Propositions of solutions for *Analysis I* by Terence Tao

Frédéric Santos

June 11, 2020

1. Introduction

No exercises in this chapter.

2. Starting at the beginning: the natural numbers

Exercise 2.2.1. — *Prove that the addition is associative, i.e. that for any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$.*

Let's use induction on c while keeping a and b fixed.

- Base case for $c = 0$: let's prove that $(a + b) + 0 = a + (b + 0)$. The left hand side is equal to $(a + b)$ according to Lemma 2.2.3. For the right hand side, if we apply the same lemma to the $(b + 0)$ part, we get $a + (b + 0) = a + b$. Both sides are equal to $a + b$, and the base case is thus done.
- Now let's suppose inductively that $(a + b) + c = a + (b + c)$: we have to prove that $(a + b) + c{++} = a + (b + c{++})$. Using Lemma 2.2.3 on the right hand side leads to $a + (b + c){++}$. Now consider the left hand side. Using still the same lemma, we get $(a + b) + c{++} = ((a + b) + c){++}$. By the inductive hypothesis, this is also equal to $(a + (b + c)){++}$. And, using the lemma 2.2.3 again, this also leads to $a + b + c{++}$. Therefore, both sides are equal to $a + b + c{++}$, and we have closed the induction.

Exercise 2.2.2. — *Let a be a positive number. Prove that there exists exactly one natural number b such that $b{++} = a$.*

Let's use induction on a.

- Base case for $a = 1$: we know that $b = 0$ matches this property, since $0{++} = 1$ by Definition 2.1.3. Furthermore, there is only one solution. Suppose that is another natural number b such that $b{++} = 1$. Then, we would have $b{++} = 0{++}$, which would imply $b = 0$ by Axiom 2.4. The base case is demonstrated.
- Let's suppose inductively that there is exactly one natural number b such that $b{++} = a$. We have to prove that there is exactly one natural number b' such that $b'{++} = a{++}$. By the induction hypothesis, and taking $b' = b{++}$, we have $b'{++} = (b{++}){++} = a{++}$. So there exists a solution, with $b' = b{++} = a$. Uniqueness is given by Axiom 2.4.: if $b'{++} = a{++}$, then we necessarily have $b' = a$.

Exercise 2.2.3. — *Let a, b, c be natural numbers. Prove the following properties of order for natural numbers:*

(a) Reflexivity: $a \geqslant a$. This is true since $a = 0 + a$ by Definition 2.2.1. By commutativity of addition, we can also write $a = a + 0$. So there is indeed a natural number n (with $n = 0$) such that $a = a + n$, i.e. $a \geqslant a$.

(b) Transitivity: if $a \geqslant b$ and $b \geqslant c$, then $a \geqslant c$. From the part $a \geqslant b$, there exists a natural number n such that $a = b + n$ according to Definition 2.2.11. A similar consideration for the part $b \geqslant c$ leads to $b = c + m$, m being a natural number. Combining together those two equalities, we can write $a = b + n = (c + m) + n = c + (m + n)$ by associativity (see Exercise 2.2.1). Then, $n + m$ being a natural number[1], the transitivity is demonstrated.

(c) Anti-symmetry: if $a \geqslant b$ and $b \geqslant a$, then $a = b$. From the part $a \geqslant b$, there exists a natural number n such that $a = b + n$. Similarly, there exists a natural number m such that $b = a + m$. Combining those two equalities leads to $a = b + n = (a + m) + n = a + (m + n)$. By cancellation law (Proposition 2.2.6), we can conclude that $0 = m + n$. According to Corollary 2.2.9, this leads to $m = n = 0$. Therefore, both m and n are null, meaning that $a = b + 0 = b$.

(d) Preservation of order: $a \geqslant b$ iff $a+c \geqslant b+c$. First, let's prove that $a+c \geqslant b+c \implies a \geqslant b$. If $a+c \geqslant b+c$, there exists a natural number n such that $a+c = b+c+n$. By cancellation law (Proposition 2.2.6)[2], we conclude that $a = b + n$, i.e. $a \geqslant b$, thus demonstrating the first implication. Conversely, let's suppose that $a \geqslant b$. There exists a natural number m such that $a = b + m$. Therefore, $a + c = b + m + c$ for any natural number c. Still by associativity and commutativity, we can rewrite this as $a + c = (b + c) + m$, i.e. $a + c \geqslant b + c$.

(e) $a < b$ iff $a{++} \leqslant b$. First, let's prove that $a{++} \leqslant b \implies a < b$. By definition of ordering, there exists a natural number n such that $b = (a{++}) + n$. By definition of addition, we can re-write: $b = (a{++} + n){++}$. Then, by commutativity and yet again by definition of addition, $b = (n + a{++}){++} = (n{++}) + (a{++})$. Thus, there exists a natural number $n{++}$ such that $b = n{++} + a$, which means that $b \geqslant a$. But we still have to prove that $a \neq b$. Let's suppose that $a = b$: in this case, by cancellation law, we would have $n{++} = 0$, which is impossible according to Axiom 2.3 (0 is not the successor of any natural number). Thus, $a \neq b$ et $b \geqslant a$: we have showed that $a < b$.

Conversely, let's prove that $a < b \implies a{++} \leqslant b$. Starting from that strict inequality, there exists a *positive*[3] natural number n such that $b = a + n$. By Lemma 2.2.10, since n is positive, it has one unique antecessor m, so that n can be written $m{++}$. Thus, $b = a + (m{++}) = (a + m){++} = (m + a){++} = m + (a{++}) = (a{++}) + m$. And, m being a natural number, this corresponds to the statement $b \geqslant a$.

(f) $a < b$ iff $b = a + d$ for some positive number d. First, let's prove the first implication, $a < b \implies b = a + d$ with $d \neq 0$. Since $a < b$, we have in particular $a \leqslant b$, and

[1] This is a trivial induction from the definition of addition.

