Notebook for Real Analysis

Guanyuming He

September 8, 2020

This document serves as a notebook for Tao's analysis book.

Contents

1 General Principles

This section describes the overall principles of the document. It illuminates how notations are explained, in what structure this document is written and so forth. This section should be read and understood comprehensively prior to reading the main content of the document.

1.1 Definitions

The document The phrase *the document* means this document (what you're reading) itself.

The book The phrase *the book* represents Tao's *Analysis* (both volume I and II).

1.2 Indices

The book has two volumes: *Analysis I* and *Analysis II*. We may notice that the indices of the two volumes both start from 1. It may lead to some confusions. So in the document, the indices are organized in such a way that: If the content comes from *Analysis I*, the corresponding index is the same as the book's. Otherwise, the corresponding index is prefixed with "2.".

For example, Exercise 3.1.3 in *Analysis I* is indexed as Exercise 3.1.3 in the document, but Exercise 3.1.3 in *Analysis II* is indexed as Exercise 2.3.1.3.

1.3 Notations

In the answers to some exercises, you may notice that the content are divided by numbers enclosed with parentheses (e.g. **(1)**, **(2)**). Tao often puts multiple questions into a single exercise, so these numbers indicates the number of the sub-questions.

For example, Exercise 3.5.4 is

> Exercise 3.5.4. Let A, B, C be sets. Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$, that $A \times (B \cap C) = (A \times B) \cap (A \times C)$, and that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Then (1) indicates the question "Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.", (2) indicates the question "Show that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.", and (3) indicates the question "Show that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$".

In logical contents,

$$\Longrightarrow, \Rightarrow, \longrightarrow, \rightarrow,$$

have the same meaning "implies". And

$$\Longleftarrow, \Leftarrow, \longleftarrow, \leftarrow,$$

also have the same meaning ($P \leftarrow Q$ means that Q implies P). Finally, these following symbols all indicate logical equality.

$$\leftrightarrow, \longleftrightarrow, \Leftrightarrow, \Longleftrightarrow, \equiv$$

.

For nested quantifiers, their order is "from left to right". For example, the following statement

$$\forall x \exists y (P(x, y))$$

means that for all object x, their exists a object y such that $P(x, y)$ is true. That is,

$$\forall x (\exists y (P(x, y)))$$

Tao uses ++ to denote the successor of a natural number. However, in the document, it is denoted by $S(n)$ most of the times.

$$\bigvee_{i=1}^{n} P(i), \bigwedge_{i=1}^{n} P(i)$$

mean that for $1 \leq i \leq n$, at least one $P(i)$ is true; and for all $1 \leq i \leq n$, $P(i)$ is true, respectively.

Some sets that have special meanings (e.g. the set of all natural numbers, the set of all real numbers) are denoted in whiteboard font (e.g. $\mathbb{N}, \mathbb{R}$).

Without special interpretation, the notation

$$(\forall x P(x))(Q(x))$$

is interpreted as

$$\forall x (P(x) \Longrightarrow Q(x))$$

For example,

$$(\forall x \in X)(Q(x)) \equiv \forall x (x \in X \Longrightarrow Q(x))$$

Part I
Natural Numbers

2 The Peano Axioms

I have learned the Peano axioms. They are descriptive rather than constructive. That is, when we are using this axiom system, we assume that natural numbers do exist, and their properties are described by these axioms. The intuition of the Peano axioms might have been counting from 0 (or 1) by the successor function, but if we try to understand the Peano axioms as constructive, for example, giving 0 first and constructing other numbers via the successor function, things may look a little weird, and the axioms may seem incomplete.

There are some remarkable things regarding the axioms. For the first axiom, Peano originally used 1 instead of 0. This is merely a difference of symbols here, though 0 and 1 have unique meanings in other areas, so 0 is more widely used today than 1. Peano also gave four axioms about the equality relation, and the first three of them (i.e. except the one that says the equality relation is closed under natural numbers) are used as more generic assumptions for general mathematical objects.

Once we have described the basic properties of natural numbers and the successor function S, we can apply our common symbol system to it. We define $1 := S(0),\ 2 := S(1)$ and so on.

There is something interesting about the mathematical induction. Consider the situation where we have a property $P(n)$ pertaining to all natural numbers n, and which is vacuously true if $n = 0$. Then do we need to check if it is true when $n = 1$, or can we just check if $P(n) \implies P(S(n))$?

The answer is, we need to check if it is true when $n = 1$. We can just choose a property $P(n)$ such that: $\neg P(0) \wedge (P(n) \implies P(S(n)))$. Then let $Q(n)$ be any property such that $Q(0)$ is vacuously true and $Q(n) \equiv P(n)$ when $n \neq 0$. We can see that $Q(n)$ may not be always true.

Another thing is, what if a property P does not pertain to 0? For example, if we let P be a property pertaining to all $n \in \mathbb{N} \wedge n \neq 0$, can we apply mathematical induction to it? Generally we can. We can define the property $Q(n)$ to be $P(S(n))$, then $Q(0) \equiv P(1)$ is the base case.

2.1 Addition of Natural Numbers

Then we define operations, such as addition, on natural numbers.

Addition The intuition is, the successor function acts like a +1 function. That is,

$$n + 1 := S(n) \tag{1}$$

And to add 2 to a number is to merely apply S two times to it. So from the informal equation 1, we can furthermore define

$$n + 2 := S(S(n)) = S(n + 1) \tag{2}$$

Note that by definition, $2 = S(1)$. Apply the substitution to equation 2, we can see that

$$n + S(1) := S(n + 1)$$

We may notice that if we define $n + 0 := n$, then equation 1 can be rewritten as

$$n + S(0) := S(n + 0)$$

So now we could try to assume two rules here:

Definition 1.
1. $0 + n := n$,
2. $S(m) + n := S(m + n)$

and see if it is a good definition of addition.

For every natural number n, we first have $0 + n = n$. Then if we want to know what $1 + n$ is, we have

$$\begin{aligned}
1 + n &= S(0) + n && \text{(By Def. of 1)}\\
&= S(0 + n) && \text{(By the second rule)}\\
&= S(n) && \text{(By the first rule)}
\end{aligned}$$

Repeat the process to gain more results:

$$\begin{aligned}
2 + n &= S(1) + n && \text{(By Def. of 2)}\\
&= S(1 + n) && \text{(By the second rule)}\\
&= S(S(n)) && \text{(By the result of } 1 + n\text{)}
\end{aligned}$$

Use induction (Suppose we have known $m + n = \underbrace{S(S(\ldots(}_{m\text{ times}} n \underbrace{)\ldots))}_{m\text{ times}}$):

$$\begin{aligned}
S(m) + n &= S(m + n) && \text{(By the second rule)}\\
&= \underbrace{S(S(\ldots(}_{m+1\text{ times}} n \underbrace{)\ldots))}_{m+1\text{ times}} && \text{(By the result of } m + n\text{)}
\end{aligned}$$

And then the add operation is defined for every natural number.

Afterward we will turn to some properties of the newly defined operation – addition. We are going to prove the commutativity and associativity of addition.

Lemma 1. *For any natural number n, $n + 0 = n$*

Proof. Firstly, by definition, $0 + 0 = 0$.

Secondly, if for natural number n, $n + 0 = n$ is true, then $S(n) + 0 = S(n + 0) = S(n)$. This closes the induction, so the proposition is right. □

Lemma 2. *For any natural number m, n, $n + S(m) = S(n + m)$*

Proof. For any fixed natural number m:

1. $0 + S(m) = S(m) + 0 = S(m + 0)$
2. Suppose that $n + S(m) = S(n + m)$, then

$$\begin{aligned} S(n) + S(m) &= S(n + S(m)) && \text{(By Def.)} \\ &= S(S(n + m)) && \text{(By assumption)} \\ &= S(S(n) + m) && \text{(By Def.)} \end{aligned}$$

This closes the induction and the proof is over. □

Proposition 1. *The addition of natural numbers is commutative. That is,*

$$m + n = n + m$$

Proof. First of all, $0 + n = n + 0$.

Then, assume that $m + n = n + m$. Thus:

$$\begin{aligned} S(m) + n &= S(m + n) && \text{(By Def.)} \\ &= S(n + m) && \text{(By Assumption)} \\ &= n + S(m) && \text{(By Lemma 2)} \end{aligned}$$

, which closes the induction. □

Proposition 2. *(Exercise 2.2.1) The addition of natural numbers is associative. That is, $(a + b) + c = a + (b + c)$.*

Proof. Use induction: First, $(0+b)+c = b+c = 0+(b+c) = b+c$.

Then, assume that $(n+b)+c = n+(b+c)$, thus

$$\begin{aligned}(S(n)+b)+(c) &= S(n+b)+c \\ &= S(n+b+c) \\ &= S(n+(b+c)) && \text{(By assumption)} \\ &= S(n)+(b+c)\end{aligned}$$

, which closes the induction. □

How fascinating! We have proven the basic properties of addition with only the definition of addition and the axioms. It seemed that we have to define these properties, but we did prove them!

Now we are about to prove some useful propositions about addition.

Proposition 3. *The cancellation law: If $a+b = a+c$, then $b = c$.*

Proof. Use induction: $0+b = 0+c \Longrightarrow b = c$.

Assume that $a+b = a+c \Longrightarrow b = c$, thus

$$\begin{gathered}S(a)+b = S(a)+c \Longrightarrow \\ S(a+b) = S(a+c) \Longrightarrow \\ S(b) = S(c) \Longrightarrow \\ b = c\end{gathered}$$

□

Then we describe natural numbers that are not equal to 0 as **positive**.

Proposition 4. *If a is positive, then for any natural number b, $a+b$ is positive.*

Proof. Use induction: $a+0 = a$ is positive.

Assume that $a+b$ is positive, then

$$a+S(b) = S(a+b)$$

can not be 0, for 0 is not a successor of any natural number. This closes the induction. □

Corollary 1. *If for natural number a, b, $a+b = 0$, then $a = 0 \wedge b = 0$*

Proof. Presume the contradiction, that there exist $a \neq 0, b \neq 0$, $a + b = 0$.

$$a \neq 0 \Longrightarrow a \text{ is positive}$$

Then according to proposition 4, $a + b$ is also positive, which can not be 0. □

We may wonder something like is it true for every natural number $n \neq 0$, n is always the successor of some other natural number. That is, 0 is the only natural number that is not the successor of any natural number. Or we can convey it in such a way as following:

Proposition 5. *(Exercise 2.2.2) For any positive natural number n, there is exactly one natural number m that $S(m) = n$.*

Proof. Use induction: When $n = 0$, the statement is vacuously right.

Assume that the statement is true for a natural number n, thus

Existence

$$S(S(m)) = S(n)$$

Uniqueness It is obvious according to axiom 3.

□

Proposition 6. *For any natural number n, $S(n) \neq n$*

Proof. Use induction: $S(0) \neq 0$ for 0 is not the successor of any natural number.

Assume that $S(n) \neq n$. Suppose that $S(S(n)) = S(n)$, then by axiom 3, $n = S(n)$, then we have a contradiction. This closes the induction. □

2.2 Order of Natural Numbers

Then I learned the order of natural numbers.

Here I introduce one my own lemma:

Lemma 3. $a = a + n \Longleftrightarrow n = 0$

Proof. On one hand, suppose that $a = a + n$ but $n \neq 0$. Try to prove the contradiction. Use induction: First, n is positive, so $0 + n \neq 0$.

Assume that $n \neq 0 \Longrightarrow a \neq a + n$, thus

$$S(a) + n = S(a + n) \neq S(a) \text{ by assumption}$$

, which closes the induction. Then by the axiom of induction, we have a contradiction, so $a = a + n \Longrightarrow n = 0$.

