setminus f[A \setminus x]) \to g[B \setminus f[A \setminus X]] = \Phi(x) = x.$$

This function g' is a *bijection* because it is both *injective* and *surjective*.

The same can be done with f:

$$f' : A \setminus x \to f[A \setminus x]$$

Where f injective $\implies$ f' bijective as above.

Thus we have

$$g' : B \setminus f[A \setminus x] \to x$$

$$\breve{g}' : x \to B \setminus f[A \setminus x]$$
$$f' : A \setminus x \to f[A \setminus x]$$

so $f' \cup \breve{g}' : A \setminus x \cup \{x\} \to B \setminus B \setminus f[A \setminus x] \cup f[A \setminus x]$. Since f' and g' are bijective on disjoint sets $f' \cup \breve{g}'$ is also a bijection (prove it!). In particular

$$h(y) = \begin{cases} \breve{g}'(y) & y \in x \\ f(x) & y \notin x \end{cases}.$$

Thus we have a bijection $h : \omega A \to B$ giving $A \approx B$. ∎

Theorem 3.112. A is countable $\iff A \preccurlyeq \omega$.

Theorem 3.113.

$$(A \text{ is countable} \wedge B \subseteq A) \implies B \text{ is countable.}$$

Theorem 3.114.

$$(\{0\} \times \omega) \cup (\{1\} \times \omega) \approx \omega.$$

Theorem 3.115.

$$(A \text{ is countable} \wedge B \text{ is countable}) \implies A \cup B \text{ is countable.}$$

Theorem 3.116. $\mathbb{Z}$ is denumerable.

Theorem 3.117. $\omega \times \omega$ is denumerable

Theorem 3.118. A is countable $\implies {}^n A$ is countable.

We now wish to consider $\text{seq}(A)$, the set of all finite sequences on a set A:

Definition 3.119 (Sequence).

$$\text{seq}(A) := \bigcup {}^n A : n \in \omega.$$

Theorem 3.120. A is countable $\implies \text{seq}(A)$ is countable.

We would like to prove at this point that the union of a countable set of countable sets is countable. But the proof of this theorem requires the Axiom of Choice, to which we later return.

3.7 Uncountable Sets

Our first task is to show that there exists an uncountable set:

Theorem 3.121. ${}^{\omega}2$ is uncountable.

This set ${}^{\omega}2$ is closely connected with an idea useful in analysis and in computer science, the "*characteristic function*" of a set y with respect to a set A.

Theorem 3.122 (Characteristic Function)**.** Let $A \neq \varnothing$ and $y \subseteq A$. Then $\chi_y^A : A \to \{0,1\}$ is the unique function such that $\chi_y^A(z) = 1$ is $z \in y$, and $\chi_y^A(z) = 0$ if $z \notin y$. Then function χ_y^A is called the *characteristic function* of y with respect to A.

If A is clear from context, we write χ_y instead.

Theorem 3.123. ${}^{A}2 \approx \mathcal{P}(A)$.

Theorem 3.124 (Cantor's Theorem)**.** $A \prec \mathcal{P}(A)$.

Theorem 3.125. $\neg\exists A\,(\mathcal{P}(A) \approx \omega)$.

Theorem 3.126.

$$(A \text{ is uncountable} \wedge A \subseteq B) \implies B \text{ is uncountable.}$$

Theorem 3.127.

$$(2 \preccurlyeq A \wedge \omega \preccurlyeq B) \implies {}^{B}A \text{ is uncountable.}$$

4 Cardinal Numbers

Before proceeding further, we wish to introduce the idea of *cardinal number*. So far, we have introduced the idea of $A \approx B$, that is, of the sets A and B being *equipotent*, which many authors write as "having the same cardinal number".

We wish to introduce what we call the *Cardinal Axiom*.

Axiom 7 (Cardinal Axiom). For every A there is a set $|A|$, called the *cardinal number* of A, and for every B and C, $|B| = |C|$ if and only if $B \approx C$.

Once we have introduced the Axiom of Choice, we will be able to *prove* this cardinal axiom from it. So the Cardinal Axiom is only a temporary assumption, but a useful one.

In particular, we require $|A|$ to satisfy the following definition.

Definition 4.1.

1. $\forall n \in \omega;\ |n| = n$,
2. $|\omega| = \omega$,
3. $2^\omega = |{}^\omega 2|$.

Notice only condition (3) defines something new, namely 2^ω, and when we introduce cardinal exponentiation, we will have to check that condition (3) is satisfied.

The be sure that conditions (1), (2), and (3) cause no problems, we need the following (easy) theorem:

Theorem 4.2.

1. $m \approx n \implies m = n$,
2. $\neg(n \approx \omega)$,

3. $\neg(n \approx {}^{\omega}2) \wedge \neg(w \approx {}^{\omega}2)$

Proof of 1. By the Cardinal Axiom and Definition 4.1.1 we have

$$m \approx n \implies |m| = |n| \implies m = n.$$

■

Proof of 2. By the Cardinal Axiom and Definition 4.1.2 we have

$$n \approx \omega \implies |n| = |\omega| \implies n = \omega. \lightning$$

■

Proof of 3. Exercise. ■

4.1 Cardinal Arithmetic

From now on, we let κ, λ, and μ (kappa, lambda, and mu), with or without subscripts, stand for cardinal numbers.

We wish to define addition on cardinal numbers. To do so, we need the following preliminary theorem:

Theorem 4.3.