[2] And also associativity and commutativity that we do not detail explicitly here.

[3] We make use here of the statement *(f)* demonstrated below. There is no circularity here, since proving *(f)* will not make use of *(e)*.

there exists a natural number d such that $b = a + d$. For the sake of contradiction, let's suppose that $d = 0$. We would have $b = a$, which would contradict the condition $a \neq b$ of the strict inequality. Thus, d is a positive number, which demonstrates the left-to-right implication.

Conversely, let's suppose that $b = a + d$, with $d \neq 0$. This expression gives immediately $a \leqslant b$. But if $a = b$, by cancellation law, this would lead to $0 = d$, a contradiction with the fact that d is a positive number. Thus, $a \neq b$ and $a \leqslant b$, which demonstrates $a < b$.

Exercise 2.2.4. — *Demonstrate three lemmas used to prove the trichotomy of order for natural numbers.*

(a) Show that we have $0 \leqslant b$ for any natural number b. This is obvious since, by definition of addition, $0 + b = b$ for any natural number b. This is precisely the definition of $0 \leqslant b$.

(b) Show that if $a > b$, then $a{+\!+} > b$. If $a > b$, then $a = b + d$, d being a positive natural number. Let's recall that $a{+\!+} = a + 1$. Thus, $a{+\!+} = a + 1 = b + d + 1 = b + (d + 1)$ by associativity of addition. Furthermore, $d+1$ is a positive natural number (by Proposition 2.2.8). Thus, $a{+\!+} > b$.

(c) Show that if $a = b$, then $a{+\!+} > b$. Once again, let's use the fact that $a{+\!+} = a + 1$. Thus, $a{+\!+} = a + 1 = b + 1$, and 1 is a positive natural number. This is the definition of $a{+\!+} > b$.

Exercise 2.2.5. — *Prove the strong principle of induction, formulated as follows: Let m_0 be a natural number, and let $P(m)$ be a property pertaining to an arbitrary natural number m. Suppose that for each $m \geqslant m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leqslant m' < m$, then $P(m)$ is also true. (In particular, this means that $P(m_0)$ is true, since in this case the hypothesis is vacuous.) Then we can conclude that $P(m)$ is true for all natural numbers $m \geqslant m_0$.*

First let's introduce a small lemma (similar to Proposition 2.2.12*(e)*).

Lemma. *For any natural number a and b, $a < b{+\!+}$ iff $a \leqslant b$.*

Proof. If $a < b{+\!+}$, then $b{+\!+} = a + n$ for a given positive natural n. By Lemma 2.2.10, there exists one natural number m such as $n = m{+\!+}$. Thus $b{+\!+} = a + m{+\!+}$, which can be rewritten $b{+\!+} = (a + m){+\!+}$ by Lemma 2.2.3[4]. By Axiom 2.4., this is equivalent to $b = a + n$, which can also be written $a \leqslant b$.

Conversely, if $a \leqslant b$, there exists a natural number m such as $b = a + m$. Thus, $b{+\!+} = (a + m){+\!+} = a + (m{+\!+})$ by Definition of addition (2.2.1). And, $m{+\!+}$ being a positive number, this means that $b > a$ according to Proposition 2.2.12*(f)*. □

Now we can prove the main proposition. Let $Q(n)$ be the property "$P(m)$ is true for all m such that $m_0 \leqslant m < n$". Let's induct on n.

- (Although this is not necessary,) we could consider two types of base cases. If $n < m_0$, $Q(n)$ is the proposition "$P(m)$ is true for all m such that $m_0 \leqslant m < n$", but there is no such natural number m. Thus, $Q(n)$ is vacuously true. If $n = m_0$, $P(m_0)$ is true by hypothesis, thus $Q(m_0)$ is also true.

[4] We could also rewrite $b + 1 = a + m + 1$ and then use the cancellation law.

- Now let's suppose inductively that $Q(n)$ is true, and show that $Q(n{++})$ is also true. If $Q(n)$ is true, $P(m)$ is true for all m such that $m_0 \leqslant m < n$. By hypothesis, this implies that $P(n)$ is true. Thus, $P(m)$ is true for any natural number m such that $m_0 \leqslant m \leqslant n$, i.e. such that $m_0 \leqslant m < n{++}$ according to the lemma introduced above. This is precisely $Q(n{++})$, and this closes the induction.

Thus, $Q(n)$ is true for all natural numbers n, which means in particular that $P(m)$ is true for any natural number $m \geqslant m_0$. This demonstrates the principle of strong induction.

EXERCISE 2.2.6. — *Let n be a natural number, and let $P(m)$ be a property pertaining to the natural numbers such that whenever $P(m{++})$ is true, then $P(m)$ is true. Suppose that $P(n)$ is also true. Prove that $P(m)$ is true for all natural numbers $m \leqslant n$; this is known as the* principle of backwards induction.

Terence Tao suggests to use induction on n. So let $Q(n)$ be the following property: "if $P(n)$ is true, then $P(m)$ is true for all $m \leqslant n$. The goal is to prove $Q(n)$ for all natural numbers n.

- Base case $n = 0$: here, $Q(n)$ means that if $P(0)$ is true, then $P(m)$ is true for any $m \leqslant 0$. By Definition 2.2.11, if $m \leqslant 0$, there exists a natural number d such that $0 = m + d$. But, by Corollary 2.2.9, this implies that both $m = 0$ and $d = 0$. Thus, the only number m such that $m \leqslant 0$ is 0 itself. Therefore, $Q(0)$ is simply the tautology "if $P(0)$ is true, then $P(0)$ is true"— a statement that we can safely accept. The base case is the, demonstrated.