On the other hand, $n = 0 \Longrightarrow a + n = a$. □

Hereby proposition 2.2.12 of Tao's book is proven.

Proposition 7. *(Exercise 2.2.3)*

1. *Order is reflective* $a \geq a$
2. *Order is transitive* $a \geq b \wedge b \geq c \implies a \geq c$
3. *Order is anti-symmetric* $a \geq b \wedge b \geq a \implies a = b$
4. *Addition preserves order* $a \geq b \implies a + c \geq b + c$
5. $a < b \iff S(a) \leq b$
6. $a < b$ *Iff for positive natural number* c, $b = a + c$

Proof. (1) It is immediately proven by $a = a + 0$.

(2)

$$\begin{gathered} a \geq b \wedge b \geq c \implies \\ a = b + m \wedge b = c + n \implies \\ a = c + n + m = c + (n + m) \implies \\ a \geq c \end{gathered}$$

(3) By definition of order,

$$\begin{aligned} a \geq b \wedge b \geq a \implies & \\ a = b + m \wedge b = a + n \implies & \\ a = a + (n + m) \implies & \\ n + m = 0 \implies & \qquad \text{(By Lemma 3)} \\ n = m = 0 \implies & \qquad \text{(By Corollary 1)} \\ b = a + 0 = a & \end{aligned}$$

(4)

$$\begin{aligned} a \geq b \equiv \\ a = b + n \equiv \\ a + c = (b + n) + c = b + (n + c) = b + (c + n) = (b + c) + n \equiv \\ a + c \geq b + c \end{aligned}$$

(5)

$$
\begin{aligned}
a < b &\iff \\
b = a + p &\iff \\
b + 1 = a + p + 1 = a + 1 + p = S(a) + p& \\
= S(a) + S(n)& \\
\text{(By proposition 5, } p \text{ is always some natural number } n\text{'s successor)}& \\
= S(a) + n + 1 &\iff \\
b = S(a) + n &\iff \qquad \text{(By cancellation law)} \\
b \geq S(a)&
\end{aligned}
$$

(6) On one hand, $b = a + c$ immediately gives $a < b$.
On the other hand, according to (5), $a < b$ gives

$$
\begin{aligned}
S(a) \leq b &\implies \\
b = S(a) + n& \\
= a + 1 + n = a + (n + 1)&
\end{aligned}
$$

, where $n + 1$ is positive. □

Proposition 8. *(Exercise 2.2.4) For two natural number m, n, m either $>$, or $=$, or $<$ n.*

Proof. Tao's book has proven that at most one statement can be true at a time.

Now we are proving the remnant. Use induction: When $m = 0$, for any natural number n, $0 = n$, or $0 \neq n$. Under the latter case:

Lemma 4. *n is positive $\iff n > 0$*

Proof. On one hand, $n > 0$ immediately gives n is positive.

On the other hand, $n = 0 + n$ gives $n \geq 0$. And n being positive implies that $n \neq 0$. So $n > 0$. □

According to the lemma, in this situation, $0 < n$. So 0 either $<$ or $=$ n.

Assume that we have proven the statement for a natural number m, thus when $m < n$, according to Proposition 2.2, $S(m) \leq n$, so $S(m)$ either $<$ or $=$ n. When $m = n$, $S(m) = n + 1 \implies S(m) > n$ by Proposition 2.2. When $m > n$, according to Proposition 2.2,

$$m = n + p \implies S(m) = n + (p + 1) \implies S(m) > n$$

. This closes the induction, implying that at least one of the three statements is true. ☐

Exercise 2.2.5

Proof. Let $Q(n)$ be a property of a natural number n such that $Q(n)$ is true iff for all $m_0 \leq m' < n$, $P(m')$ is always true. Use induction: $Q(0)$ is vacuously true.

Assume that $Q(n)$ is true. Here we will be using the proposition we just proved, for because we have known that there will and only will be one true statement, we can classify the conditions as following: When $S(n) < m_0$, $Q(S(n))$ is also vacuously true. When $S(n) = m_0$, $Q(S(n))$ is true because $P(m_0)$ is true. And when $S(n) > m_0$:

First we need to prove that n is the only natural number $\geq m_0$ which satisfies $m_0 \leq n < S(n)$ but doesn't satisfy $m_0 \leq n < n$, so that we only need to prove $P(n)$ is true in the induction, which is obvious.

Lemma 5. *There is no natural number between* n *and* $S(n)$*. That is, there is no such natural number* m *that* $n < m < S(n)$*.*

Proof. Presume the contradiction. Thus, $m = n + p \wedge S(n) = m + q$, where p, q are positive. Substituting m with $n + p$ we have $S(n) = n + p + q$. Let $p = S(a) = a + 1$, which is always possible according to Proposition 5. Thus $n + 1 = n + 1 + a + q \Longrightarrow n = n + a + q$, which means $a + q$ has to be 0, and which is impossible. ☐

Given a natural number a, it either $\geq$ or $<$ $S(n)$, and also either $\geq$ or $<$ n. Should it satisfy $m_0 \leq a < S(n)$ but doesn't satisfy $m_0 \leq a < n$, it then must satisfy $n \leq a < S(n)$, that is, either $a = n$ or $n < a < S(n)$. The latter, according to the lemma, is impossible. So n is the only natural number $\geq m_0$ which satisfies $m_0 \leq n < S(n)$ but doesn't satisfy $m_0 \leq n < n$.

Then $Q(S(n)) \Longleftrightarrow Q(n) \wedge P(n)$, which is true. This closes the induction. So $Q(n)$ is true for all natural number $n \geq m_0$. And this implies that $P(n)$ is true. ☐

Exercise 2.2.6

Proof. Use induction: When $n = 0$, for all natural number $m \leq 0$, $P(m)$ is true.

Assume that we have proven for a natural number n that if $P(n)$ is true, then for all natural number $m \leq n$, $P(m)$ is also true. Thus, $P(S(n)) \Longrightarrow$

$P(n) \implies \forall m \leq n, P(m)$ is true. According to Lemma 5, $(\forall m \leq n, P(m)) \wedge P(S(n)) \iff \forall m \leq S(n), P(m)$. This closes the induction. □

2.3 Multiplication of Natural Numbers

Lemma 6. *(Exercise 2.3.1) Multiplication is commutative. That is,* $a \times b = b \times a$.

Proof. I

Try to imitate the way we prove the commutativity of addition.

Lemma 7.

$$0 \times a = a \times 0$$

Proof. Use induction: $0 \times 0 = 0$. Assume that $n \times 0 = 0$ is true. Thus, $S(n) \times 0 = (n \times 0) + 0 = 0$, which closes the induction. □

Lemma 8.

$$a \times S(b) = a \times b + a$$

Proof. Use induction: $0 \times S(b) = 0 = 0 \times b + 0$.

Assume that $a \times S(b) = ab + a$ is true. Thus,

$$\begin{aligned} S(a)S(b) &= aS(b) + S(b) && \text{(By Def.)} \\ &= ab + a + S(b) && \text{(By assumption)} \\ &= ab + S(a) + b && \text{(By addition's properties)} \\ &= (ab + b) + S(a) && \text{(By addition's properties)} \\ &= S(a)b + S(a) && \text{(By Def.)} \end{aligned}$$

, which closes the induction. □

Now use induction on a. First, when $a = 0$, by Lemma 7 we have $ab = ba$. Assume that $ab = ba$ is true. Thus,

$$\begin{aligned} S(a)b &= ab + b \\ &= ba + b \\ &= bS(a) && \text{(Lemma 8)} \end{aligned}$$

, which close the induction.

□

Proof. II In this proof we will use the distribution law of multiplication.

First, we have Lemma 7

Before we prove the remnant, we need to prove the distribution law. That is, $a \times (b + c) = ab + ac$

Proof. Use induction: $0 \times (b + c) = 0 \times b + 0 \times c = 0$.

Assume that $a \times (b + c) = ab + ac$ is ture. Thus,

$$
\begin{aligned}
S(a) \times (b + c) &= (a(b + c)) + (b + c) \\
&= (ab + ac) + (b + c) && \text{(By assumption)} \\
&= (ab) + b + (ac) + c \\
&= S(a)b + S(a)c
\end{aligned}
$$

, which closes the induction. □

We still have to prove $n \times 1 = n$ before proceeding. Use induction: $0 \times 1 = 0$. Assume that $n \times 1 = n$. Thus, $S(n) \times 1 = (n \times 1) + 1 = n + 1 = S(n)$.

Now we can proceed the proof. Assume that $a \times b = b \times a$. Thus,

$$
\begin{aligned}
S(a)b &= (ab) + b \\
&= (ba) + b && \text{(By assumption)} \\
&= b(a + 1) && \text{(By } b \times 1 = b \text{ and the distribution law)} \\
&= b \times S(a)
\end{aligned}
$$

. This closes the induction. □

Lemma 9. *(Exercise 2.3.2)*

$$mn \neq 0 \Longleftrightarrow m \neq 0 \wedge n \neq 0$$

Proof. On one hand, let $m = S(a),\ n = S(b)$, where a, b are natural numbers.

$$
\begin{aligned}
mn &= S(a)S(b) \\
&= aS(b) + S(b)
\end{aligned}
$$

which, if $a \neq 0$, is the sum of two positive numbers, and is thus positive, and which, if $a = 0$, is a positive number $S(b)$.

On the other hand, if either of m, n is 0, then mn must be zero. So $mn \neq 0 \Longrightarrow m \neq 0 \wedge n \neq 0$. □

Distribution law has been proved here.

Proposition 9. *(Exercise 2.3.3)*

$$(ab)c = a(bc)$$

Proof. Use induction on a. First, $(0b)c = 0c = 0 = 0(bc)$.

Assume that $(ab)c = a(bc)$ is true. Thus,

$$\begin{aligned}
(S(a)b)c &= (ab + b)c \\
&= c(ab + b) && \text{(Commutativity)} \\
&= c(ab) + cb && \text{(Distribution law)} \\
&= (ab)c + bc && \text{(Commutativity)} \\
&= a(bc) + bc && \text{(The induction hypothesis)} \\
&= S(a)(bc)
\end{aligned}$$

. And now we can close the induction. □

Proposition 10. *Multiplication preserves order. That is, if $a > b \wedge c > 0$, then $ac > bc$.*

Proof.

$$\begin{aligned}
a > b &\implies \\
a = b + p &\implies \\
ac = bc + pc &
\end{aligned}$$

According to Lemma 9, pc is positive. Therefore, $ac > bc$. □

Corollary 2. *Cancellation law.*

$$ac = bc \wedge c \neq 0 \implies a = b$$

Proof. Either $a = b$, or $a < b$, or $a > b$. Suppose that $a \neq b$. Therefore, ac either $<$ or $>$ bc, which, according to Proposition 10, gives a contradiction. So $a = b$. □

Proposition 11. *(Exercise 2.3.4)*

$$(a + b)^2 = a^2 + 2ab + b^2$$

(Suppose that we have known $n^2 = n \times n$)

Proof.

$$\begin{aligned}
(a+b)(a+b) &= (a+b)a + (a+b)b && \text{(Distribution law)}\\
&= a(a+b) + b(a+b) && \text{(Commutativity)}\\
&= a^2 + ab + ba + b^2 && \text{(Distribution law)}\\
&= a^2 + ab + ab + b^2 && \text{(Commutativity)}
\end{aligned}$$

Now we prove that $2ab = ab + ab$.

$$\begin{aligned}
2ab &= S(1)ab\\
&= (1ab) + ab\\
&= (S(0)ab) + ab\\
&= (0ab + ab) + ab\\
&= ab + ab
\end{aligned}$$

The proof is over. □

Proposition 12. *(Exercise 2.3.5) Euclidean algorithm. For any natural number n, positive number p, there exist natural numbers m, r such that $n = mp + r$.*

Proof. For any natural number p, we induct on n. Firstly, $0 = 0p + 0$.