1. $\forall\kappa\,\forall\lambda\,\exists A\,\exists B : \kappa = |A| \wedge \lambda = |B| \wedge A \cap B = \varnothing$,
2. $\forall\kappa\,\forall\lambda\,\exists!\mu\,\exists A\,\exists B : \kappa = |A| \wedge \lambda = |B| \wedge A \cap B = \varnothing \wedge \mu = |A \cup B|$.

Proof of 1. By the Cardinal axiom there is A' and B' such that $\kappa = |A'|$ and $\lambda = |B'|$. Let $A = A' \times \{0\}$ and $B = B' \times \{1\}$ so that clearly $A \cap B = \varnothing$. Since $A' \approx A$ and $B' \approx B$ the result follows. ■

Definition 4.4. $k + \lambda$ is the unique μ given by Theorem 4.3.2.

Theorem 4.5.

1. $\kappa + \lambda = \lambda + \kappa$,
2. $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$,
3. $\kappa + 0 = \kappa$.

Proof. By the cardinal axiom there is A, B, C such that $A \cap B = A \cap C = B \cap C = \varnothing$ and $\kappa = |A|$, $\lambda = |B|$, and $\mu = |C|$.

1. $\kappa + \gamma = |A| + |B| = |A \cup B| = |B \cup A| = |B| + |A| = \lambda + \kappa$.

2. $\kappa + (\lambda + \mu) = |A| + (|B| + |C|) = |A| + |B \cup C| = |A \cup (B \cup C)| = |(A \cup B) \cup C| = (\kappa + \lambda) + |C| = (\kappa + \lambda) + \mu$.

3. $\kappa + 0 = |A| + |\varnothing| = |A \cup \varnothing| = |A| = \kappa$. ∎

Theorem 4.6.

1. A is D-infinite $\implies n + |A| = |A|$,

2. $\omega + \omega = \omega$.

Proof of 1. Without loss of generality assume $n \cap A = \varnothing$. As $n + |A| = |n| + |A| = |n \cup A|$ it suffices to show $n \cup A \approx A$.

For fixed A, let $\psi(n) \iff n \cup A \approx A$ and notice

$$\psi(0) \iff \varnothing \cup A \approx A \iff A \approx A \iff \top.$$

Suppose $\psi(n)$ and note A is D-infinite. This means we have

$$\begin{aligned} f &: A \to A && f \text{ injective not surjective,} \\ g &: n \cup A \to A && g \text{ bijective,} \end{aligned}$$

and $\exists a \in A \setminus \operatorname{rng}(f)$. Consider $h : n \cup A \to A$ given by

$$h = f \circ g \cup \{(\{n\}, a)\}.$$

It is easily shown h is injective and thus $n \cup \{n\} \cup A = \operatorname{suc}(n) \cup A \preccurlyeq A$. As clearly $A \preccurlyeq n \cup A$ we have by Cantor-Bernstein that $\operatorname{suc}(n) \cup A \approx A$.

The result follows from the PMI. ∎

Proof of 2. $\omega + \omega = |\omega| + |\omega| = |\omega \times \{0\}| + |\omega \times \{1\}| = |\omega \times \{0\} \cup \omega \times \{1\}|$. Then it suffices to show that $\omega \times \{0\} \cup \omega \times \{1\} \approx \omega$. This follows from **??** but one could also prove

$$\begin{aligned} h \;:\; \omega \times \{0\} \cup \omega \times \{1\} &\to \omega \\ (x, y) &\mapsto 2x + y \end{aligned}$$

is a bijection. ∎

When we consider $m + n$, we might mean $m + n$ as defined on natural numbers at 3.32, or we might mean $m + n$ as the sum of two cardinals as defined at 4.4. So whenever we mean $m + n$ as the sum of two cardinals, we will write $m +_c n$ with a subscript c on the plus sign.

However, our next theorem shows that, for m and n, these two definitions of addition agree:

Theorem 4.7. $m +_c n = m + n$.

Proof. Notice:

$$\begin{aligned} m +_c n = m + n & \\ &\iff |m \times \{0\} \cup n \times \{1\}| = |m + n| \\ &\iff m \times \{0\} \cup n \times \{1\} \approx m + n. \end{aligned}$$

So we proceed by proving, using the PMI, that

$$\psi(n) \iff m \times \{0\} \cup n \times 1 \approx m + n.$$

The base case is valid because

$$\begin{aligned} \psi(0) &\iff m \times \{0\} \cup \varnothing \times \{1\} \approx m + 0 \\ &\iff m \times \{0\} \approx m \\ &\iff \top. \end{aligned}$$

and, assuming $\psi(n)$, we have

$$\begin{aligned} m \times \{0\} \cup n \times \{1\} \approx m + n & \\ &\implies m \times \{0\} \cup n \times \{1\} \cup \{(\{n\}, 1)\} \approx m + n \cup \{m + n\} \\ &\implies m \times \{0\} \cup \mathrm{suc}(n) \times 1 \approx \mathrm{suc}(m + n) \\ &\implies m \times \{0\} \cup \mathrm{suc}(n) \times 1 \approx m + \mathrm{suc}(n). \end{aligned}$$

The result follows. ∎

We now introduce cardinal multiplication, after first showing the preliminary theorem needed to justify the definition of cardinal multiplication:

Theorem 4.8. $\forall \kappa \, \forall \lambda \, \exists! \mu \, \exists A \, \exists B \, : \, \kappa = |A| \wedge \lambda = |B| \wedge \mu = |A \times B|$.