- Let's suppose inductively that $Q(n)$ is true: we must show that $Q(n{++})$ is also true. If $P(n{++})$ is true, then by definition of P, $P(n)$ is also true. Then, by induction hypothesis, $P(m)$ is true for all $m \leqslant n$. We have showed that $P(n{++})$ implies $P(m)$ for all $m \leqslant n{++}$[5], which is precisely $Q(n{++})$. This closes the induction.

EXERCISE 2.3.1. — *Show that multiplication is commutative, i.e., if n and m are natural numbers, show that $n \times m = m \times n$.*

We will use an induction of n while keeping m fixed. However, this is not a trivial result, and even the base case is not straightforward. We will first introduce some lemmas.

Lemma. *For any natural number n, $n \times 0 = 0$.*

Proof. Let's induct on n. For the base case $n = 0$, we know by Definition 2.3.1 of multiplication that $0 \times 0 = 0$, since $0 \times m = 0$ for any natural number m.

Now let's suppose that $n \times 0 = 0$. Thus, $n{++} \times 0 = (n \times 0) + 0$ by Definition 2.3.1. But by induction hypothesis, $n \times 0 = 0$, so that $n{++} \times 0 = 0 + 0 = 0$. This closes the induction. □

Lemma. *For all natural numbers m and n, we have $m \times n{++} = (m \times n) + m$.*

[5] Actually, we use here yet another lemma, similar to the one introduced for the previous exercise. We use the fact that $m \leqslant n{++}$ is equivalent to $m = n{++}$ or $m \leqslant n$, which is easy to prove, but is not part of the "standard" results presented in the textbook.

Proof. Let's induct on m. The base case $m = 0$ is easy to prove: $0 \times n{+}{+} = 0$ by Definition 2.3.1 of multiplication, and $(0 \times n) + 0 = 0$.

Now suppose inductively that $m \times n{+}{+} = (m \times n) + m$, and we must show that

$$m{+}{+} \times n{+}{+} = (m{+}{+} \times n) + m{+}{+} \tag{1}$$

We begin by the left hand side: by Definition 2.3.1, $m{+}{+} \times n{+}{+} = (m \times n{+}{+}) + n{+}{+}$. By induction hypothesis, this is equal to $(m \times n) + m + n{+}{+}$.

Then, apply the definition of multiplication to the right hand side: $(m{+}{+} \times n) + m{+}{+} = (m \times n) + n + m{+}{+}$. The Lemma 2.2.3 and the commutativity of addition leads to $(m \times n) + n + m{+}{+} = (m \times n) + (n + m){+}{+} = (m \times n) + (m + n){+}{+} = (m \times n) + m + n{+}{+}$, which is equal to the left hand side.

Thus, both sides of equation (1) are equal, and we can close the induction. □

Now it is easier to prove the main result ($n \times m = m \times n$), by an induction on n.

- Base case $n = 0$: we already know by Definition 2.3.1 that $0 \times m = 0$. The first lemma introduced in this exercise also provides $m \times 0 = 0$. Thus, the base case is proved, since $0 \times m = m \times 0$ $(= 0)$.

- Now we suppose inductively that $n \times m = m \times n$, and we must prove that:

$$n{+}{+} \times m = m \times n{+}{+} \tag{2}$$

  By Definition 2.3.1 of multiplication, the left hand side is equal to $(n \times m) + m$.

  Using the lemma introduced above, the right hand side is equal to $(m \times n) + m$. By induction hypothesis, this is also equal to $(n \times m) + m$, which closes the induction.

EXERCISE 2.3.2. — *Show that positive natural numbers have no zero divisors, i.e. that* $nm = 0$ *iff* $n = 0$ *or* $m = 0$*. In particular, if* n *and* m *are both positive, then* nm *is also positive.*

We will prove the second statement first. Suppose, for the sake of contradiction, that $nm = 0$ and that both n and m are positive numbers. Since they are positive, by Lemma 2.2.10, there exists two (unique) natural numbers a and b such that $n = a{+}{+}$ and $m = b{+}{+}$. Thus, the hypothesis $nm = 0$ can also be written $(a{+}{+}) \times (b{+}{+}) = 0$. But, by Definition 2.3.1 of multiplication, $(a{+}{+}) \times (b{+}{+}) = (a \times b{+}{+}) + b{+}{+}$. Thus, we should have $(a \times b{+}{+}) + b{+}{+} = 0$. By Corollary 2.2.9, this implies that both $(a \times b{+}{+}) = 0$ and $b{+}{+} = 0$, which is impossible since zero is the successor of no natural number (Axiom 2.3).

Thus, we have proved that if n and m are both positive, then nm is also positive. The main statement can now be proved more easily.

- The right-to-left implication is straightforward: if $n = 0$, then by Definition of multiplication, $n \times m = 0 \times m = 0$. Since multiplication is commutative, we have the same result if $m = 0$.

- The left-to-right implication is exactly the contrapositive of the statement we have just proved above.

Exercise 2.3.3. — *Show that multiplication is associative, i.e., for any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.*

We will induct on c while keeping a and b fixed.

- Base case: for $c = 0$, we must prove that $(a \times b) \times 0 = a \times (b \times 0)$. The left hand side is equal to 0 by definition (and commutativity) of multiplication[6]. The right hand side is equal to $a0$, which is also 0. Both sides are null, and the base case is proved.
- Suppose inductively that $(a \times b) \times c = a \times (b \times c)$, and let's prove that $(a \times b) \times c{+}{+} = a \times (b \times c{+}{+})$. By definition (and commutativity) of multiplication, the left hand side is equal to $(a \times b) \times c + (a \times b)$. The right hand side is equal to $a \times (b \times c + b)$, and by distributive law (i.e., Proposition 2.3.4), this is also $a \times (b \times c) + a \times b$. But then, by inductive hypothesis, this can be rewritten $(a \times b) \times c + a \times b$, which is equal to the left hand side. The induction is closed.