Assume that the statement for n is true. We know that $r < p$. Then $S(r)$ either $=$ or $<$ p (Proposition 2.2). On the latter case, simply let $r' = S(r),\ m' = m$, which satisfies the restriction $0 \le r' < p$

On the former case, let $m' = S(m),\ r' = 0$, and we have

$$\begin{aligned}
m'p + r' &= S(m)p + 0\\
&= mp + p\\
&= mp + S(r) && (p = S(r))\\
&= S(mp + r)\\
&= S(n)
\end{aligned}$$

. And now we can close the induction. □

Part II
Set Theory

3 Fundamentals

Exercise 3.1.1

Proof. Reflexive: $\forall x \in S, x \in S$.

Symmetric:

$$\begin{aligned} X = Y &\iff \\ \forall x \in X, x \in Y \wedge \forall x \in Y, x \in X &\iff \\ Y = X & \end{aligned}$$

Transitive: $X = Y \implies \forall x \in X, x \in Y$. Because $x \in Y$ and $Y = Z$, we can conclude that $\forall x \in X, x \in Z$. Conduct the process from inversely, we can get $\forall x \in Z, x \in X$. Therefore, $X = Z$. $\square$

The reason for the content beneath Axiom 3.2 is clearly demonstrated in the proof of Lemma 3.1.6.

In Remarks 3.1.9, there are three "Why"s. The reason can be concluded as: Because of the "if and only if" in Axiom 3.3, or more precisely, "only if", if x is a element in one of such sets, x must $= a$ or b. And because of the "if", x is thus in another set. So the two sets are equal according to Definition 3.1.4.

Exercise 3.1.2

Proof. According to Axiom 3.2, $\varnothing$ exists, and is thus an object as stated by Axiom 3.1. Therefore, by Axiom 3.3, $\{\varnothing\}$ also exists. $\varnothing$ is an element of $\{\varnothing\}$, but it is not an element of $\varnothing$ because any object $\notin \varnothing$.

For the same reason, any set that contains element(s) is not the same set as $\varnothing$. Furthermore, there exists an object $\{\varnothing\}$ (Axiom 3.3 and 3.1), which is an element of $\{\varnothing, \{\varnothing\}\}$, but which is not an element of $\{\varnothing\}$. So the two sets are not equal. $\square$

Remarks 3.1.12

Proof. Let $x \in A' \cup B$. $x \in A' \implies x \in A$ And if $x \notin A'$, $x \in B$. So either way $x \in A \cup B$ and vice versa. $\square$

Exercise 3.1.3

Proof. (1)

$$x \in A \cup B \equiv (x \in A \vee x \in B)$$

$$x \in A \Longrightarrow x \in B \cup A$$

$$x \in B \Longrightarrow x \in B \cup A$$

So $x \in A \cup B \Longrightarrow x \in B \cup A$. And vice versa.

(2) $x \in A \Rightarrow x \in A \cup A$ and $x \in A \cup A \Rightarrow x \in A$.

(3)

$$\begin{aligned} x \in A \cup \varnothing &\Longrightarrow \\ x \in A \vee x \in \varnothing &\Longrightarrow \\ x \in A & \qquad (\forall a, a \notin \varnothing) \end{aligned}$$

And obviously $x \in A \Rightarrow x \in A \cup \varnothing$. So $A \cup \varnothing = A$.

By transitivity of equality, and commutativity of pairwise union, we can conclude the others. □

Examples 3.1.17

Proof.

$$\forall x (x \in A \Longrightarrow x \in A)$$

And

$$\forall x (x \in \varnothing \Longrightarrow x \in A)$$

is vacuously true. □

Exercise 3.1.4

Proof. (1) On one hand,

$$A \subseteq B \equiv \forall x (x \in A \Longrightarrow x \in B)$$

. On the other hand,

$$B \subseteq A \equiv \forall x (x \in B \Longrightarrow x \in A)$$

. Thus $A = B$.

(2) First, we prove that $A \subsetneq B \Longrightarrow \exists x (x \in B \wedge x \notin A)$. Suppose the contradiction, that is, $\forall x (x \in B \Longrightarrow x \in A)$, which is impossible since $(A \subseteq B \equiv \forall x (x \in A \Longrightarrow x \in B)) \wedge A \neq B$.

According to what's proven in the book, $A \subsetneq B \wedge B \subsetneq C \implies A \subseteq C$.

Now we prove that $\exists x(x \in C \wedge x \notin A)$. Since $x \in A \implies x \in B$, $x \notin B \implies x \notin A$. Because $B \subsetneq C$, $\exists x(x \in C \wedge x \notin B)$, and thus for such x, $x \notin A$. Then $A \neq C$.

So $A \subsetneq C$. □

Axiom 3.5 (1) Because $x \in \{x \in A : P(x)\} \Rightarrow x \in A$.

(2) Because both $\in$ and $P(x)$ obey the axiom of substitution.

Exercise 3.1.5

Proof. First we prove that $A \subseteq B \equiv A \cup B = B$. On one hand,

$$\begin{aligned} A \subseteq B \equiv \\ \forall x(x \in A \implies x \in B) \implies \\ \forall x((x \in A \vee x \in B) \implies x \in B) \equiv \\ A \cup B = B \end{aligned}$$

.

On the other hand,

$$\forall x((x \in A \vee x \in B) \implies x \in B) \implies \forall x(x \in A \implies x \in B)$$

. The statement is therefore proven.

Then we prove that $A \subseteq B \equiv A \cap B = A$. On one hand,

$$\begin{gathered} (A \cap B = A \equiv \forall x(x \in A \wedge x \in B \equiv x \in A)) \implies \\ (\forall x(x \in A \Rightarrow x \in B) \equiv (A \subseteq B)) \end{gathered}$$

.

On the other hand,

$$\forall x(x \in A \wedge x \in B \implies x \in A)$$

is always true (Vacuously true if $x \notin B$).

Logical equality is transitive, and thus all of the three statements are equal. □

Proposition 3.1.28 (Exercise 3.1.6)

Proof. (a) The two are identical to

$$\forall x(x \in A \vee x \in \varnothing \equiv x \in A)$$

, and

$$\nexists x(x \in A \wedge x \in \varnothing)$$

, which are all true since $\forall x(x \notin \varnothing)$.

(b) We have $A \subseteq X$. According to what we have proven in Exercise 3.1.5, the two statements are all true.

(c) Obvious since

$$\forall x(x \in A \vee x \in A \equiv x \in A)$$

and

$$\forall x(x \in A \wedge x \in A \equiv x \in A)$$

(d) All true since *logical or* and *logical and* are commutative.

(e) See Lemma 3.1.13. I believe that this can be concluded by the fact that *logical or* and *logical and* are also associative.

(f) First we prove the latter. On one hand, suppose

$$x \in A \cup (B \cap C)$$

is ture.

If $x \in A$, then $x \in$ both $A \cup B$ and $A \cup C$, and thus $\in (A \cup B) \cap (A \cup C)$.

If $x \notin A$, then $x \in B \cap C$, then $x \in$ both $A \cup B$ and $A \cup C$, and thus $\in (A \cup B) \cap (A \cup C)$.

On the other hand, suppose

$$x \in (A \cup B) \cap (A \cup C)$$

is true.

If $x \in A$, obviously $x \in A \cup (B \cap C)$.

If $x \notin A$, then x must $\in B \cap C$, and thus also $\in A \cup (B \cap C)$.

Now we prove the former. On one hand, suppose

$$x \in A \cap (B \cup C)$$

is true.

If $x \in A \wedge x \in B$, then $x \in A \cap B$, and thus $\in (A \cap B) \cup (A \cap C)$.

If $x \notin A \vee x \notin B$, then

1. if $x \notin A$, this is impossible.
2. if $x \in A$, then $x \notin B$. But $x \in B \cup C$, so $x \in C$. And thus $x \in A \cap C \Rightarrow x \in (A \cap B) \cup (A \cap C)$.

On the other hand, suppose that

$$x \in (A \cap B) \cup (A \cap C)$$

is true.

First we can see that $x \in A$.

If $x \in B$, then $x \in B \cup C$, and thus $\in A \cap (B \cup C)$.

If $x \notin B$, then $x \in C$. So $x \in B \cup C$, and thus $\in A \cap (B \cup C)$.

(g) Now we prove the former: On one hand, suppose that

$$x \in A \cup (X - A)$$

.

If $x \in A$, then $x \in X$ since $A \subseteq X$.

If $x \notin A$, then $x \in X - A$, and thus also $\in X$.

On the other hand, suppose that

$$x \in X$$

If $x \in A$, then $x \in A \cup (X - A)$.

If $x \notin A$, then $x \in X - A$, and thus $\in A \cup (X - A)$.

(h) $x \in X - A$ requires $x \notin A$. So $\forall x(x \in A \cap (X - A))$ is always false. Thus

$$\forall x(x \in A \cap (X - A) \iff x \in \varnothing)$$

(vacuously true). □

Exercise 3.1.7

Proof. (1) $\forall x(x \in A \cap B \implies x \in A)$. Similarly, we can prove that $A \cap B \subseteq B$. (This can also be achieved via the commutativity).

(2) On one hand, suppose that

$$C \subseteq A \wedge C \subseteq B$$

is true. Then,

$$\forall x(x \in C \implies x \in A \wedge x \in B \implies x \in A \cap B)$$

.

On the other hand, suppose that

$$C \subseteq A \cap B$$

is true. Then,

$$\forall x(x \in C \Longrightarrow x \in A \wedge x \in B)$$

. That is, $C \subseteq A \wedge C \subseteq B$.

(3) It is immediately given by

$$\forall x(x \in A \Longrightarrow x \in A \cup B)$$

. Since $\cup$ is commutative, the latter case is proven.

(4) On one hand, suppose that $A \subseteq C \wedge B \subseteq C$ and let $x \in A \cup B$.

If $x \in A$, then $x \in C$.

If $x \notin A$, then $x \in B$, and thus $x \in C$.

On the other hand, suppose that $A \cup B \subseteq C$. Then,

$$\forall x(x \in A \Longrightarrow x \in A \cup B \Longrightarrow x \in C)$$

$$\forall x(x \in B \Longrightarrow x \in A \cup B \Longrightarrow x \in C) \qquad \square$$

.

Exercise 3.1.8

Proof. The former: On one hand, Suppose that

$$x \in A \cap (A \cup B)$$

.

If $x \in A$, then $x \in A$.

If $x \notin A$, this is impossible.

On the other hand, suppose that $x \in A$. Then $x \in A \wedge x \in (A \cup B)$, so $x \in A \cap (A \cup B)$.

The latter: On one hand, suppose that $x \in A \cup (A \cap B)$.

$$x \in A \Longrightarrow x \in A.$$

$$x \notin A \Longrightarrow x \in (A \cap B) \Longrightarrow x \in A$$

.

On the other hand, Suppose that $x \in A$, then $x \in A \cup (A \cap B)$. $\square$

Exercise 3.1.9

Proof.

Lemma 10.
$$\nexists x \forall B \forall A (x \in A \wedge x \in B \wedge A \cap B = \varnothing)$$

Proof. Suppose the contradiction: $x \in A \wedge x \in B \wedge A \cap B = \varnothing$, then $x \in A \cap B$, and thus $\in \varnothing$, which is impossible. □

The former: On one hand, suppose that $x \in A$. Then $x \notin B$ by Lemma 10. And
$$x \in A \implies x \in A \cup B \implies x \in X$$
. So $x \in (X - B)$.