Definition 4.9. $\kappa\lambda$ is the unique μ given by 4.8. We also write $\kappa \cdot \lambda$.

Theorem 4.10.

1. $\kappa\lambda = \lambda\kappa$,
2. $\kappa(\lambda\mu) = (\kappa\lambda)\mu$,
3. $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$,
4. $\kappa \cdot 1 = \kappa$.

Proof. By the cardinal axiom there is A, B, C such that $A \cap B = A \cap C = B \cap C = \varnothing$ and $\kappa = |A|$, $\lambda = |B|$, and $\mu = |C|$.

1. $\kappa\lambda = |A \times B| = |B \times A| = \lambda\kappa$.

2. $\kappa(\lambda\mu) = |A| \cdot |B \times C| = |A \times (B \times C)| = |(A \times B) \times C| = |A \times B| \cdot |C| = (\kappa\gamma)\mu$.

3. $\kappa(\lambda + \mu) = |A| \cdot |B \cup C| = |A \times (B \cup C)| = |A \times B \cup A \times C| = |A \times B| + |A \times C| = \kappa\lambda + \kappa\mu$.

4. $\kappa \cdot 1 = \kappa \cdot |\{\varnothing\}| = |\kappa \times \{\varnothing\}| = |\kappa| = \kappa$. ∎

Theorem 4.11. $\omega \cdot \omega = \omega$.

Proof. Notice $\omega \times \omega \approx \omega \implies |\omega \times \omega| = |\omega| \implies \omega \cdot \omega = \omega$ so we need only prove $\omega \times \omega \approx \omega$.

It is obvious $\omega \preccurlyeq \omega \times \omega$ so let us show $\omega \times \omega \preccurlyeq \omega$. To that end consider

$$\begin{aligned} h : \omega \times \omega &\to \omega \\ (n, m) &\mapsto p^n q^m. \end{aligned}$$

This is an injection (requires the Fundamental Theorem of Algebra) and thus $\omega \times \omega \preccurlyeq \omega$. ∎

As with addition, we multiply m and n, we may mean mn as defined by recursion on natural numbers at 3.35, or we may mean $m \cdot n$ as the product of two cardinals defined at 4.9. In the latter case, we write $m \cdot_c n$ with a subscript c (for cardinal) on the multiplication sing.

We now show that these two definitions of multiplication agree on m and n:

Theorem 4.12. $m \cdot_c n = mn$.

Proof. Let

$$\psi(n) \iff m \cdot_c n = mn$$

clearly $\psi(0) \iff m \cdot_c 0 = n0 \iff 0 = 0 \iff \top$. Moreover

$$\begin{aligned} m \cdot_c \operatorname{suc}(n) &= |m \times \operatorname{suc}(n)| \\ &= |m \times n \cup m \times \{n\}| \\ &= m \cdot_c n + m \cdot_c 1 \\ &= m \cdot_c n + m \\ &= mn + m && \text{by } \psi(n). \end{aligned}$$

and therefore $\psi(\mathrm{suc}(n))$. The result follows from the PMI. ∎

Finally, we introduce exponentiation or cardinal numbers, after the usual preliminary theorem:

Theorem 4.13. $\forall\kappa\,\forall\lambda\,\exists!\mu\,\exists A\,\exists B\,:\,\kappa = |A| \wedge \lambda = |B| \wedge \mu = \left|{}^{B}A\right|$.

Definition 4.14. κ^{λ} is the unique μ given by 4.13, with the proviso that $\mu = 2^{\omega}$ if $\kappa = 2$ and $\lambda = \omega$.

(This last proviso is inserted because 4.1.3.)

Theorem 4.15.

1. $\kappa^0 = 1$,
2. $\kappa^1 = \kappa$,
3. $1^{\kappa} = 1$.

Proof. By the cardinal axiom there is A such that $\kappa = |A|$.

1. $\kappa^0 = |{}^{\varnothing}A| = |\,\{\varnothing\}\,| = |\,\mathrm{suc}(\varnothing)\,| = 1$.
2. $\kappa^1 = |{}^{\mathrm{suc}(0)}A| = |{}^{\{\varnothing\}}A| = |A| = \kappa$.
3. $1^{\kappa} = |{}^{A}\mathrm{suc}(0)| = |{}^{A}\{\varnothing\}| = |\,\{(a,\{\varnothing\})\,:\,a \in A\}\,| = 1$

∎

As with addition and multiplication, we need to distinguish between m^n, the exponentiation on natural numbers, defined at 3.38, and $(m^n)_c$, the exponentiation on natural numbers defined at 4.14. We now show that these two definitions of exponentiation agree for m and n:

Theorem 4.16. $(m^n)_c = m^n$.

Proof. Let

$$\psi(n) \iff (m^n)_c = m^n$$

and note $\psi(0) \iff (m^0)_c = m^0 \iff 1 = 1 \iff \top$.

Now consider (note, we take for granted ${}^{\mathrm{suc}(n)}m =^n m \times^{\{n\}} m$ as this is a special case of 4.17)

$$\begin{aligned}(m^{\mathrm{suc}(n)})_c &= |{}^{\mathrm{suc}(n)}m| \\ &= |{}^{n}m \times^{\{n\}} m| \\ &= |{}^{n}m| \cdot |{}^{\{n\}}m| \\ &= |{}^{n}m| \cdot |m| \\ &= m^n m\end{aligned}$$

$$= m^{n+1}$$

The result follows from PMI. ∎

The next three theorems are needed to prove general laws on cardinal exponentiation.