Exercise 2.3.4. — *Prove the identity $(a + b)^2 = a^2 + 2ab + b^2$ for all natural numbers a, b.*

By distribution law (i.e., Proposition 2.3.4) and commutativity of multiplication, we have:

$$\begin{aligned}
(a+b)^2 &= (a+b)(a+b) = (a+b)a + (a+b)b \\
&= a \times a + b \times a + a \times b + b \times b \\
&= a^2 + a \times b + a \times b + b^2 \\
&= a^2 + 2ab + b^2
\end{aligned}$$

(For the last step, we recall that, by Definition 2.3.1, $2 \times m = m + m$ for any natural number m.)

Exercise 2.3.5. — *Euclidean algorithm. Let n be a natural number, and let q be a positive number. Prove that there exists natural numbers m, r such that $0 \leqslant r < q$ and $n = mq + r$.*

We will induct on n while remaining q fixed.

- Base case: if $n = 0$, there exists an obvious solution, namely $m = 0$ and $r = 0$.
- Suppose inductively that there exists m, r such that $n = mq + r$ with $0 \leqslant r < q$, and let's prove that there exists m', r' such that $n + 1 = m'q + r'$, with $0 \leqslant r' < q$.

  By the induction hypothesis, we have $n + 1 = mq + r + 1$. Since $r < q$, we have $r + 1 \leqslant q$ (this is Proposition 2.2.12). Thus, we have two cases here:

  1. If $r + 1 < q$, then $n + 1 = mq + (r + 1)$, with $0 \leqslant r + 1 < q$, so that choosing $m' = m$ and $r' = r + 1$ is convenient.
  2. If $r + 1 = q$, then $n + 1 = mq + q = (m + 1)q$ according to the distributive law (Proposition 2.3.4). Thus, choosing $m' = m + 1$ and $r' = 0$ is convenient.

This closes the induction.

[6]Actually, we use the second lemma introduced for the resolution of Exercise 2.3.1.

3. Set theory

Exercise 3.1.2. — *Using only Definition 3.1.4, Axiom 3.1, Axiom 3.2, and Axiom 3.3, prove that the sets $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, and $\{\varnothing, \{\varnothing\}\}$ are all distinct (i.e., no two of them are equal to each other).*

As a general reminder, we recall that sets are objects (Axiom 3.1) and the empty set $\varnothing$ is such that no object is an element of $\varnothing$, thus $\varnothing \notin \varnothing$.

1. First let's show that $\varnothing$ is different from all other sets. $\varnothing$ is an element of $\{\varnothing\}$ and $\{\varnothing, \{\varnothing\}\}$, and $\{\varnothing\}$ is an element of $\{\{\varnothing\}\}$. But none of those two objects are elements of $\varnothing$ (by Axiom 3.2), thus $\varnothing$ is different from all three other sets.

2. Then let's show that $\{\varnothing\} \neq \{\{\varnothing\}\}$. By Axiom 3.3, the singleton $\{\varnothing\}$ is such that $x \in \{\varnothing\} \iff x = \varnothing$. Similarly, the singleton $\{\{\varnothing\}\}$ is such that $x \in \{\{\varnothing\}\} \iff x = \{\varnothing\}$. But we already know that $\varnothing \neq \{\varnothing\}$ so there exists an object, $\varnothing$, which is a element of $\{\varnothing\}$ but not an element of $\{\{\varnothing\}\}$. Those sets are not equal.

3. Now let's show that $\{\varnothing\} \neq \{\varnothing, \{\varnothing\}\}$. By Axiom 3.3, the pair $\{\varnothing, \{\varnothing\}\}$ is such that x is an element of this set iff $x = \varnothing$ or $x = \{\varnothing\}$. Thus, $\{\varnothing\}$ is an element of $\{\varnothing, \{\varnothing\}\}$, but is not an element of $\{\varnothing\}$ (if it was, we should have $\varnothing = \{\varnothing\}$, which would be a contradiction with the first point of this proof). Those two sets are thus different.

4. Finally, we also have $\{\{\varnothing\}\} \neq \{\varnothing, \{\varnothing\}\}$. Indeed, we have $\varnothing \in \{\varnothing, \{\varnothing\}\}$ by Axiom 3.3. However, $\varnothing \in \{\{\varnothing\}\} \iff \varnothing = \{\varnothing\}$ by definition of a singleton, and we know this latest statement is false by the first point of this proof. Those two sets are also different.

Exercise 3.1.3. — *Prove the remaining claims in Lemma 3.1.13.*

Those claims are the following:

1. $\{a, b\} = \{a\} \cup \{b\}$. By Axiom 3.3, the pair $\{a, b\}$ is such that $x \in \{a, b\} \iff x = a$ or $x = b$. Let's consider three cases:

   - if $x = a$, $x \in \{a\}$ by Axiom 3.3, thus $x \in \{a\} \cup \{b\}$ by Axiom 3.4
   - if $x = b$, $x \in \{b\}$ by Axiom 3.3, thus $x \in \{a\} \cup \{b\}$ by Axiom 3.4
   - if $x \neq a$ and $x \neq b$, $x \notin \{a\}$ and $x \notin \{b\}$ by Axiom 3.3, so that $x \notin \{a\} \cup \{b\}$

   Thus, $\{a, b\}$ and $\{a\} \cup \{b\}$ have the same elements, and are equal.

2. $A \cup B = B \cup A$ for all sets A and B. Indeed, $x \in A \cup B \iff x \in A$ or $x \in B$. If $x \in A$, then $x \in B \cup A$ by Axiom 3.4. A similar argument holds if $x \in B$. Thus, in both cases, $x \in B \cup A$. We can show in a similar fashion that any element of $B \cup A$ is in $A \cup B$.

3. $A \cup \varnothing = \varnothing \cup A = A$. Since we've just showed that union is commutative, proving $A \cup \varnothing = A$ is sufficient. If $x \in A$, then $x \in A \cup \varnothing$. The converse is also true: if $x \in A \cup \varnothing$, then $x \in A$ or $x \in \varnothing$. But there is no element in $\varnothing$, so that we have necessarily $x \in A$. Thus, $A \cup \varnothing$ and A have the same elements: they are equal.