On the other hand, suppose that $x \in (X - B)$, then $x \in A \cup B$. But $x \notin B$, so $x \in A$ by Lemma 10.

The latter is immediately proven since $\cap, \cup$ are commutative. □

Exercise 3.1.10

Proof. Firstly we prove that $(A - B) \cap (A \cap B) = \varnothing$.

$x \in (A \cap B)$ gives $x \in B$, but $x \in (A - B)$ gives $x \notin B$. So the two statements can not be true simultaneously. Which means
$$x \in (A - B) \cap (A \cap B) \implies x \in \varnothing$$

And obviously
$$x \in (A - B) \cap (A \cap B) \impliedby x \in \varnothing$$
.

Similarly we can conclude all of the three sets are disjoint by the fact that $\nexists x \in$ either two of the three sets.

Now we are showing that their union is $A \cup B$.

On one hand, suppose that
$$x \in (A - B) \cap (A \cap B) \cap (B - A)$$
. x can at most be in one of these sets since they are disjoint. If $x \in A$, then $x \in A \cup B$.

If $x \notin A$, then $x \in (B - A)$, and thus $x \in B$. So $x \in A \cup B$.

On the other hand, suppose that $x \in A \cup B$. Then x either

1. $\in A$, but $\notin B$, or
2. $\in B$, but $\notin A$, or
3. $\in$ both A, B.

If (1), then $x \in (A - B)$.
If (2), then $x \in (B - A)$.
If (3), then $x \in A \cap B$.
In conclusion, we can see that $x \in (A - B) \cap (A \cap B) \cap (B - A)$. □

Exercise 3.1.11

Proof. Let S be a set. Let $P(x, y)$ be a property pertaining to $x \in S$ and any object y, and is true iff $Q(x) \wedge y = x$, where $Q(x)$ is a property pertaining to $x \in S$.

According to Axiom 3.6, there exists a set Z, such that $y \in Z \equiv x \in S \wedge P(x, y)$, which means $y \in Z \equiv x \in S \wedge Q(x) \wedge x = y$. So is the axiom of specification proven. □

4 Russell's paradox

I think one major reason for building such a "cumbersome" axiom system is to restrict the way to construct sets. We can not construct just any set we want, there only exist certain kinds of sets.

Exercise 3.2.1

Proof. (Axiom 3.2) To prove the existence of the empty set, simply choose a property that is false for all objects.

(Axiom 3.3) To prove the existence of a *pair set*, say $\{a, b\}$, let $P(x)$ be a property pertaining to any object x, and is true iff $x = a \vee x = b$.

(Axiom 3.4) Let the property be $P(x) : x \in A \vee x \in B$.

(Axiom 3.5) Let the property be $Q(x) : x \in A \wedge P(x)$, where $P(x)$ is a property pertaining to elements of A.

(Axiom 3.6) Let the property be $Q(y) : P(x, y)$ is true for some $x \in A$. □

Exercise 3.2.2

Proof. (1) Suppose the contradiction: $\exists A(A \in A)$. Then by Axiom 3.3, construct a set $B := \{A\}$. A is the only element in B. A is a set. A is not disjoint from B, for $A \in A \wedge A \in B$.

(2) Suppose the contradiction: $A \in B \wedge B \in A$. Construct a set S : $\{A, B\}$. A is an element of S. A is a set. A is not disjoint from S, for $B \in A \wedge B \in S$. □

Exercise 3.2.3 On one hand, if Axiom 3.8 is true, we can choose a property $P(x)$ which is true for all objects. Thus we have Ω.

On the other hand, if there exists such a set as Ω, we can use Axiom 3.5 to construct any set we want from it. (e.g. If we want a set to have these elements: $a, b, \ldots$, we can let $P(x) := x = a \vee x = b, \vee \ldots$.)

5 Functions

In Example 3.3.3, Tao asked why $x' = x \Rightarrow f(x') = f(x)$. The reason is, the property $P(x, y)$ obeys the axiom of substitution. Thus, $P(x, y) \equiv P(x', y)$. According to definition, since $x' \in X$, y is unique.

In Example 3.3.9, Tao asked why all functions whose domain is $\varnothing$ and whose range is the same are equal. The reason is $x \in \varnothing \Longrightarrow f(x) = g(x)$ is vacuously true.

Exercise 3.3.1

Proof. The properties of equality are all true since in definition, we only use $f(x) = g(x)$, in which the $=$ obeys these rules, plus the fact that the output is unique.

Then the substitution:

$$\begin{aligned} f = \widetilde{f} \Longrightarrow \\ f(x) = \widetilde{f}(x) \Longrightarrow \\ g(f(x)) = g(\widetilde{f}(x)) \end{aligned}$$

. And then $\widetilde{g}(\widetilde{f}(x)) = g(\widetilde{f}(x)) = g(x)$. □

Exercise 3.3.2

Proof. The former: Suppose the contradiction:

$$\exists x \exists x'(g(f(x)) = g(f(x')) \wedge x \neq x')$$

Then,

$$\begin{aligned} g(f(x)) = g(f(x')) &\implies \\ f(x) = f(x') &\implies && (g \text{ is injective}) \\ x = x' & && (f \text{ is injective}) \end{aligned}$$

, which is impossible.

The latter: Suppose the contradiction:

$$\exists z \forall x(z \in Z \wedge g \circ f(x) \neq z)$$

Then, we can conclude that $\exists y \forall x(y \in Y \wedge y \neq f(x))$, since g is surjective. This is impossible as f is surjective. □

Exercise 3.3.3

Proof. **Attention:** Different interpretations for injectivity may result in different conclusions. I have asked a question at Stack Exchange regarding this problem.

Let the range be Y, and the function be f. Injectivity:

$$\forall x' \forall x((x \in \varnothing \wedge x' \in \varnothing) \implies (x \neq x' \implies f(x) \neq f(x')))$$

, which is always vacuously true.

Surjectivity:

$$\forall y(y \in Y \implies \exists x(x \in \varnothing \wedge f(x) = y))$$

, which is false if $Y \neq \varnothing$, and which is vacuously true if $Y = \varnothing$.

Bijective: True if $Y = \varnothing$. □

Exercise 3.3.4

Proof. The former: $f, \tilde{f}$ have the same range and domain.

$$\forall x(g \circ f = g \circ \tilde{f} \implies g(f(x)) = g(\tilde{f}(x)))$$

We know that g is injective, so $\forall x \in X, f(x) = \widetilde{f}(x)$. Thus $f = \widetilde{f}$.

It is not true if g is not injective. Consider an extreme condition, where g is constant. So whatever $f, \widetilde{f}$ are, $g \circ f = g \circ \widetilde{f}$ are always equal.

The latter: Suppose the contradiction:$g \neq \widetilde{g}$. $g, \widetilde{g}$ have the same range and domain. But they are not equal, so $\exists y(y \in Y \wedge g(y) \neq \widetilde{g}(y))$. Because f is surjective, $\exists x(x \in X \wedge f(x) = y)$. However, $g \circ f(x) = \widetilde{g} \circ f(x)$, so this is impossible.

It is not true if f is not surjective. We can make $g(y) = \widetilde{g}(y)$ when $y = f(x)$, but as well make $g(y') \neq \widetilde{g}(y')$ if $\nexists x(y' = f(x))$. □

Exercise 3.3.5

Proof. Injectivity: Suppose the contradiction, that

$$\exists x \exists x'(x \neq x' \wedge f(x) = f(x'))$$

, which immediately gives

$$g(f(x)) = g(f(x'))$$

, and thus is impossible.

g has not to be also injective, because f being so ensures that an unique input x gives an unique input to g.

Surjectivity: If g is not surjective, then $\exists z \forall y(z \in Z \wedge y \in Y \wedge z \neq g(y))$ And whatever x is, $f(x) \in Y$, so $g(f(x)) \neq z$, which is a contradiction.

f has not to be surjective as long as its "real" domain is large enough to form the set Z through g. For example (Informal), let g be $z = |y|, \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$, and let f be $y = x, \mathbb{R}^+ \cup \{0\} \to \mathbb{R}$. □

Exercise 3.3.6

Proof. The latter: By definition, $P(y, x)$ of $x = f^{-1}(y)$ is $f(x) = y$. Substitute x with $f^{-1}(y)$, and here we have $f(f^{-1}(y)) = y$, where $y \in Y$.

The former: Let $y = f(x)$. According to what we have proven, $f(f^{-1}(y)) = y$. Substitute y with $f(x)$, we have $f(f^{-1}(f(x))) = f(x)$. Since that $f(x)$ is injective, we have $f^{-1}(f(x)) = x$.

Now we need to show that f^{-1} is bijective. Assume that it is not injective, thus $\exists x \exists x'(x \in Y \wedge x' \in Y \implies (x \neq x' \implies f^{-1}(x) = f^{-1}(x')))$. However, according to the latter conclusion, $f^{-1}(x) = f^{-1}(x') \implies x = x'$, a contradiction, so f^{-1} must be injective.

And it is also surjective. $\forall x \in X$, $\exists y \in Y, f^{-1}(y) = x$. According to the former conclusion, y is $f(x)$.

So now f^{-1} is bijective, and thus has its inverse. By definition, $P(x, y)$ of $y = (f^{-1})^{-1}(x)$ is $f^{-1}(y) = x$, where $x \in X$. According to the former conclusion, $f^{-1}(f(x)) = x$. Thus

$$f^{-1}(y) = f^{-1}(f(x)) \Longrightarrow y = f(x) \Longrightarrow (f^{-1})^{-1}(x) = f(x)$$

, which is true $\forall x \in X$. And since they have the same domain and range, $(f^{-1})^{-1} = f$. □

Exercise 3.3.7

Proof. Injectivity:

$$g \circ f(x) = g \circ f(x') \Longrightarrow f(x) = f(x') \Longrightarrow x = x'$$

Surjectivity: For each $z \in Z$, we need to find $x \in X$ such that $g \circ f(x) = z$. By the surjectivity of g, we can find $y \in Y$ such that $g(y) = z$. We can also find $a \in X$ such that $f(a) = y$ as f is surjective. So a is our desired x.

The $P(z, x)$ of $x = (g \circ f)^{-1}(z)$ is $z = g \circ f(x)$. Consider the following expression:

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

So $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Therefore, they are equal as they have the same domain and range. □

Exercise 3.3.8

Proof. (a) First they have the same domain and range. Finally,

$$\forall x(x \in X \Longrightarrow x = x \Longrightarrow \iota_{Y \to Z} \circ \iota_{X \to Y} = \iota_{X \to Z})$$

(b) On one hand, they have the same domain and range.

On the other hand,

$$\begin{aligned} f \circ \iota_{A \to A}(x) &= f(\iota_{A \to A}(x)) \\ &= f(x) \\ &= \iota_{B \to B}(f(x)) \\ &= \iota_{B \to B} \circ f(x) \end{aligned}$$

(c) It is easy to see that they have the same domain and range.

$$f \circ f^{-1}(b) = b = \iota_{B \to B}$$
$$f \circ f^{-1}(a) = a = \iota_{A \to A}$$

(d) It is easy to see that they have the same domain and range.
Let h be $h(x) = f(x)$, if $x \in X$, $h(x) = g(x)$, if $x \in Y$.
For each $x \in X$, $\iota_{X \to X \cup Y}(x) = x$, so $h(\iota_{X \to X \cup Y}(x)) = f(x)$.
Similarly we can prove $h(\iota_{Y \to X \cup Y}(x)) = g(x)$ for each $x \in Y$. □

6 Images and inverse Images

Definition 3.4.1 To prove that $f(S)$ is well-defined by using the axiom of specification, we need to apply it to set Y, not X. Let $P(y)$ be a property pertaining to each $y \in Y$, which is true iff $\exists x(x \in S \wedge f(x) = y)$. According to the axiom of specification, there exists a set that contains every $y \in Y$ such that $P(y)$ is true.