Theorem 4.17. Suppose $A \cap B = \varnothing$. Then

$$^{A\cup B}C \approx {}^{A}C \times {}^{B}C.$$

Proof $\preccurlyeq$. We show $^{A\cup B}C \preccurlyeq {}^{A}C \times {}^{B}C$.

$$f \in {}^{A\cup B}C \preccurlyeq {}^{A}C \implies f : A \cup B \to C$$

Thus f can be decomposed into two functions $g : A \to C$ and $h : B \to C$ given by

$$g = f \cap A \times C$$
$$h = f \cap B \times C$$

and thus $^{A\cup B}C \preccurlyeq {}^{A}C \times {}^{B}C$ ∎

Proof $\succcurlyeq$. We show $^{A}C \times {}^{B}C \preccurlyeq {}^{A\cup B}C$.

$$(g,h) \in {}^{A}C \times {}^{B}C \implies g : A \to C \wedge h : B \to C.$$

Thus we can identify any (g,h) with $g \cup h = f \in {}^{A\cup B}C$. It follows $^{A}C \times {}^{B}C \preccurlyeq {}^{A\cup B}C$.

Cantor-Berstein gives $^{A\cup B}C \approx {}^{A}C \times {}^{B}C$. ∎

Theorem 4.18. $^{C}(A \times B) \approx {}^{C}A \times {}^{C}B$.

Proof. We have $f \in {}^{C}(A \times B) \implies f : C \to A \times B$ and it is easy to see we can identify this f with $(g,h) \in {}^{C}A \times {}^{C}B$ (and vice verse) using

$$f \mapsto (f \cap C \times A, f \cap C \times B).$$

We thus have $^{C}(A \times B) \preccurlyeq {}^{C}A \times {}^{C}B$ and $^{C}(A \times B) \succcurlyeq {}^{C}A \times {}^{C}B$. By Cantor-Bernstein $^{C}(A \times B) \approx {}^{C}A \times {}^{C}B$. ∎

Theorem 4.19. $^{C}(^{B}A) \approx {}^{B\times C}A$.

Proof. Assignment 4. ∎

Theorem 4.20.

1. $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$,
2. $(\kappa\lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$,
3. $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$.

Proof. By the cardinal axiom there is A, B, C such that $A \cap B = A \cap C = B \cap C = \varnothing$ and $\kappa = |A|$, $\lambda = |B|$, and $\mu = |C|$.

1. $\kappa^{\lambda+\mu} = |A|^{|B \cup C|} = |{}^{B\cup C}A| = |{}^B A \times {}^C A| = \kappa^\lambda \cdot \kappa^\mu$,
2. $(\kappa\lambda)^\mu = |{}^C(A \times B)| = |{}^C A| \cdot |{}^C B| = \kappa^\mu \cdot \lambda^\mu$, and
3. Assignment 4. ∎

We call the cardinal number 2^ω *the power of the continuum* since, as we will see a little later, it is the cardinal number of the set of all real numbers.

Definition 4.21. 2^ω is the power of the continuum.

Then we establish some basic properties of the power of the continuum.

Theorem 4.22. $2^\omega = 2^\omega + 2^\omega = 2^\omega \cdot 2^\omega = (2^\omega)^\omega$.

Proof. Bounty. ∎

4.2 Rational Numbers

In section **??**, we extend ω to obtain our *integers* $\mathbb{Z}$, where we defined $-n$ as $(0, n)$ for all $n > 0$. We then defined $<_\mathbb{Z}$ by extending $<_\omega$ and showed that $<_\mathbb{Z}$ is a strict order.

Now we wish to extend $\mathbb{Z}$ to get what we will use as $\mathbb{Q}$, the set of all rational numbers. There are many ways to do so, but all of them result in isomorphic structures. We shall only concern ourselves with extending $<_\mathbb{Z}$ to get a strict order on $\mathbb{Q}$, and shall not take the time to extend addition and multiplication to $\mathbb{Q}$.

Definition 4.23 (Proper Fractions)**.** Let $\mathcal{F}$ denote the set of proper fractions.

$$\mathcal{F} := \{(a, b) : b \in \omega \setminus \{0, 1\} \wedge a \in \mathbb{Z} \setminus \{0\}\}.$$

Theorem 4.24. $\mathbb{Z} \cap \mathcal{F} = \varnothing$.

Proof. Exercise (easy). ∎

We now define the set of $\mathbb{Q}$ of all *rational numbers* as the union of these two sets.

Definition 4.25. $\mathbb{Q} := \mathbb{Z} \cup \mathcal{F}$.

If $(a, b) \in \mathcal{F}$, we could defined $\frac{a}{b}$ to be (a, b), but we do not do so since we will have no need for division.