Exercise 3.1.4. — *Prove the remaining claims from Proposition 3.1.18.*

Let A, B, C be sets. Those claims are the following:

1. If $A \subseteq B$ and $B \subseteq A$, then $B = A$. According to Definition 3.1.4, two sets A and B are equal iff every element of A is an element of B, and vice versa. This is precisely the present claim.

2. If $A \subsetneq B$ and $B \subsetneq C$, then $A \subsetneq C$. Let x be an element of A. Since $A \subsetneq B$, x is also an element of B. And since $B \subsetneq C$, x is also an element of C. This holds for any x in A, and thus it demonstrates that $A \subset C$. Furthermore, since $A \subsetneq B$, there exists an element $y \in B$ which is not an element of A. As $B \subsetneq C$, y is also an element of C. Thus we have y, an element of C which is not in A. Combined to the previous result $A \subset C$, this demonstrates $A \subsetneq C$.

Exercise 3.1.5. — *Let A, B be sets. Show that the three statements $A \subseteq B$, $A \cup B = B$ and $A \cap B = A$ are logically equivalent (i.e., any one of them implies the other two).*

1. First, we prove that $A \subseteq B \implies A \cup B = B$. The first inclusion $B \subseteq A \cup B$ is trivial, since any element of a set B is always either in A or B. For the converse inclusion, let x be an element of $A \cup B$, and let's prove that $x \in B$. By Axiom 3.4, we have $x \in A$ or $x \in B$. If $x \in B$, the result holds. If $x \in A$, then we also have $x \in B$ since $A \subseteq B$. Thus, any element of $A \cup B$ is an element of B, which demonstrates the equality $A \cup B = B$.

2. Then, we prove that $A \cup B = B \implies A \cap B = A$. The first inclusion is trivial: if $x \in A \cap B$, then we always have $x \in A$. Now let's prove the converse inclusion: let x be an element of A; we must show that $x \in A \cap B$. If $x \in A$, then $x \in A \cup B$. But, by hypothesis, $A \cup B = B$, thus $x \in B$. So, $x \in A$ and $x \in B$, i.e. $x \in A \cap B$. This demonstrates the implication.

3. Finally, we prove that $A \cap B = A \implies A \subseteq B$. Let $x \in A$. Since $A \cap B = A$, we have $x \in A \cap B$. It follows that $x \in B$. We have proved that any element $x \in A$ is also an element of B, i.e. $A \subseteq B$.

Exercise 3.1.8. — *Let A, B be sets. Prove the absorption laws $A \cap (A \cup B) = A$ and $A \cup (A \cap B) = A$.*

1. The first inclusion $A \cap (A \cup B) \subseteq A$ is trivial: if $x \in A \cap (A \cup B)$ then in particular $x \in A$ by Definition 3.1.23 of an intersection[7]. Thus, we have $A \cap (A \cup B) \subseteq A$.

   For the converse inclusion, let x be an element of A. Then by definition $x \in A$, and we have also $x \in A \cup B$ since $x \in A$. Thus, $x \in A \cap (A \cup B)$, which proves the converse inclusion.

   Consequently, $A = A \cap (A \cup B)$.

2. First we show that $A \cup (A \cap B) \subseteq A$. Let $x \in A \cup (A \cap B)$. By Definition of an union, we have either $x \in A$, or $x \in A \cap B$. In both cases[8], we have $x \in A$, so that the inclusion is proved.

[7]This intersection is not empty since A and $A \cup B$ are not disjoint.

[8]If A and B are disjoint, then the first case $x \in A$ necessarily holds, since $x \in A \cup B$ is impossible.

Conversely, let $x \in A$. Then in particular, we have $x \in A \cup (A \cap B)$ by Definition of an union, because $x \in A$. Thus, $x \in A \cup (A \cap B)$.

We have proved that $A \cup (A \cap B) = A$.

EXERCISE 3.1.9. — *Let A, B, X be sets such that $A \cup B = X$ and $A \cap B = \varnothing$. Show that $A = X \backslash B$ and $B = X \backslash A$.*

The two sets A and B play a symmetrical role here, so that proving one of these two assertions is sufficient. For instance, we prove that $A = X \backslash B$.

- Let x be an element of A. Since $x \in A$, we also have $x \in A \cup B$ by definition of an union. But $A \cup B = X$, and then $x \in X$. On the other hand, we cannot have $x \in B$, because $x \in A$ and the sets A, B are disjoint. Thus, $x \in X$ and $x \notin B$, which means that $x \in X \backslash B$. We have proved that $A \subseteq X \backslash B$.

- Conversely, let x be an element of $X \backslash B$. By definition, this means that $x \in X$, i.e. $x \in A \cup B$, and $x \notin B$. Since $x \in A \cup B$, we have either $x \in A$ or $x \in B$, but we know that the latter is impossible. Thus, we have necessarily $x \in A$. We have proved that $X \backslash B \subseteq A$.

- We can conclude that $X \backslash B = A$.

EXERCISE 3.1.11. — *Prove that the axiom of replacement (Axiom 3.6) implies the axiom of specification (Axiom 3.5).*

Let's recall the axiom of replacement. Let A be a set. For every $x \in A$, and for every (abstract) object y, let $P(x, y)$ be a statement pertaining to both x and y, such that for any $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y : P(x, y) \text{ is true for some } x \in A\}$, such that for any object z,

$$z \in \{y : P(x, y) \text{ is true for some } x \in A\} \iff P(x, z) \text{ is true for some } x \in A$$

Now, let A be a set, x an element of A, and y an object. We accept the axiom of replacement, and show that it implies the axiom of specification.