In some places where Tao asked "(Why?)", the reason is obvious, so I don't write them here.

Example 3.4.6 This is because

$$f^{-1}(f(\{-1, 0, 1, 2\})) = f^{-1}(\{1, 0, 4\}) = \{-1, 1, 0, 2, -2\}$$

.

More generally, if f (whose domain is X, and whose range is Y) is not injective, then

$$\exists x \exists x'((x \in X \wedge x' \in X) \wedge (x \neq x' \wedge f(x) = f(x')))$$

. Let $D \subseteq X$ such that $x \in D \wedge x' \notin D$. Then $f(x) = f(x') \in f(D)$. And thus $x, x' \in f^{-1}(f(D)) \implies f^{-1}(f(D)) \neq D$.

Exercise 3.4.1

Proof. $f^{-1}(V)$ may be interpreted in two different ways:

(1) Interpret $f^{-1}(V)$ as an inverse image, that is,

$$(\forall x \in X)(x \in f^{-1}(V) \equiv f(x) \in V)$$

$$(\forall x \notin X)(x \notin f^{-1}(V))$$

(2) Interpret $f^{-1}(V)$ as an image, where we regard f^{-1} as a function. So,

$$\forall x(\exists y(y \in V \land x = f^{-1}(y)) \equiv x \in f^{-1}(V))$$

We need to show that if the two statements are well-defined($x \in X$) , they are logically equivalent.

Let S_1 be the set defined in form (1), S_2 be the set defined in form (2). For every $x \in S_1$, $f(x) \in V$. Let $y' = f(x), x' = f^{-1}(y')$, then by definition (2) we have $x' \in S_2$. But $x' = x$, so $\forall x(x \in S_1 \implies x \in S_2)$.

On the other hand, for every $a \in S_2$, $\exists b \in V$, such that $a = f^{-1}(b)$. Then $a \in X$. $f(a) = f(f^{-1}(b)) = b \in V$, so $a \in S_1$. Thus, $S_1 = S_2$. □

Exercise 3.4.2 (1) Generally we can say $S \subseteq f^{-1}(f(S))$ but we cannot say that they are equal; (2) we can say $f(f^{-1}(U)) \subseteq U$ but we cannot say that they are equal.

Proof. (1) $x \in S \implies f(x) \in f(S) \implies x \in f^{-1}(f(S))$. However, it is possible that $\exists x(x \in X \land x \notin S \land f(x) \in f(S))$

(2)

$$x \in f^{-1}(U) \implies f(x) \in U \implies (y \in f(f^{-1}(U)) \implies y \in U)$$

However, it is still possible that

$$\exists y(y \in U \land \forall x(x \in X \implies f(x) \neq y))$$

□

Exercise 3.4.3

Proof. (1)

$$x \in A \cap B \implies f(x) \in f(A) \land f(x) \in f(B) \implies f(x) \in f(A) \cap f(B)$$

$$y \in f(A \cap B) \equiv \exists x(x \in A \cap B \land f(x) = y)$$

So $y \in f(A) \cap f(B)$, thus $f(A \cap B) \subseteq f(A) \cap f(B)$.

(2)

$$x \in A \setminus B \implies f(x) \in f(A \setminus B)$$

$$y \in f(A) \setminus f(B) \implies \exists x(x \in A \land x \notin B \land f(x) = y)$$

So $y \in f(A \setminus B)$, thus $f(A) \setminus f(B) \subseteq f(A \setminus B)$.

(3) On one hand,

$$y \in f(A \cup B) \equiv \exists x(x \in A \cup B \wedge f(x) = y)$$

$$\begin{aligned} x \in A \cup B \Longrightarrow x \in A \vee x \in B \Longrightarrow \\ f(x) \in f(A) \vee f(x) \in f(B) \Longrightarrow f(x) \in f(A) \cup f(B) \end{aligned}$$

On the other hand,

$$y \in f(A) \cup f(B) \Longrightarrow \exists x((x \in A \vee x \in B) \wedge f(x) = y)$$

$$x \in A \vee x \in B \Longrightarrow x \in A \cup B \Longrightarrow f(x) \in f(A \cup B)$$

□

(1) $\subseteq$ can not be improved. Since it is possible that

$$\exists x \exists x'(x \in A \wedge x' \in B \wedge x \neq x' \wedge f(x) = f(x'))$$

(2) $\subseteq$ can not be improved. Since it is possible that

$$\exists x \exists x'(x \in A \setminus B \wedge x' \in B \wedge f(x) = f(x'))$$

Exercise 3.4.4

Proof. (1)

$$\begin{aligned} x \in f^{-1}(U \cup V) \equiv (x \in X \wedge f(x) \in U \cup V) \equiv \\ (x \in X \wedge (f(x) \in U \vee f(x) \in V)) \end{aligned}$$

$$\begin{aligned} x \in f^{-1}(U) \cup f^{-1}(V) &\equiv (x \in X \wedge f(x) \in U) \vee (x \in X \wedge f(x) \in V) \\ &\equiv (x \in X \wedge (f(x) \in U \vee f(x) \in V)) \end{aligned}$$

(2) and (3) can be proven in similar manners. □

Exercise 3.4.5

Proof. (1) On one hand, if $f(f^{-1}(S)) = S$ for every $S \subseteq Y$, then $f(f^{-1}(Y)) = Y$. That means, $y \in Y \implies \exists x(x \in f^{-1}(Y) \wedge f(x) \in Y)$. So even $f^{-1}(Y)$ is enough for f to be surjective. And $f^{-1}(Y) \subseteq X$, so f is surjective.

On the other hand, if f is surjective, then for each $S \subseteq Y$,

$$y \in S \implies \exists x(x \in X \wedge f(x) = y)$$

Such x are elements of $f^{-1}(S)$ of course, so $f(f^{-1}(S)) = S$.

(2) On one hand, we show that $\forall S(S \subseteq X \implies f^{-1}(f(S)) = S)$ implies that f is injective. Suppose the contradiction, that when

$$\forall S(S \subseteq X \implies f^{-1}(f(S)) = S)$$

, but f is not injective. Since f is not injective,

$$\exists x \exists x'(x \in X \wedge x' \in X \wedge x \neq x' \wedge f(x) = f(x'))$$

Let $S \subseteq X$ and $x \in S \wedge x' \notin S$. There is always such a set S. For example, we can let $S = X \setminus \{x'\}$. So we have $f^{-1}(f(S)) \neq S$ because $x' \in$ it.

On the other hand, if f is injective, then for every $S \subseteq X$, and for every $x \in S$, we have $f(x) \in f(S)$. And $f(x)$ are the only elements in $f(S)$, that is, $y \in f(S) \implies y = f(x)$ for some $x \in S$. So now we know that $S \subseteq f^{-1}(f(S))$. Moreover, for every $x' \in f^{-1}(f(S))$, $f(x') \in f(S)$. We can let $f(x') = y = f(x)$. As f is injective, $x = x'$, so $x' \in S$. That means $f^{-1}(f(S)) \subseteq S$. So $f^{-1}(f(S)) = S$. □

Exercise 3.4.6

Proof. **My own proof:** According to Axiom 3.10, we can construct the set X^X. Apply the axiom of replacement to each element of X^X, we construct a set Z such that

$$\forall x(x \in Z \equiv \exists f(f \in X^X \wedge x = f(X)))$$

Let $Y = \{\varnothing\} \cup Z$.

Now we prove that Y is the set we want. On one hand, for any $S \subseteq X$, if $S = \varnothing$, then $S \in Y$, as $Y = \{\varnothing\} \cup Z$.

If $S \neq \varnothing$, there exists a surjective function $g : X \to S$. $g \in X^X$, and $g(X) = S$, so $S \in Z$, and thus $S \in Y$. (To show the existence of g, for example, let $x \in X, g(x) = x$ if $x \in S$, and for $x \in X \wedge x \notin S$, $g(x)$ can be any element of X.)

On the other hand, for any $S' \nsubseteq X$, $\exists a(a \in S' \wedge a \notin X)$. To prove that $S' \notin Y$, we need to show that $\nexists f(f \in X^X \wedge S' = f(X))$. We know that $\nexists x(x \in X \wedge f(x) = a)$, so $a \notin f(X)$. Therefore $S' \neq f(X)$, so $S' \notin Y$.

Y is the set we want.

I posted a question here for verification for this proof. Thanks to answers of people at Stack Exchange so that my proof can be refined.

Proof By Tao's Hint: For each $S \subseteq X$, let a function f_S be $f_S(x) = 1$ if $x \in S$, and $f_S(x) = 0$ if $x \in X \wedge x \notin S$. Then $f_S^{-1}(\{1\})$ gives S.

Now we show that any element in $\{0,1\}^X$ is some f_S. Let $g \in \{0,1\}^X$. Then if $\forall x \in X, g(x) = 0$, then $g = f_\varnothing$. Otherwise, there exists a set that contains all x such that $g(x) = 0$ by axiom of specification, namely R. Then $g = f_R$.

On the other hand, each f_S is obviously an element of $\{0,1\}^X$.

Use the axiom of replacement, we construct a set Y such that

$$\forall x(x \in Y \equiv \exists f(f \in \{0,1\}^X \wedge x = f^{-1}(\{1\})))$$

According to what we have proven, Y is the set we want. □

Exercise 3.4.7

Proof. As stated by the previous exercise, there exists a set $\mathbb{X}$ whose elements are all subsets of X, and a set $\mathbb{Y}$ whose elements are all subsets of Y.

For every element $x \in \mathbb{X}$, apply the axiom of replacement to $\mathbb{Y}$, to obtain a set $S_x := \{y^x\}$ for every element $y \in \mathbb{Y}$.

According to the axiom of union, using $\mathbb{X}$ as the index set, we have the set

$$Z = \bigcup_{x \in \mathbb{X}} S_x$$

Apply again the axiom of union to Z to obtain R, which contains all elements of elements of Z. Now we show that R is the set we want.

On one hand, let f be an arbitrary function with the domain of $X' \subseteq X$, and the range of $Y' \subseteq Y$. We can see that $f \in {Y'}^{X'} \in S_{X'}$. ${Y'}^{X'}$ becomes an element of Z. And thus f becomes an element in R.

On the other hand, from the construction of R, we can see that R contains only these elements.

□

Exercise 3.4.8

Proof. Let A, B be two arbitrary sets. They are also objects as stated by Axiom 3.1. So according to Axiom 3.3, there exists a set $S = \{A, B\}$. By Axiom 3.11, we have a set Z such that

$$\forall x(x \in Z \equiv \exists X(X \in S \land x \in X))$$

Now we show that Z is the set we want. If $x \in A \lor x \in B$, then $\exists X(X \in S \land x \in X)$ is true. So $x \in Z$.

If $x \notin A \land x \notin B$, then $\forall X(X \in S \implies x \notin X)$, that is, $\exists X(X \in S \land x \in X)$ is false. So $x \notin Z$.

Z is therefore the set we want. □

Example 3.4.11 In (3.3), why do Tao choose some element β of I? This is because we need to apply the axiom of specification to A_β with the restriction $x \in A_\alpha$ for all $\alpha \in I$.