Next we extend $<_{\mathbb{Z}}$, our strict oder on $\mathbb{Z}$, to $\mathbb{Q}$:

Definition 4.26.

$$\begin{aligned} <_{\mathbb{Q}} := <_{\mathbb{Z}} &\cup \{(a,(b,c)) \,:\, a \in \mathbb{Z} \wedge (b,c) \in \mathbb{Q} \setminus \mathbb{Z} \wedge ac <_{\mathbb{Z}} b\} \\ &\cup \{((b,c),a) \,:\, a \in \mathbb{Z} \wedge (b,c) \in \mathbb{Q} \setminus \mathbb{Z} \wedge b <_{\mathbb{Z}} ac\} \\ &\cup \{((b,c),(b',c')) \,:\, (b,c),(b',c') \in \mathbb{Q} \setminus \mathbb{Z} \wedge bc' <_{\mathbb{Z}} b'c\}. \end{aligned}$$

Theorem 4.27. $<_{\mathbb{Q}}$ is a strict order with no least and no greatest element.

Proof. Exercise. ∎

Theorem 4.28. $\mathbb{Q}$ is denumerable.

Proof. $\mathbb{Q}$ and $\omega \times \omega$ are equipotent via the *bijection*

$$f : \mathbb{Q} \to \omega \times \omega$$

given by

$$f(a) = \begin{cases} (a_0, a_1) & a = (a_0, a_1) \in \mathcal{F} \\ (a, 0) & a \in \mathbb{Z}^{-1} \\ (a, 1) & a \in \mathbb{N}. \end{cases}$$

So $\mathbb{Q} \approx \omega \times \omega$ and since $\omega \times \omega \approx \omega$ we have $\mathbb{Q} \approx \omega$ and thereby $\mathbb{Q}$ is denumerable by defintion. ∎

We wish to characterize $<_{\mathbb{Q}}$ as an ordering:

Definition 4.29 (Dense)**.** Let R be a strict order. R is *dense if and only if*

$$\forall x \forall y \, (xRy \implies \exists z \,:\, xRz \wedge zRy) \wedge |\operatorname{fld}(R)| \geq 2.$$

Theorem 4.30. $<_{\mathbb{Q}}$ is dense.

Proof. Let $a = (a_0, a_1), b = (b_0, b_1) \in \mathbb{Q}$ such that $(a_0, a_1) <_{\mathbb{Q}} (b_0, b_1)$ and $a, b > 0$. Thus we have $a_0 b_1 < b_0 a_1$ (i.e. $\frac{a_0}{a_1} < \frac{b_0}{b_1} \implies a_0 b_1 < b_0 a_1$).

Claim. (The idea here is to show $a < \frac{a+b}{2} < b$.)

$$(a_0,\ a_1) <_{\mathbb{Q}} (a_1 b_0 + a_0 b_1,\ 2a_1 b_1) <_{\mathbb{Q}} (b_0,\ b_1)$$

Notice

$$a_0b_1 < b_0a_1 \implies a_0a_1b_1 < a_1^2b_0 \implies 2a_0a_1b_1 < a_1^2b_0 + a_0a_1b_1$$

and thus $(a_0,\ a_1) <_{\mathbb{Q}} (a_1b_0 + a_0b_1,\ 2a_1b_1)$. Similarly

$$a_0b_1 < b_0a_1 \implies a_0b_1^2 < a_1b_0b_1 \implies a_1b_0b_1 + a_0b_1^2 < 2a_1b_0b_1$$

and thus $(a_1b_0 + a_0b_1,\ 2a_1b_1) <_{\mathbb{Q}} (b_0,\ b_1)$ and the claim follows.

By repeating this proof two more times with $a < 0$, $b > 0$ and $a > 0$, $b < 0$ we can show $\mathbb{Q}$ is dense. ■

Theorem 4.31. $<_{\mathbb{Q}}$ is a dense denumerable strict order with no $<_{\mathbb{Q}}$-least and no $<_{\mathbb{Q}}$-greatest element.

Proof. Immediate consequence of Theorems 4.27, 4.28, and 4.30. ■

This Theorem 4.31 characterizes $<_{\mathbb{Q}}$ as we now show:

Theorem 4.32. If R and S are dense denumerable strict orders with no least and no greatest element, then R and S are isomorphic.

Proof. Bounty. ■

Moreover, $<_{\mathbb{Q}}$ is *universal* among countable strict orders.

Theorem 4.33. If A is countable and ordered by R then A can be embedded in $\mathbb{Q}$.

Proof. It suffices to show there exists an injective and homomorphic function $f : A \to \mathbb{Q}$.

Notice A countable and ordered $\implies$ $A = \{a_0, a_1, a_2, \ldots\}$. Let us show how to construct a homomorphic $f : A \to \mathbb{Q}$. First let $f(a_0) = 0$ and assume that f is homomorphic on

$$f : \{a_0, \ldots, a_n\} \to \mathbb{Q}.$$

That is $a_i < a_j \leq a_n \implies f(a_i) < f(a_j)$.

We define $f(a_{n+1})$ to maintain this property. Let

$$X = \{a \in \{a_0, \ldots, a_n\} : a < a_{n+1}\}$$
$$Y = \{a \in \{a_0, \ldots, a_n\} : a > a_{n+1}\}$$

and notice, by design

$$x \in f[X] \wedge y \in f[Y] \implies f(x) <_{\mathbb{Q}} f(y).$$

Because $\mathbb{Q}$ *is dense*

$$\exists q \in \mathbb{Q} : \sup(f[X]) < q < \inf(f[Y]).$$

Letting $f(a_n) = q$ we see $(a < a_n \implies f(a) < f(a_n))$ and $(a > a_n \implies f(a) > f(a_n))$.