Let $Q(x, y)$ be the property "$x = y$ and $P(x)$". According to the axiom of replacement, there exists a set $\{y : Q(x, y) \text{ is true for some } x \in A\}$ such that:

$$\begin{aligned}
& z \in \{y : Q(x, y) \text{ is true for some } x \in A\} \\
\iff & Q(x, z) \text{ is true for some } x \in A \\
\iff & x = z \text{ and } P(x) \text{ is true for some } x \in A \\
\iff & x = z \text{ and } P(z) \text{ is true for some } x \in A \text{ (by axiom of substitution)} \\
\iff & z \in A \text{ and } P(z) \text{ is true}
\end{aligned}$$

Thus, we have proved the existence of a set (the set $\{y : Q(x, y) \text{ is true for some } x \in A\}$) satisfying the axiom of specification: z belongs to this set iff $z \in A$ and $P(z)$ is true.

EXERCISE 3.3.1. — *Show that the definition of equality in Definition 3.3.7 is reflexive, symmetric and transitive. Also verify the substitution property: if $f_1, f_2 : X \to Y$ and $g_1, g_2 : Y \to Z$ are functions such that $f_1 f_2$ and $g_1 = g_2$, then $g_1 \circ f_1 = g_2 \circ f_2$.*

1. Definition 3.3.7 says that two functions f and g are equal if they have same domain X and range Y, and if, for all $x \in X$, $f(x) = g(x)$. This definition of equality is obviously reflexive, symmetric and transitive if we assume that the objects in the domain X and the range Y verify themselves the axioms of equality.

2. Since $f_1 = f_2$, they have same domain X and same range Y. This is also the case for g_1 and g_2, with domain Y and range Z. Thus, $g_1 \circ f_1$ has domain X and range Z, and so has $g_2 \circ f_2$. Furthermore, we have, for all $x \in X$:

$$\begin{aligned} g_2 \circ f_2(x) &= g_2 \circ f_1(x) \text{ (since } f_1 = f_2) \\ &= g_1 \circ f_1(x) \text{ (since } g_1 = g_2) \end{aligned}$$

which closes the demonstration.

Exercise 3.3.2. — *Let $f : X \to Y$ and $g : Y \to Z$ be functions. Show that if f and g are both injective, then so is $g \circ f$. Similarly, show that if f and g are both surjective, then so is $g \circ f$.*

First let's note that $g \circ f : X \to Z$.

1. Suppose that f and g are both injective, and let $x, x' \in X$. We have successively :

$$\begin{array}{rcl} g \circ f(x) & = & g \circ f(x') \\ g(f(x)) & = & g(f(x')) \\ f(x) & = & f(x') \text{ because } g \text{ is injective} \\ x & = & x' \text{ because } f \text{ is injective} \end{array}$$

We have showed that $g \circ f(x) = g \circ f(x') \Rightarrow x = x'$ for all $x, x' \in X$, i.e. that $g \circ f$ is injective.

2. Suppose that f and g are both surjective, and let be $z \in Z$. Since g is surjective, there exists $y \in Y$ such that $z = g(y)$. And since f is surjective, there exists $x \in X$ such that $y = f(x)$. Thus, combining those two results, there exists $x \in X$ such that $z = g(f(x))$. This means precisely that $g \circ f$ is surjective.

Exercise 3.3.3. — *When is the empty function injective? surjective? bijective?*

Let f be the empty function, i.e. $f : \varnothing \to Y$ for a certain range Y.

1. f is injective iff $x \neq x' \Rightarrow f(x) \neq f(x')$. This can be considered as vacuously true since there are no such x and x'. f can be considered as always injective, for any range Y.

2. f is surjective iff for any $y \in Y$, there exists $x \in \varnothing$ such that $y = f(x)$. We can clearly see that this assertion is false if $Y \neq \varnothing$, since any $y \in Y$ will have no antecedent in $\varnothing$. Conversely, if $Y = \varnothing$, the assertion is vacuously true, since there is no element in Y. Thus, f is surjective iff $Y = \varnothing$.

3. Since f is always injective, and is surjective iff $Y = \varnothing$, it is clear that f is bijective iff $Y = \varnothing$.

Exercise 3.3.4. — *Let $f : X \to Y$, $\tilde{f} : X \to Y$, $g : Y \to Z$, $\tilde{g} : Y \to Z$ be functions. Show that if $g \circ f = g \circ \tilde{f}$ and g is injective, then $f = \tilde{f}$. Is this statement true if g is not injective? Also, show that if $g \circ f = \tilde{g} \circ f$ and f is surjective, then $g = \tilde{g}$. Is this statement true if f is not surjective?*

This exercise introduces some cancellation laws for composition.

1. First, note that f and $\tilde{f}$ have same domain and range, which is the first condition for two functions to be equal (by Definition 3.3.7). Then, suppose that $g \circ f = g \circ \tilde{f}$ and g is injective. For the sake of contradiction, suppose that there exists $x \in X$ such that $f(x) \neq \tilde{f}(x)$. Since g is injective, we would thus have $g(f(x)) \neq g(\tilde{f}(x))$, which would be a contradiction to the hypothesis $g \circ f = g \circ \tilde{f}$. Thus, there is no x such that $f(x) = \tilde{f}(x)$, or in other words, $f = \tilde{f}$.

   This property is false if g is not injective. As a counterexample, one can think of $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x$, $\tilde{f} : \mathbb{R} \to \mathbb{R}$ with $\tilde{f}(x) = -x$, and $g : \mathbb{R} \to \mathbb{R}_+$ with $g(x) = |x|$.

2. As previously, first note that g and $\tilde{g}$ have same domain and range. Let be $y, y' \in Y$. Since f is surjective, there exist $x, x' \in X$ such that $y = f(x)$ and $y' = f(x')$ respectively. Since $g \circ f = g \circ \tilde{f}$, we have $g(f(x)) = g(f(x'))$, i.e. $g(y) = g(y')$. We have showed that, for any $y, y' \in Y$, we have $g(y) = g(y')$, which means that $g = \tilde{g}$.