Exercise 3.4.9

Proof. This is quiet easy to prove. Let the left-handed side set be S, the RHS set be S'. For any $x \in S$, $x \in A_\alpha$ for all $\alpha \in I$. So $x \in A_{\beta'}$. And $x \in A_\alpha$ for all $\alpha \in I$. Therefore $x \in S'$.

It is nearly the same the prove $x \in S' \implies x \in S$. □

Exercise 3.4.10

Proof. For the sake of convenience, let $(\bigcup_{\alpha\in I} A_\alpha) \cup (\bigcup_{\alpha\in J} A_\alpha)$ be S, $\bigcup_{\alpha\in I\cup J} A_\alpha$ be S', $(\bigcap_{\alpha\in I} A_\alpha) \cap (\bigcap_{\alpha\in J} A_\alpha)$ be Z, $\bigcap_{\alpha\in I\cup J} A_\alpha$ be Z'.

(1) When $I, J \neq \varnothing$: On one hand,

$$x \in S \implies (x \in \bigcup_{\alpha\in I} A_\alpha \lor x \in \bigcup_{\alpha\in J} A_\alpha)$$

If $x \in \bigcup_{\alpha\in I} A_\alpha$, then $x \in \bigcup_{\alpha\in I\cup J} A_\alpha$. If $x \in \bigcup_{\alpha\in J} A_\alpha$, then $x \in \bigcup_{\alpha\in I\cup J} A_\alpha$.

On the other hand, if $x \in S'$, then there exists an object $a \in I \cup J$ such that $x \in A_a$. If $a \in I$ then $x \in x \in \bigcup_{\alpha\in I} A_\alpha \implies x \in S$. If $a \in J$ then $x \in x \in \bigcup_{\alpha\in J} A_\alpha \implies x \in S$.

When I, J are both empty, S, S' are all empty.

When there is only one of I, J is empty, say it is I, then $S = \varnothing \cup \bigcup_{\alpha\in J} = \bigcup_{\alpha\in J}$. And $S' = \bigcup_{\alpha\in\varnothing\cup J} A_\alpha = \bigcup_{\alpha\in J}$.

(2)

$$x \in Z \equiv \forall a(a \in I \Longrightarrow x \in A_a) \wedge \forall b(b \in J \Longrightarrow x \in A_b)$$

, which is equal to $\forall a(a \in I \cup J \Longrightarrow x \in A_a) \equiv x \in Z'$. □

Exercise 3.4.11

Proof. (1) Let the LHS be S, the RHS be S'.

$$\begin{aligned} x \in S \equiv \\ x \in X \wedge x \notin \bigcup_{\alpha \in I} A_\alpha \equiv \\ x \in X \wedge \forall a(a \in I \Longrightarrow x \notin A_a) \end{aligned}$$

$$\begin{aligned} x \in S' \equiv \\ \forall a(a \in I \Longrightarrow x \in X \setminus A_a) \equiv \\ x \in X \wedge \forall a(a \in I \Longrightarrow x \notin A_a) \end{aligned}$$

.

So $S = S'$.

(2) Let the LHS be Z, the RHS be Z'.

$$\begin{aligned} x \in Z \equiv \\ x \in X \wedge x \notin \bigcap_{\alpha \in I} A_\alpha \equiv \\ x \in X \wedge \neg(\forall a(a \in I \Longrightarrow x \in A_a)) \equiv \\ x \in X \wedge \exists a(a \in I \Longrightarrow x \notin A_a) \end{aligned}$$

$$\begin{aligned} x \in Z' \equiv \\ x \in X \wedge \bigvee_{\alpha \in I} (x \notin A_\alpha) \equiv \\ x \in X \wedge \exists a(a \in I \Longrightarrow x \notin A_a) \end{aligned}$$

Thus, $Z = Z'$ □

7 Cartesian products

Exercise 3.5.1

Proof. First we show that $(x, y) = \{\{x\}, \{x, y\}\}$ is a good definition. Let S_1 denote $(x_1, y_1) = \{\{x_1\}, \{x_1, y_1\}\}$, S_2 denote $(x_2, y_2) = \{\{x_2\}, \{x_2, y_2\}\}$.

On one hand, if $x_1 = x_2 \wedge y_1 = y_2$, then obviously $S_1 = S_2$ for they have the same elements.

On the other hand, if $S_1 = S_2$, then

$$\{x_1\} \in S_2 \wedge \{x_1, y_1\} \in S_2 \wedge \{x_2\} \in S_1 \wedge \{x_2, y_2\} \in S_1$$

. We have that

$$\begin{aligned}\{x_1\} \in S_2 &\equiv \{x_1\} = \{x_2\} \vee \{x_1\} = \{x_2, y_2\} \\ &\equiv x_1 = x_2 \vee x_1 = x_2 = y_2 \\ &\implies x_1 = x_2\end{aligned}$$

$$\begin{aligned}\{x_1, y_1\} \in S_2 &\equiv \{x_1, y_1\} = \{x_2\} \vee \{x_1, y_1\} = \{x_2, y_2\} \\ &\equiv x_1 = x_2 = y_1 \\ &\vee ((x_1 = x_2 \wedge y_1 = y_2) \vee (x_1 = y_2 \wedge y_1 = x_2))\end{aligned}$$

Similarly we have that

$$\begin{aligned}\{x_2, y_2\} \in S_1 &\equiv x_2 = x_1 = y_2 \\ &\vee ((x_2 = x_1 \wedge y_2 = y_1) \vee (x_2 = y_1 \wedge y_2 = x_1))\end{aligned}$$

We may notice that the red-colored text are two same statements. Thus from $\{x_1, y_1\} \in S_2$ and $\{x_2, y_2\} \in S_1$ we can always conclude that $y_1 = y_2$. Therefore, $S_1 = S_2 \implies x_1 = x_2 \wedge y_1 = y_2$.

Then we show that if X, Y are two sets, then $X \times Y$ is also a set. For each element $x \in X$, construct a set S_x, where we replace each element $y \in Y$ with (x, y). Then construct the set $\bigcup_{x \in X} S_x$. □

Exercise 3.5.2

Proof. Since x, y are two functions, they are equal means that $\forall 1 \le i \le n$, $x(i) = y(i)$. That is, $x_i = y_i, 1 \le i \le n$.

Now we show that $\prod_{1 \le i \le n} X_i$ is a set. Let set F be the set that contains all partial functions from $N = \{i \in \mathbb{N} : 1 \le i \le n\}$ to $X = \bigcup_{1 \le i \le n} X_i$ (Exercise 3.4.7). Use the axiom of specification, select such elements f from F that:

1. the element is surjective, and
2. its domain is N, and
3. $f(i) \in X_i$

, and use all of them to construct a set Z, which is the set we want. □

Exercise 3.5.3

Proof. The definition is entirely based on the equality of objects (e.g. $x = x'$). The proof is immediately done since this equality is reflective ($x = x$), symmetric ($x = x' \equiv x' = x$), and transitive ($x_0 = x_1 \wedge x_1 = x_2 \implies x_0 = x_2$). □

Exercise 3.5.4

Proof. (1)

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

(2)

$$\begin{aligned}(x, y) \in A \times (B \cap C) &\equiv x \in A \wedge y \in (B \cap C)\\ &\equiv x \in A \wedge (y \in B \wedge y \in C)\\ &\equiv (x \in A \wedge y \in B) \wedge (x \in A \wedge y \in C)\\ &\equiv ((x, y) \in A \times B) \wedge ((x, y) \in A \times C)\\ &\equiv (x, y) \in (A \times B) \cap (A \times C)\end{aligned}$$

(3)

$$\begin{aligned}(x, y) \in A \times (B \setminus C) &\equiv x \in A \wedge y \in (B \setminus C)\\ &\equiv x \in A \wedge (y \in B \wedge \neg(y \in C))\\ &\equiv (x \in A \wedge y \in B) \wedge \neg(x \in A \wedge y \in C)\\ &\text{(The statement } x \in A \text{ implies } \neg(x \in A \wedge y \in C) \implies \neg(y \in C))\\ &\equiv ((x, y) \in A \times B) \wedge \neg((x, y) \in A \times C)\\ &\equiv (x, y) \in (A \times B) \setminus (A \times C)\end{aligned}$$

□

Exercise 3.5.5

Proof. (1)

$$\begin{aligned}(x,y)\in(A\times B)\cap(C\times D)&\equiv(x,y)\in(A\times B)\wedge(x,y)\in(C\times D)\\&\equiv(x\in A\wedge y\in B)\wedge(x\in C\wedge y\in D)\\&\equiv(x\in A\wedge x\in C)\wedge(y\in B\wedge y\in D)\\&\equiv x\in A\cap C\wedge y\in B\cap D\\&\equiv(x,y)\in(A\cap C)\times(B\cap D)\end{aligned}$$

(2) It is not true since

$$\begin{aligned}(x,y)\in(A\times B)\cup(C\times D)&\equiv(x,y)\in(A\times B)\vee(x,y)\in(C\times D)\\&\equiv(x\in A\wedge y\in B)\vee(x\in C\wedge y\in D)\\&\not\Leftrightarrow(x\in A\vee x\in C)\wedge(y\in B\vee y\in D)\end{aligned}$$

Generally

$$(x\in A\wedge y\in B)\vee(x\in C\wedge y\in D)\Longrightarrow(x\in A\vee x\in C)\wedge(y\in B\vee y\in D)$$

, but

$$(x\in A\vee x\in C)\wedge(y\in B\vee y\in D)\not\Rightarrow(x\in A\wedge y\in B)\vee(x\in C\wedge y\in D)$$

.

(3) It is not true since

$$\begin{aligned}(x,y)\in(A\times B)\setminus(C\times D)&\equiv(x,y)\in(A\times B)\wedge(x,y)\notin(C\times D)\\&\equiv(x\in A\wedge y\in B)\wedge(x\notin C\vee y\notin D)\\&\not\Leftrightarrow(x\in A\wedge x\notin C)\wedge(y\in B\wedge y\notin D)\end{aligned}$$

□

Exercise 3.5.6

Proof. (1) On one hand, if $A\subseteq C$ and $B\subseteq D$, then

$$\begin{aligned}(x,y)\in A\times B&\equiv x\in A\wedge y\in B\\&\Longrightarrow x\in C\wedge y\in D\\&\Longrightarrow(x,y)\in C\times D\end{aligned}$$

, which means $A\times B\subseteq C\times D$.

On the other hand, if $A \times B \subseteq C \times D$, but we suppose that

$$\neg(A \subseteq C \wedge B \subseteq D)$$

. We only consider that $A \nsubseteq C$, the other situations are similar. Then $\exists x(x \in A \wedge x \notin C)$. Let $p = (x, y)$, where $y \in B$, then $p \in A \times B$. But $x \notin C$, so $p \notin C \times D$, a contradiction. Therefore,

$$A \times B \subseteq C \times D \Longrightarrow A \subseteq C \wedge B \subseteq D$$

(2) On one hand, if $A = C \wedge B = D$, then

$$\begin{aligned}(x, y) \in A \times B &\equiv x \in A \wedge y \in B \\ &\equiv x \in C \wedge y \in D \\ &\equiv (x, y) \in C \times D\end{aligned}$$

.

On the other hand, if $A \times B = C \times D$, but we suppose that $\neg(A = C \wedge B = D)$. We only consider that $A \neq C$, the other situations are similar. Then we only consider $\exists x(x \in A \wedge x \notin C)$, for the other situations are similar.

(3) It is easy to prove that $X \times \varnothing = \varnothing$ and $\varnothing \times X = \varnothing$. Let $A = \varnothing$, we can see that even if $B \nsubseteq D$, $A \times B \subseteq C \times D$.