Therefore $f : A \to \mathbb{Q}$ defined by

$$f(a_0) = 0$$
$$f(a_{n+1}) = q$$

for any q

$$\sup(f[\{a \in \{a_0, \ldots, a_n\} : a < a_{n+1}\}]) < q < \inf(f[\{a \in \{a_0, \ldots, a_n\} : a < a_{n+1}\}])$$

is a homomorphic function from $F : A \times A$ into $<_{\mathbb{Q}}$. ∎

For any strict order, we can define the *closed interval* $[a, b]$ and the *open interval* $\langle a, b \rangle$.

Definition 4.34. Let R be a strict oder.

$$[a, b] := \begin{cases} \{p : (aRp \wedge pRb) \vee (p = a) \vee (p = b)\} & \text{when } aRb \vee a = b \in \mathrm{fld}(R) \\ \varnothing & \text{otherwise} \end{cases}$$

$$\langle a, b \rangle := \begin{cases} \{p : (aRp \wedge pRb)\} & \text{when } aRb \\ \varnothing & \text{otherwise} \end{cases}$$

Theorem 4.35. Let R be an infinite strict order. If $[a, b]$ is finite for all $a, b \in \mathrm{fld}(R)$, then R is isomorphic to $<_{\mathbb{Z}}$ or $\in_\omega$ or $\breve{\in}_\omega$.

Exercise 4.36. Prove or refute: Let R be an infinite strict order. If $\langle a, b \rangle$ is finite for all $a, b \in \mathrm{fld}(R)$, then R is isomorphic to $<_{\mathbb{Z}}$ or $\in_\omega$ or $\breve{\in}_\omega$.

4.3 Real Numbers

We wish to construct the set $\mathbb{R}$ of all real numbers from the set $\mathbb{Q}$ or rational numbers by "filling in the gaps". It turns out that this construction can be applied to any strict order.

Definition 4.37. Let R be a strict order and let $A = \mathrm{fld}(R)$. Then (B, C) is an *ordered partition* of A *if and only if*

$$(B \cup C = A) \wedge (B \cap C = \varnothing) \wedge (B \neq \varnothing) \wedge (C \neq \varnothing)$$

$$\wedge\, \forall y \forall z (y \in B \wedge z \in C \implies yRz).$$

Definition 4.38. Let R be a strict order and let $A = \mathrm{fld}(R)$ and (B, C) be an ordered partition of A.

1. (B, C) is a *jump* $\iff$ (B contains an R-last element and C contains an R-first element),
2. (B, C) is a *Dedekind cut* $\iff$ $\forall z\,((z \text{ is an } R\text{-infimum of } c) \implies z \in C)$.

Definition 4.39. Let R be a strict oder and $A = \mathrm{fld}(R)$.

1. Let $B \subseteq A$. The B is *dense* in A when

$$\forall x \forall z (xRz \implies \exists y : y \in B \wedge xRy \wedge yRz)$$

2. A is *Dedekind-complete if and only if* every non-empty subset E of A which has an R-upper bound also has an R-least upper bound (an R-supremum).

Theorem 4.40 (Dedekind-completion of $\mathbb{Q}$)**.** There is a Dedekind-completion strict order S with no S-first or S-last element such that,

1. $\mathbb{Q} \subseteq \mathrm{fld}(S)$ and $<_{\mathbb{Q}} \subseteq S$ and S agree on $\mathbb{Q}$, and
2. $\mathbb{Q}$ is dense in $\mathrm{fld}(S)$.

$E = \mathrm{fld}(S)$ is unique up to isomorphism; that is, if S_1 and S_2 are two such relations with $E_1 = \mathrm{fld}(S_1)$ and $E_2 = \mathrm{fld}(S_2)$, then there is an isomorphism h between E_1 and E_2 such that $h(a) = a$ for all $a \in \mathbb{Q}$.

Definition 4.41 (Real Numbers)**.** Let $\mathbb{R}$, called the set of real numbers, be the set E constructed in Theorem 4.40, and $<_{\mathbb{R}}$ be the relation S constructed there.

Theorem 4.42. $|\mathbb{R}| = 2^{\omega}$.

Proof. Assignment 4. ∎

Theorem 4.43. $|\mathbb{R} \times \mathbb{R}| = 2^{\omega}$.

Proof. Exercise. ∎

Theorem 4.44. $n \neq 0 \implies |{}^{n}\mathbb{R}| = 2^{\omega}$.

Proof. Bounty. ∎

Theorem 4.45. $|{}^{\omega}\mathbb{R}| = 2^{\omega}$.

Proof. Exercise. ∎

Theorem 4.46. A is countable $\implies |\mathbb{R} \setminus A| = 2^{\omega}$.

Proof. Bounty. ∎

5 Well-Orderings and Ordinal Number

This chapter continues the development which began with the definition of well-ordering (§**??**) and with Chapter 3 on the natural numbers.

5.1 Initial Segments

Throughout this section we assume that "less than" $<$ is a *strict partial order* on a set A; we extend $<$ to "less than or equal to" by

Definition 5.1 ($\leq$). $\forall x, y \in A;\ x \leq y \iff (x < y \vee x = y)$.

Definition 5.2 (Initial Segment). Let $B \subseteq A$. Then B is an *initial segment* of A *if and only if* $B \subset A$ and

$$\forall x \forall y;\ (y \in B \wedge x < y) \implies x \in B.$$

Theorem 5.3. If $<$ well-orders A and B is an initial segment of A then $\exists a \in A\ :\ B = \{y\ :\ y \in A \wedge y < a\}$.