   This statement is false if f is not surjective. For instance, let f be a constant function, e.g. $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 1$ for all x. Let $g, \tilde{g} : \mathbb{R} \to \mathbb{R}$ with $g(x) = 0$ and $\tilde{g}(x) = -x + 1$. We have $g(1) = \tilde{g}(1)$, i.e. $g(f(x)) = \tilde{g}(x)$ for all $x \in X$, but we obviously do not have $g = \tilde{g}$.

Exercise 3.3.5. — *Let $f : X \to Y$ and $g : Y \to Z$ be functions. Show that if $g \circ f$ is injective, then f must be injective. Is it true that g must also be injective? Show that if $g \circ f$ is surjective, then g must be surjective. Is it true that f must be surjective?*

1. If $g \circ f$ is injective, then for any given objects $x, x' \in X$, we have $g(f(x)) = g(f(x')) \implies x = x'$. For the sake of contradiction, suppose that f is not injective. In this case, there exist two elements $a, a' \in X$ such that $a \neq a'$ and $f(a) = f(a')$. We would thus have $g(f(a)) = g(f(a'))$ (axiom of substitution) and $a \neq a'$, which is incompatible with the hypothesis that $g \circ f$ is injective.

   Thus, $g \circ f$ injective implies that f is injective.

   However, g does not need to be injective. For instance, let's consider $X = \{1, 2\}$ and $Y = Z = \{1, 2, 3\}$. Let's define the function f as the mapping $f(1) = 1$, $f(2) = 2$. Let's define the function g as the mapping $g(1) = 1$, $g(2) = 2$, $g(3) = 2$. Here, f is injective, so is $g \circ f$, but g is not injective.

2. If $g \circ f$ is surjective, then for all $z \in Z$, there exists $x \in X$ such that $z = g(f(x))$. For the sake of contradiction, suppose that g is not surjective: then, there exists $z \in Z$ such that for all $y \in Y$, $z \neq g(y)$. In particular, for all $x \in X$, since $f(x) \in Y$, we would have $g(f(x)) \neq z$, which would be a contradiction with $g \circ f$ surjective.

   However, f does not need to be surjective. For instance, let's consider $X = Y = \{1, 2\}$ and $Z = \{1\}$. Let f be the mapping $f(1) = f(2) = 1$, and g be the mapping $g(1) = g(2) = 1$. Here, $g \circ f$ is surjective, but f is not.

Exercise 3.3.6. — *Let $f : X \to Y$ be a bijective function, and let $f^{-1} : Y \to X$ be its inverse. Verify the cancellation laws $f^{-1}(f(x)) = x$ for all $x \in X$ and $f(f^{-1}(y)) = y$ for all $y \in Y$. Conclude that f^{-1} is also invertible and has f as its inverse.*

Recall that, by definition, for all $y \in Y$, $f^{-1}(y)$ is the only element $x \in X$ such that $f(x) = y$.

1. Let a be an element of X, we thus have $f(a) \in Y$. Let's apply the definition to the element $y = f(a) \in Y$: by definition, $f^{-1}(f(a))$ is the only element $x \in X$ such that $f(x) = f(a)$. Since f is bijective, this implies $x = a$. We thus have proved that $f^{-1}(f(a)) = a$.

2. The proof for $f(f^{-1}(y)) = y$ is similar.

3. To prove that f^{-1} is also invertible, we need to prove that f^{-1} is bijective, i.e. injective and surjective.

   For any given $y \in Y$, since f is bijective, there exists exactly one $x \in X$ such that $y = f(x)$. Similarly, for any given $y' \in Y$, there exists exactly one $x' \in X$ such that $y' = f(x')$. In other words, $f^{-1}(y) = x$ and $f^{-1}(y') = x'$. Suppose that $f^{-1}(y) = f^{-1}(y')$. This can be written $x = x'$, which necessarily implies $f(x) = f(x')$ since f is a function (and by axiom of substitution). And this can also be written $y = y'$. We thus have proved that for any $y, y' \in Y$, $f^{-1}(y) = f^{-1}(y') \implies y = y'$. Thus, f^{-1} is injective.

   Furthermore, for any given $x \in X$, let's denote $y = f(x)$. Since f is bijective, this means that $f^{-1}(y) = x$. Thus, any $x \in X$ has a predecessor $y \in Y$ for f^{-1}, i.e. f^{-1} is surjective.

Exercise 3.3.7. — *Let $f : X \to Y$ and $g : Y \to Z$ be functions. Show that if f and g are bijective, then so is $g \circ f$, and we have $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

The first point is an immediate consequence of Exercise 3.3.2. We just have to show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Let be any given element $z \in Z$. Since g is bijective, there exists one single element $y \in Y$ such that $z = g(y)$, i.e. $y = g^{-1}(z)$. And since f is also bijective, there exists exactly one single element $x \in X$ such that $y = f(x)$, i.e. $x = f^{-1}(y) = f^{-1}(g^{-1}(z))$.

Thus, for every $z \in Z$, there exists exactly one $x \in X$ such that $g \circ f(x) = z$, and this element is $f^{-1}(g^{-1}(z))$. This means exactly that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exercise 3.4.1. — *Let $f : X \to Y$ be a bijective function, and let $f^{-1} : Y \to X$ be its inverse. Let V be any subset of Y. Prove that the forward image of V under f^{-1} is the same as the inverse image of V under f; thus the fact that both sets are denoted as f^{-1} will not lead to any inconsistency.*

Since "$f^{-1}(V)$" may refer to two different things here, let's first introduce some notations to avoid any confusion :

- Let F be the *forward image* of V under f^{-1}, i.e. $F = \{f^{-1}(y) \mid y \in V\}$.
- Let I be the *inverse image* of V under f, i.e. $I = \{x \in X \mid f(x) \in V\}$.