Let $A = D = \varnothing$, then even if $A \neq C$, $A \times B = C \times D$. □

Exercise 3.5.7

Proof. Existence: Let $h(t) := (f(t), y(t))$. It is easy to verify that $h(t) \in X \times Y$, and that given a $t \in Z$, $h(t)$ is unique. Therefore, h is a function. And it is obvious that $\pi_{X \times Y \to X} \circ h = f$ and that $\pi_{X \times Y \to Y} \circ h = g$.

Uniqueness: $\pi_{X \times Y \to X} \circ h = f$ and $\pi_{X \times Y \to Y} \circ h = g$ imply that if there is another function h' that satisfies the requirements, then $h'(t) = h(t)$. So h is unique. □

Exercise 3.5.8

Proof. On one hand, if for some $i, X_i = \varnothing$, then

$$\forall (x_i)_{1 \leq i \leq n} (\bigwedge_{i=1}^{n} x_i \in X_i \equiv (x_i)_{1 \leq i \leq n} \in \varnothing)$$

, which means that $\varnothing = \prod_{i=1}^{n} X_i$.

On the other hand, if $\prod_{i=1}^{n} X_i = \varnothing$ but we suppose that $X_i \neq \varnothing$. Then for each i, $\exists x_i \in X_i$. We thus have a tuple $(x_i)_{1 \leq i \leq n}$, which should be an element of $\prod_{i=1}^{n} X_i$. Therefore we have a contradiction. □

Exercise 3.5.9

Proof. On one hand, let $x \in (\bigcup_{\alpha \in I} A_\alpha) \cap (\bigcup_{\beta \in J} B_\beta)$. Then

$$\exists a(a \in I \wedge x \in A_a) \wedge \exists b(b \in J \wedge x \in B_b)$$

It is obvious that $x \in A_a \cap B_b$ and that $(a, b) \in I \times J$. Therefore

$$x \in \bigcup_{(\alpha,\beta) \in I \times J} (A_\alpha \cap B_\beta)$$

.

On the other hand, let $x \in \bigcup_{(\alpha,\beta) \in I \times J}(A_\alpha \cap B_\beta)$. Then

$$\begin{aligned} \exists (a, b) \in I \times J(x \in A_a \cap B_b) &\Longrightarrow x \in A_a \wedge x \in B_b \\ &\Longrightarrow x \in \bigcup_{\alpha \in I} A_\alpha \wedge x \in \bigcup_{\beta \in J} B_\beta \\ &\Longrightarrow x \in (\bigcup_{\alpha \in I} A_\alpha) \cap (\bigcup_{\beta \in J} B_\beta) \end{aligned}$$

□

Exercise 3.5.10

Proof. We denote $\tilde{f}$ as f', the graph of f as G, and the graph of f' as G' for the sake of simplification.

(1) On one hand, if $f = f'$, then for every $(x, f(x)) \in G$, we can find $(x, f'(x)) \in G'$, and obviously $(x, f(x)) = (x, f'(x))$, and vice versa.

On the other hand, if $G = G'$, then for each $(x, f(x)) \in G$, $(x, f(x)) \in G'$. Note that each element of G' obeys the form $(x, f'(x))$, so $f(x) = f'(x)$ for every $x \in X$, that is, $f = f'$.

(2) Existence: Let $f(x)$ be such a value that $(x, f(x)) \in G$. Thus the value is unique, so f is a function. According to its definition, the graph of f is G.

Uniqueness: As proven in (1), if f, f' have the same graph, then they are equal. □

Exercise 3.5.11 I think this exercise is meaningless. Lemma 3.4.6 is proven by the fact that X^Y exists, which depends on Axiom 3.10. Then the exercise asks us to prove Axiom 3.10 using Lemma 3.4.6. So I looked up some books about set theory and found out that the power set axiom is essentially Lemma 3.4.6, not Axiom 3.10.

Nevertheless, here is the proof:

Proof. Let set Z contains all subsets of $X \times Y$. The specify such element in Z that obey the vertical line test, and let them form the set S. According to the previous exercise, for each element in S, there exists an unique function whose graph is the element. Then we replace all elements in S with these functions to construct the set F. Obviously, each element in F is a function with the domain X and the range Y.

Now we show that every function f from X to Y is in F. Denote the graph of f as G. We know that G obeys the vertical line test and $G \subseteq X \times Y$, so $G \in S$. Since G is the graph of f, $f \in F$. □

Exercise 3.5.12 I am confused by this exercise. It seems that simply applying induction to a can solve the problem, just like what we did in Proposition 2.1.16. What is wrong?

By the way, according to the corrections, edit the exercise as the following:

> Let X be an arbitrary set containing at least an element c and obeys the Peano axioms. Let f be a function from $N \times X$ to X. ...
>
> Show that there exists an unique function a from X to X such that
> $$a(0) = c$$
> and
> $$a(n++) = f(n, a(n)), \forall n \in X$$
> ...
>
> such that $a_N(0) = c$ and $a_N(n++) = f(n, a_N(n))$ ...

Note that all properties (e.g. orders, addition) in section 2 are deduced from the Peano axioms and their definitions. Since X obeys these rules, we use such properties on elements of X without proof.

The proof is now reserved for further research.

Proof. □

Exercise 3.5.13

Proof. Use induction.

Existence: We need to prove that for all $n \in \mathbb{N}$, $f(n)$ is defined. Use induction: $f(0) = 0'$ is define. And the definition is unique for 0 is not the successor of any natural number. Now suppose that $f(n) = n'$ is defined, then $f(S(n)) = S'(f(n)) = S'(n')$ is also defined. The definition is also unique. So we know that f exists.

Injectivity: We need to prove that $f(m) = f(n) \implies m = n$. If $f(m) = f(n)$, then $m' = n'$, and thus $m = n$.

Surjectivity: Use induction: The basic case is, for $0' \in \mathbb{N}'$, $f(0) = 0'$.

Now suppose that for $n' \in \mathbb{N}'$, we can find $n \in \mathbb{N}$ such that $f(n) = n'$, then for $S'(n')$, we have $f(S(n)) = S'(n')$. We can close the induction now. □

8 Cardinality of Sets

Exercise 3.6.1

Proof. Reflexivity: Let $f(x) := x, X \to X$. f is bijective since $f^{-1}(x) = x$ exists.

Symmetry: If X, Y have the same cardinality, then $\exists f : X \to Y$ which is bijective. So f^{-1} exists, and is also a bijection. Thus Y, X have the same cardinality. Since then, we can say that two sets have the same cardinality without caring about the order.

Transitivity: If X, Y have the same cardinality, and Y, Z also have the same cardinality, then there exist two bijections: $f : X \to Y$ and $g : Y \to Z$. It is easy to verify that $g \circ f$ is also a bijection and is from X to Z (See Exercise 3.3.7). □

Remark 3.6.6 It is $f(n) := S(n)$. We are now proving something stronger

Lemma 11. *For any natural number m, n, $\{i \in \mathbb{N} : 0 \leq i \leq n\}$ and $\{i \in \mathbb{N} : m \leq i \leq n + m\}$ have the same cardinality.*

Proof. Use induction on m. When $m = 0$, the statement is obviously true. Simply give the function $f(n) := n$.

Suppose that for some m, we have proven the statement. Then there exists a bijection:

$$f : \{i \in \mathbb{N} : 0 \leq i \leq n\} \to \{i \in \mathbb{N} : m \leq i \leq n + m\}$$

. Let g be a function from $\{i \in \mathbb{N} : 0 \leq i \leq n\}$ to $\mathbb{N}$ such that $g(x) = S(f(x))$. We prove that g is a bijection from $\{i \in \mathbb{N} : 0 \leq i \leq n\}$ to $\{i \in \mathbb{N} : S(m) \leq i \leq n + S(m)\}$.

First we prove that $g(n)$ always in $\{i \in \mathbb{N} : S(m) \leq i \leq n + S(m)\}$, which is immediately given by the fact that addition preserves order.

Surjectivity: For any $a \in \{i \in \mathbb{N} : S(m) \leq i \leq n + S(m)\}$, a is positive. Then a is always some number's successor, that is $a = S(b) = b+1$ for some natural number b. Since addition preserves order, $b \in \{i \in \mathbb{N} : m \leq i \leq n + m\}$. f being surjective implies that there is some x in the domain such that $f(x) = b$, and $g(x) = f(x) + 1 = a$.

Injectivity: By cancellation law, $f(x) + 1 \neq f(x') + 1 \equiv f(x) \neq f(x') \equiv x \neq x'$.

We can now close the induction. $\square$

Lemma 3.6.9 Empty functions are not injective when the range is not empty (See Exercise 3.3.3).

Now we show that g is bijective:

Proof. Injectivity: f being injective implies that

$$\forall x \forall x'((x \in X \land x' \in X) \implies (f(x) = f(x') \Rightarrow x = x'))$$

For $a, a' \in X - \{x\}$, they also $\in X$. If $g(a) = g(a')$, then either directly $f(a) = f(a')$ or $f(a) - 1 = f(a') - 1$, which gives $f(a) = f(a')$. Thus $a = a'$. (Note that subtraction is not defined yet, see the footnote about this in the book).

Surjectivity: The surjectivity of f gives

$$(\forall 1 \leq i \leq n)(\exists a(a \in X \land f(a) = i))$$

.

If $f(x) = n$, then $g(a) = f(a)$ for all meaningful a. Then for $1 \leq i \leq n-1$, we can find a such that $a \in X \land a \neq x$, that is, $x \in X - \{x\}$. So $g(a)$ is meaningful, then g is surjective.

If $f(x) \neq n$, then $f(x) < n$. For those $1 \leq i < f(x)$, g is obviously surjective. For $n - 1 \geq i \geq f(x)$, since $S(i) \leq n$, $\exists a(a \in X \land f(a) = S(i))$. And we know that $S(i) \neq f(x)$, then $a \in X - \{x\}$. So $g(a) = f(a) - 1 = i$. $\square$

Exercise 3.6.2

Proof. On one hand, if X is empty, then we know that the empty function whose range is also empty is injective, (See Exercise 3.3.3) so its cardinality is 0.

On the other hand, if $\#X = 0$ but $X \neq \varnothing$, then there exists an bijection $f : X \to \varnothing$, which is impossible. $\square$

Exercise 3.6.3

Proof. When $n = 0$, this is vacuously true. The base case then becomes $n = 1$. We simply let $M = f(1)$.

Suppose that the statement for n is true. And for $1 \leq i \leq n$ we have the number M. Then $f(S(n))$ either $\geq$ or $< M$. On the former case, let $f(S(n))$ be M', and on the latter case, let $M' = M$. It is east to verify that M' is the number we want. $\square$

From now on we will denote $\{i \in \mathbb{N} : 1 \leq i \leq n\}$ as $\mathbb{N}_n$

Exercise 3.6.4

Proof. (a) Let $n = \#X$. There is an injective f from X to $\{i \in \mathbb{N} : 1 \leq i \leq n\}$. Let g be a function from $X \cup \{x\}$ to $\{i \in \mathbb{N} : 1 \leq i \leq n+1\}$ such that $g(a) = f(a)$ if $a \neq x$, and $g(x) = n+1$. Now we show that g is bijective.

Injectivity: We know that $\forall x \in X$, g is already injective. Since that $g(x) = n + 1 \neq g(a)$ for all $a \in X$, so g is injective on $X \cup \{x\}$.