Proof. Since $<$ is a well-order

$$\exists a \in A\ :\ a = \min(A \setminus B)$$

We have $a \notin B$ so it follows

$$\begin{aligned} a = \min(A \setminus B) & \\ \iff & (\forall x \in A \setminus B;\ x \geq a) \\ \iff & (\forall x \in A;\ x \notin B \implies x \geq a) \\ \iff & (\forall x \in A;\ x < a \implies x \in B). \end{aligned}$$

Thus $\{y \in A : y < A\} \subseteq B$.

Moreover, by definition,

$$\begin{aligned} y \in B &\implies (\forall x \in A;\ x < y \implies x \in B) \\ &\implies (\forall x \in A;\ x \notin B \implies x \geq y) \\ &\text{Note } x \notin B \implies x \neq y \text{ so} \\ &\implies (\forall x \in A;\ x \notin B \implies x > y) \\ &\implies a > y \\ &\implies y \in \{y : y \in B \wedge y < a\} \\ &\implies y \in \{y : y \in A \wedge y < a\} \end{aligned}$$

Thus $B \subseteq \{y : y \in A \wedge y < a\}$ and the result follows. ∎

Exercise 5.4. *Prove or refute.*

1. Suppose $<$ is a strict partial order but is *not* connected. Then there is some initial segment B of $A = \text{fld}(<)$ such that

$$\forall a \in A\,(B \neq \{x : x \in A \wedge x < a\}).$$

2. For every C with at least 4 elements, there is some strict partial order R with $\text{fld}(R) = C$ and some initial segment B of C such that

$$\forall a \in C;\ B \neq \{x : x \in C \wedge xRa\}.$$

3. There is some C and some R such that R orders C, and there is some initial segment B of C such that

$$\forall a \in C;\ B \neq \{x : x \in C \wedge xRa\}.$$

Definition 5.5. $f : A \to A$ is said to be increasing when

$$\forall x, y \in A;\ x < y \implies f(x) < f(y).$$

Theorem 5.6. If $<$ well-orders A and $f : A \to A$ is increasing, then $\forall x \in A\,(x \leq f(x))$.

Proof. Assume the premise, let $X = \{x \in A : f(x) < x\}$, and towards a contradiction assume $X \neq \varnothing$. Because A is well ordered X must have a least element (say) z where $f(z) < z$.

Notice because f is increasing

$$f(z) < z \implies f(f(z)) < f(z)$$

Thereby $f(z) < z$ satisfies the property for which z was assumed minimal. $\lightning$ ∎

Exercise 5.7. Any isomorphism $A \approx_f B$ must preserve the well ordering. In particular $f(\min(A)) = \min(B)$.

Theorem 5.8. Let $<$ well-order A. Then,

1. no initial segment of A is isomorphic to A,
2. A has only one automorphism, the identity function on A,
3. if A and B are isomorphic *and* well-ordered, then the isomorphism between A and B is unique.[1]

Proof of 1. Assume $<$ well-orders A and, towards a contradiction, assume there is some $a \in A$ such that

$$A \approx_f \{x \in A : x < a\}$$

(i.e. that A is isomorphic to some initial segment of itself).

Consider $B = \{x : x \neq f(x)\}$ and let $m = \min(B)$. As $f(m) \neq m$ we have either $f(m) < m$ or $m < f(m)$.

Case: $f(m) < m$

$$f(m) < m \implies f(f(m)) = f(m) \implies f(m) = m \lightning.$$

Case: $m < f(m)$
Let $f(a) = m$ and notice $a > m$ otherwise $f(a) = a$.

$$a > m \implies f(a) > f(m) \implies m > f(m) \lightning$$

Thus we must have $f(m) = m$ which contradicts our original assumption. The result follows. ∎

Proof of 2. Assume towards a contradiction there is f such that $A \approx_f A$ and f is *not* the identity. Thereby we have $B = \{x : x \neq f(x)\} \neq \varnothing$ and can use the same argument as 1. ∎

[1] This is sometimes referred to as the "rigidity lemma."

Proof of 3. Suppose, towards a contradiction, that

$$A \approx_f B \wedge A \approx_g B \wedge f \neq g.$$

Let $A := A_1 \cup A_2 = \{a : f(a) = g(a)\} \cup \{a : f(a) \neq g(a)\}$ and notice

1. $A_1 \neq \varnothing$ because by Exercise 5.7
2. $A_2 \neq \varnothing$ because $f \neq g$, and $f(\min(A)) = g(\min(A))$.

Let $B_1 := f(A_1)$ and note by definition that $f(A_1) = g(A_1)$. We have that

$$f(\min(A_2)) = \min(B \setminus B_1) = g(\min(A_2)).$$

But by definition $f(a) \neq g(a)$ for $a \in A_2$. ↯ ∎

Theorem 5.9. Let R well-order A, and S well-order B. Then exactly one of the following conditions is true:

1. A is isomorphic to B,
2. A is isomorphic to an initial segment of B,
3. B is isomorphic to an initial segment of A.

Exercise 5.10. *Prove or refute.* Let $<$ well-order A, and $B \subset A$. Then B is well-ordered by $<_B$ and is isomorphic to an initial segment of A.

6 Axiom of Choice

This axiom was once controversial, but plays an important role in branches of mathematics.