In this exercise we must show that $F = I$, so as to ensure that the two definitions of f^{-1} are equivalent. So, we will prove that $F \subseteq I$ and $I \subseteq F$.

1. Let be $x \in F$. Thus, there exists $y \in V$ such that $x = f^{-1}(y)$. By definition, this is equivalent to $f(x) = y$. But since $y \in V$, we can say that $f(x) \in V$. Thus, we have both $x \in X$ (beacuse $F \subseteq X$) and $f(x) \in V$, which means that $x \in I$.

2. Conversely, let be $x \in I$. By definition, this means that $x \in X$ and that $f(x) \in V$, i.e. there exists a certain element $y \in V$ such that $y = f(x) \in V$. This latter statement is equivalent to $x = f^{-1}(y)$. Thus, we have $x \in X$ and $x = f^{-1}(y)$ for a certain $y \in V$, which means that $x \in F$.

Exercise 3.4.2. — *Let $f : X \to Y$ be a function, let S be a subset of X and let U be a subset of Y. What, in general, can one say about $f^{-1}(f(S))$ and S? What about $f(f^{-1}(U))$ and U?*

This exercise gives a first taste of Exercise 3.4.5 below.

1. First consider $f^{-1}(f(S))$ and S.

   - Do we have $f^{-1}(f(S)) \subset S$? Generally, no. As an counterexample, let's consider $f(x) = x^2$ with $X = Y = \mathbb{R}$ and $S = \{0, 2\}$. We have $f^{-1}(f(S)) = f^{-1}(\{0, 4\}) = \{-2, 0, 2\}$. In this set, we have an element, -2, which is not an element of S.
   - Do we have $S \subset f^{-1}(f(S))$? Yes. Let be $x \in S$. Then, by definition, $f(x) \in f(S)$. So, $x \in X$ and is such that $f(x) \in f(S)$: this is precisely the definition of $x \in f^{-1}(f(S))$.
   - Conclusion: generally speaking, S and $f^{-1}(f(S))$ are not equal, but $S \subset f^{-1}(f(S))$.

2. Now consider $f(f^{-1}(U))$ and U.

   - Do we have $U \subset f(f^{-1}(U))$? Generally, no. As a counterexample, let's consider $f(x) = \sqrt{x}$ with $X = \mathbb{R}_+$, $Y = \mathbb{R}$ and $U = [-1, 1]$. We have $f(f^{-1}(U)) = f([0, 1]) = [0, 1]$, which is clearly not a subset of U.
   - Do we have $f(f^{-1}(U)) \subset U$? Yes. Let be $y \in f(f^{-1}(U))$. By definition, there exists $x \in f^{-1}(U)$ such that $y = f(x)$. But if $x \in f^{-1}(U)$, we have $f(x) \in U$. And since $y = f(x)$, this means that $y \in U$.
   - Conclusion: generally speaking, $U \neq f(f^{-1}(U))$, but $f(f^{-1}(U)) \subset U$.

Exercise 3.4.3. — *Let A, B be two subsets of X, and let be $f : X \to Y$. Show that $f(A \cap B) \subseteq f(A) \cap f(B)$, that $f(A) \backslash f(B) \subseteq f(A \backslash B)$, and $f(A \cup B) = f(A) \cup f(B)$. Is it true that, for the first two statements, the $\subseteq$ relation can be improved to $=$?*

Let's prove the three statements successively:

1. If $y \in f(A \cap B)$, then there exists $x \in A \cap B$ such that $f(x) = y$. Since $x \in A \cap B$, we have both $x \in A$ and $x \in B$, which implies $y = f(x) \in f(A)$ and $y = f(x) \in B$ respectively. Thus, $y \in f(A) \cap f(B)$, and we have proved that $f(A \cap B) \subseteq f(A) \cap f(B)$.

   However, the converse inclusion is false in general. For instance, let's consider the two sets $A = \{1, 2\}$, $B = \{2, 3\}$ and the (non injective) function f defined as the mapping $f(1) = 1$, $f(2) = 2$, $f(3) = 1$. We have $f(A) = \{1, 2\}$, $f(B) = \{1, 2\}$, thus $f(A) \cap f(B) = \{1, 2\}$. This is not a subset of $f(A \cap B) = f(\{2\}) = \{2\}$.

2. If $y \in f(A)\backslash f(B)$, then there exists $x_0 \in A$ such that $y = f(x_0)$, but we have $f(b) \neq y$ for all $b \in B$. Suppose that $x_0 \in B$: in this case, $f(x_0) \neq y$, a contradiction. Thus, $y = f(x_0)$ with $x_0 \in A\backslash B$, which proves that $f(A)\backslash f(B) \subseteq f(A\backslash B)$.

   However, the converse inclusion is false in general. For instance, let's consider the two sets $A = \{1, 2, 3\}$, $B = \{3\}$ and the function f defined as the mapping $f(1) = 1$, $f(2) = 2$, $f(3) = 1$. We have $f(A\backslash B) = \{1, 2\}$ but $f(A)\backslash f(B) = \{2\}$.

3. If $y \in f(A \cup B)$, then there exists $x \in A \cup B$ such that $y = f(x)$. If $x \in A$, then $f(x) \in f(A)$, which implies $x \in f(A) \cup f(B)$. There is an identical result if $x \in B$. Thus, $f(A \cup B) \subseteq f(A) \cup f(B)$.

   Conversely, if $y \in f(A) \cup f(B)$, then we have either $y \in f(A)$ or $y \in f(B)$ (or both). In the first case, there exists $x \in A$ such that $y = f(x)$. But since $x \in A$, we also have $x \in A \cup B$, so that $y \in f(A \cup B)$. The same result holds if $y \in B$. Thus, in both cases, $y \in f(A \cup B)$.