Surjectivity: We know that $\forall i \in \{i \in \mathbb{N} : 1 \leq i \leq n\}$, we can find $a \in X \cup \{x\}$ such that $g(a) = i$. And we have $g(x) = n+1$, so $\forall a \in \{i \in \mathbb{N} : 1 \leq i \leq n+1\}$, we can find $a \in X \cup \{x\}$ such that $g(a) = i$.

(b) First we prove that if X, Y are disjoint, then $\#X + \#Y = \#(X \cup Y)$. Let f be a bijection from X to $\mathbb{N}_{\#X}$, and g be a bijection from Y to $\mathbb{N}_{\#Y}$. According to this Lemma, there exists a bijection h from $\mathbb{N}_{\#Y}$ to $\{i \in \mathbb{N} : \#X + 1 \leq i \leq \#X + \#Y\}$. Thus $h \circ g$ is also a bijection. Let u be a function from $X \cup Y$ to $\mathbb{N}_{\#X} \cup \{i \in \mathbb{N} : \#X + 1 \leq i \leq \#X + \#Y\}$. Now we show that u is bijective.

Injectivity: For $x \neq x'$ in the domain. If x, x' are both in X or Y, then $f(x) \neq f(x')$ is immediately given by the injectivity of f and $h \circ g$. If one of them is in X, and the other is in Y, then they can also never be equal because the ranges of the two functions are disjoint.

Surjectivity: It is easy to verify that the range is equal to $\mathbb{N}_{\#X+\#Y}$. For any y in the range, if $y \in$ the range of f, then u is surjective since f is, and if $y \in$ the range of $h \circ g$, u is surjective for the same reason. The range consists of only this two sets, so u is surjective on the whole range.

The proof is over. This also implies that $X \cup Y$ is finite. Now we need only to show that $\#(X \cup Y) < \#X + \#Y$ when X, Y are not disjoint. It is easy to see that

$$\begin{aligned}\#A + \#B &= \#(A - A\cap B) + \#(A\cap B) + \#(B - A\cap B) + \#(A\cap B)\\ &= (\#(A - A\cap B) + \#(A\cap B) + \#(B - A\cap B)) + \#(A\cap B)\\ &= \#(A\cup B) + \#(A\cap B)\\ &> \#(A\cup B)\end{aligned}$$

(c) If $X \subseteq Y \wedge X \neq Y$, then $\#(Y \setminus X) \neq 0$.

$$\#Y = \#X + \#(Y \setminus X) > \#X$$

.

If $X = Y$, then $\#(Y \setminus X) = 0$, and $\#Y$ becomes $\#X$.

(d) $f : X \to f(X)$ is always surjective. If f is also injective, then f is bijective. On this occasion, $\#f(X) = \#X$. If f is not injective, we can select a set $X' \subseteq X \wedge X' \neq X$, on which f is bijective. Then $\#X' = \#f(X') = \#f(X)$. According to (c), $\#X' < \#X$, so $\#f(X) < \#X$.

(e) Suppose that $\#Y = n$. Use induction on n.

When $n = 0$, Y is empty, then $\#(X \times Y) = 0 = \#X \times 0$. Here we additionally prove that when $n = 1$, this is also true for further usage. When $n = 1$, let $Y = \{a\}$. Then the bijection is $f(x) := (x, a), X \to X \times \{a\}$.

Suppose that we have proven for some n, $\#(X \times Y) = \#X \times \#Y$. Then when $\#Y = S(n)$, let $Y = Y \setminus \{x\} \cup \{x\}$, where $x \in Y$. Lemma 3.6.9 tells us that $\#(Y \setminus \{x\}) = S(n) - 1 = n$. And Exercise 3.5.4 tells us that $X \times Y = X \times (Y \setminus \{x\}) \cup X \times \{x\}$.

$$\begin{aligned}\#(X \times Y) &= \#(X \times (Y \setminus \{x\}) \cup X \times \{x\})\\ &= \#(X \times (Y \setminus \{x\})) + \#(X \times \{x\})\\ &= \#X \times n + \#X\\ &= \#X \times S(n)\end{aligned}$$

We can now close the induction.

(f) We should first define m^n for natural numbers m, n.

Definition 2.
- $m^0 = 1$,
- $m^{S(n)} = m^n \times m$

Suppose that $\#Y = m, \#X = n$. Use induction on n.

When $n = 0$, X is empty, then Y^X has one function $f : \varnothing \to Y$.

Suppose that we have proven the statement for some n. Before we proceed the proof, we need some lemmas.

Lemma 12. *If X is not empty,*

$$\#Y^{X\setminus\{x'\}\cup\{x'\}} = \#Y^{X\setminus\{x'\}} \times \#Y$$

, where x' is an element of X.

Proof. By (e) we know that

$$\#Y^{X\setminus\{x'\}} \times \#Y = \#(Y^{X\setminus\{x'\}} \times Y)$$

.

Try to build a bijection between $Y^{X\setminus\{x'\}} \times Y$ and Y^X. Let $f' \in Y^X$. Let h be a function from Y^X to $Y^{X\setminus\{x'\}} \times Y$ such that

$$h(f') = (f, f'(x')),$$

where $f(x) := f'(x)$ when $x \neq x'$. Now we show that h is bijective.

Injectivity: If ${f_1}' \neq {f_2}'$, then

$${f_1}'(x') \neq {f_2}'(x') \vee \exists x(x \neq x' \wedge {f_1}'(x) \neq {f_2}'(x))$$

That is,

$${f_1}'(x') \neq {f_2}'(x') \vee f_1 \neq f_2,$$

which means

$$(f_1, {f_1}'(x')) \neq (f_2, {f_2}'(x')).$$

Surjectivity: For any $(f, a) \in Y^{X\setminus\{x'\}} \times Y$, let f' be f if $x \neq x'$, and $f'(x') = a$. Then $f' \in Y^X$ and $h(f') = (f, a)$.

So,

$$\#Y^X = \#(Y^{X\setminus\{x'\}} \times Y)$$

, which gives the lemma. □

Now we proceed the proof. Suppose that $\#X = n+1$, then $\#(X\setminus\{x'\}) = n$. By induction hypothesis, $\#(Y^{X\setminus\{x'\}}) = m^n$.

By the lemma,

$$\#Y^X = \#Y^{X\setminus\{x'\}\cup\{x'\}} = \#Y^{X\setminus\{x'\}} \times \#Y,$$

which equals to $m^n \times m$.

Now we can close the induction.

We have proven that the cardinality of power sets obeys the definition of power. This ensures the exercise. □

Exercise 3.6.9

Proof.

$$\begin{aligned}
\#A + \#B &= \#(A - A \cap B) + \#(A \cap B) + \#(B - A \cap B) + \#(A \cap B) \\
&= (\#(A - A \cap B) + \#(A \cap B) + \#(B - A \cap B)) + \#(A \cap B) \\
&= \#(A \cup B) + \#(A \cap B)
\end{aligned}$$

□

Part III
Mathematical Logic

9 Mathematical Statements

Exercise A.1.1 It is ((both X, Y are false) or (both X, Y are true)).

Exercise A.1.2 It is ((Y can be true even if X is false) or (Y can be false even if X is true)).

Exercise A.1.3 Yes. That's the definition of logical equivalent.

Exercise A.1.4 No. It is still possible that (even if X is false, Y is still true).

Consider a statement Y that satisfies:

1. If X, then Y.

2. If X is false, then Y or (exclusively) Y is false.

X, Y satisfy the description in the exercise, but they are not logical equivalent.

Exercise A.1.5 Yes. (Now I'm using the symbols defined in the A.2 for the sake of simplification) $X \iff Y$ means $X \implies Y \wedge \neg X \implies \neg Y$. So does Y and Z. So

$$(X \implies Y \implies Z \wedge \neg X \implies \neg Y \implies \neg Z) \implies \\ (X \implies Z \wedge \neg X \implies \neg Z)$$

, which means X and Z are logical equivalent.

(Note that $A \implies B$ can also be interpreted as a statement, meaning "If A is true, then B is true", just like we did in this example.)

Exercise A.1.6 Yes. $(X \implies Y \implies Z) \implies (X \implies Z)$.

Now we are proving that $Z \implies X \equiv \neg X \implies \neg Z$. Assume that $\neg X \wedge Z$. Since $Z \implies X$, we have a contradiction: $X \wedge \neg X$.

So $X \implies Z \wedge \neg X \implies \neg Z$. Therefore, X, Z are logical equivalent. Besides, we can conclude that $Y \implies X$. Thus X, Y are also logical equivalent.

10 Implication

Why did Tao say

> If X, then Y can also be written as "X can only be true when Y is true"

?

Assume the $X \wedge \neg Y$, but $X \implies Y$. So we have a contradiction $Y \wedge \neg Y$.

Define "when $x \neq 2$, $X : x = 2 \implies x^2 = 4$ is vacuously true" to ensure that X is always true regardless of the value of x.

My Own Exercise Most of the time, rules of implication are intuitive. But they can be confusing some times. So hereby I introduce an example which I encountered, and which has confused me for a short time.

Proposition 13. *Let P, Q, R be statements, thus*

$$P \implies (Q \implies R) \equiv (P \wedge Q) \implies R$$

Proof. In order to ascertain that two statements in the form of implication are logically equivalent, we must deeply understand what they are. At one time (that is, when all variables have definite value), a statement can only be either true or false, not both. And for a statement in the form of implication: $X \implies Y$, it is true iff (*If* X, then Y). We do not need to check it if X is not true.

Now back to the subject. To prove that the two are logically equivalent, we need to show that both (if the former is true, then the latter is true) and (if the latter is true, then the former is true).

Now suppose that $P \implies (Q \implies R)$ is true. That is, if P, then (if Q, then R). To show that under this condition the latter is true, we need to show that if P, Q are both true, then R is true. Suppose that $P \wedge Q$. Since P is true, (if Q, then R) is true. And we know that Q is true, so R is true. so the latter is true.

Now suppose that the latter is true. We need to verify that the former is also true under this condition. Suppose P is true, then we need to show $Q \implies R$ is true, that is, if Q, then R, and we furthermore suppose that Q is true. Now $P \wedge Q$ is true, so we have R is true. □

11 Nested Quantifiers

Exercise A.5.1 **(a)** Let P be $y^2 = x$ is true for each positive number y. And this statement means P is true for each positive number x.

Gaming metaphor: Me and my friend each randomly pick up a positive, say x and y, and check if $y^2 = x$.

The statement is false.

(b) There is at least one positive number x such that for every positive number y, $y^2 = x$.

Gaming metaphor: I have to pick up a positive number x such that whatever positive number y my friend picks up, $y^2 = x$ is always true.

The statement is false.

(c) There is at least two positive numbers x, y such that $y^2 = x$.

Gaming metaphor: Me and my friend each have to pick up a positive number, say x and y, such that $y^2 = x$.

The statement is true. For example, $1^2 = 1$.

(d) The statement $\exists x > 0, y^2 = x$ is true for every $y > 0$.

Gaming metaphor: For each positive number y my friend picks up, I have to pick up a positive number x such that $y^2 = x$.

The statement is true, because y^2 is also positive.

(e) There is at least one positive number y such that for every positive number x, $y^2 = x$ is always true.

Gaming metaphor: I have to find a number $y > 0$ such that regardless of what number x my friend picks up, $y^2 = x$ is always true.

The statement is false.

12 Equality

Exercise A.7.1

Proof. Let $F(x) := x + c$. By axiom 4, $F(a) = F(b)$. That is, $a + c = b + c$. Similarly, by letting $G(x) := a + x$, we have $a + c = a + d$, which, according to axiom 2, becomes $a + d = a + c$. Now we have $a + d = a + c, a + c = b + c$. According to axiom 3, we can conclude that $a + d = b + c$. $\square$

Table of Answers