Definition 6.1 (Choice Function). B has a *choice function* $\iff$ there is some function f with $f(z) \in z$ for every non-empty z with $z \in B$.

Example 6.2. Let $\{\{1,4,7\}, \{9\}, \{2,7\}\}$ then a choice function f is given by

$$f(\{1,4,7\}) = 7 \qquad f(\{9\}) = 9 \qquad f(\{2,7\}) = 2.$$

Theorem 6.3. Every finite set has a choice function.

Proof. Let B be an arbitrary finite set. We have then that B is countable and can be written

$$B = \{S_0, S_1, \ldots, S_n\}$$

for some $n \in \mathbb{N}$. Proceeding with the PMI let

$$\psi(n) \iff B = \{S_0, \ldots, S_n\} \text{ has a choice function.}$$

Notice $\{S_0\}$ trivially has a choice function because $S_0 \neq \varnothing \implies \exists s \in S_0$ so we can let the choice function be given by $f(S_0) = s$.

Consider $B = \{S_0, \ldots, S_n, S_{n+1}\}$, let f be the choice function on $\{S_0, \ldots, S_n\}$ ensured by $\psi(n)$, and note $S_{n+1} \neq \varnothing \implies \exists s \in S_{n+1}$. Thus

$$f' = f \cup \{(S_{n+1}, s)\}$$

is a choice function for B. ∎

Note the proof for the above uses induction over n so does *not* prove there are choice functions for infinite sets (only arbitrary large finite sets).

Theorem 6.4. B can be well-ordered $\iff$ $\mathcal{P}(B)$ has a choice function.

$\implies$. Assume B is well-ordered which means any nonempty subset of B has a least element. Thereby the function

$$\begin{aligned} f : \mathcal{P}(B) \setminus \{\varnothing\} &\to B \\ x &\mapsto \min(x) \end{aligned}$$

is a choice function for $\mathcal{P}(B)$. ∎

$\impliedby$. Assume $\mathcal{P}(B)$ has a choice function $f : \mathcal{P}(B) \setminus \{\varnothing\} \to B$. We can build a well-ordering $b_0 < b_1 < b_2 \cdots$ from f as follows.

$$\begin{aligned} b_0 &= f(B) \\ b_1 &= f(B \setminus \{b_0\}) \\ b_2 &= f(B \setminus \{b_0, b_1\}) \\ &\vdots \\ b_n &= f(B \setminus \{b_0, \ldots, b_{n-1}\}) \\ &\vdots \end{aligned}$$

∎

Definition 6.5. If A is a function, then A_i is defined to be $A(i)$, provided that $i \in \operatorname{dom}(A)$.

We now define union, intersection, and Cartesian product over such an index set I:

Definition 6.6. Let $I \subseteq \operatorname{dom}(A)$, where A is a function:

1. $\bigcup_{i \in I} A_i = \cup \{A_i : i \in I\}$,
2. $\bigcap_{i \in I} A_i = \cap \{A_i : i \in I\}$,
3. $\prod_{i \in I} A_i = \{f : \operatorname{dom}(f) = I \wedge \forall i \, (i \in I \implies f(i) \in A_i)\}$.

Then $\prod_{i \in I} A_i$ is called the *Cartesian product* of $\{A_i : i \in I\}$.

As an aside, notice that $\prod_{i \in \{0,1\}} A_i$ is *not* generally equal to $A_0 \times A_1$:

Exercise 6.7. There are sets A_0 and A_1 such that

$$\prod_{i \in \{0,1\}} A_i \neq A_0 \times A_1.$$

However, we have the following:

Theorem 6.8. For every A_0 and A_1,

$$\prod_{i\in\{0,1\}} A_i \approx A_0 \times A_1.$$

We now state the following *Axiom of Choice* but we do not yet assume it:

Axiom 7 (AC). Every set has a choice function.

Theorem 6.9. The following are equivalent:

1. the axiom of choice,
2. every set can be well-ordered,
3. $\prod_{i\in I} A_i \neq \varnothing \iff \forall i \in I\,(A_i \neq \varnothing)$.

Theorem 6.10. The following are equivalent:

1. the axiom of choice,
2. **The Maximal Principle**. Let $<_A$ be a strict partial order on a set A. Let B be a subset of A such that $<_A$ is a strict order on B. Then there exists an $\subseteq$-maximal subset C of A such that $B \subseteq C$ and $<_A$ is a strict order on C.

We now give some consequences of the axiom of choice that cannot be proved from our other axioms alone:

Theorem 6.11. The axiom of choice implies that the following are equivlanet:

1. B is infinite,
2. $\omega \preccurlyeq B$.

Theorem 6.12. The axiom of choice $\implies$ (the union of a countable set of countable sets is countable).

Theorem 6.13. The axiom of choice $\implies$ (the set $\mathbb{R}$ of all real numbers is not countable union of countable sets).

Theorem 6.14. The axiom of choice $\implies$ (every vector space has a basis).

Theorem 6.15. The axiom of choice $\implies$ (there is a function $f : \mathbb{R} \to \mathbb{R}$ such that, for all $x, y \in \mathbb{R}$, $f(x+y) = f(x) + f(y)$ but $f(x)$ is not linear).

For all *continuous* real functions, if $f(x+y) = f(x) + f(y)$ for all x, y, then $f(x) = kx$ for some constant k.

And they lived happily ever after...