Propositions of solutions for *Analysis I* by Terence Tao

Frédéric Santos

November 26, 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 $a + c \geqslant b + c \Longrightarrow a \geqslant b$. 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 $a{+}{+} \leqslant b \Longrightarrow a < b$. 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 $a < b \Longrightarrow a{+}{+} \leqslant b$. 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, $a < b \Longrightarrow b = a + d$ 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 :

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

   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, $y \in f(A \cup B)$.

Exercise 3.4.4. — *Let be $f : X \to Y$ a function, and let A, B be subsets of Y. Show that $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, that $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$, and that $f^{-1}(A\backslash B) = f^{-1}(A)\backslash f^{-1}(B)$.*

We prove only the first statement here; since only very small adjustments are required in its proof to prove the last two ones.

- Let be $x \in f^{-1}(A \cup B)$. By definition, $f(x) \in A \cup B$, so that we have either $f(x) \in A$ or $f(x) \in B$.

  If $f(x) \in A$, then $x \in f^{-1}(A)$ by definition. This implies that $x \in f^{-1}(A) \cup f^{-1}(B)$.

  The same conclusion holds if $f(x) \in B$. Thus, we have demonstrated that $f^{-1}(A \cup B) \subseteq f^{-1}(A) \cup f^{-1}(B)$.

- For the conserve inclusion, let be $x \in f^{-1}(A) \cup f^{-1}(B)$. We have either $x \in \inf f(A)$ or $x \in f^{-1}(B)$.

  If $x \in f^{-1}(A)$, then $f(x) \in A$, and since $A \subset A \cup B$, we have $f(x) \in A \cup B$. This implies $x \in f^{-1}(A \cup B)$.

  The same conclusion holds if $x \in f^{-1}(B)$. Thus, $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$.

- This proves the equality $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Exercise 3.4.5. — *Let $f : X \to Y$ be a function. Show that $f^{-1}(f(S)) = S$ for every $S \subseteq Y$ iff f is surjective. Show that $f(f^{-1}(S)) = S$ for every $S \subseteq X$ iff f is injective.*

This exercise is a continuation of Exercise 3.4.2. Let's recall its results, that will reduce the amount of things to be proven here:

- we always have $f^{-1}(f(S)) \subseteq S$ for every $S \subseteq Y$, thus we just have to prove that f is surjective iff $S \subseteq f^{-1}(f(S))$ for every $S \subseteq Y$.

- we always have $S \subseteq f(f^{-1}(S))$ for every $S \subseteq X$, thus we just have to prove that f is injective iff then $f(f^{-1}(S)) \subseteq S$ for every $S \subseteq X$.

Let's prove those two statements.

1. Let f be surjective: let's show that $S \subseteq f(f^{-1}(S))$ for all $S \subseteq Y$. Let S be a subset of Y, and $y \in S$[9]. Since f is surjective, there exists $x \in X$ such that $y = f(x)$. Recall that $y \in S$: this means that$f(x) \in S$, i.e. $x \in f^{-1}(S)$. Thus, $y = f(x) \in f(f^{-1}(S))$. We have proved that, if f is surjective, $y \in S \Rightarrow y \in f(f^{-1}(S))$, i.e. $S \subseteq f(f^{-1}(S))$.

   Conversely, suppose that $S \subseteq f(f^{-1}(S))$ for every $S \subseteq Y$ and let's show that f is surjective. Let's choose $S = Y$: by hypothesis, we have $Y \subseteq f(f^{-1}(Y))$. Then, let be $y \in Y$. There exists $x \in f^{-1}(Y) \subseteq X$ such that $y = f(x)$. This means precisely that f is surjective.

   The first equivalence is proved.

2. Let f be injective, and $S \subseteq X$. Let be $x \in f^{-1}(f(S))$. Thus, by definition, $f(x) \in f(S)$. This means that there exists $x' \in f(S)$ such that $f(x) = f(x')$. And since f is injective, $x = x' \in S$. Thus, if f is injective, $f^{-1}(f(S)) \subseteq S$ for every $S \subseteq X$.

   Conversely, suppose that $f^{-1}(f(S)) \subseteq S$ for every $S \subseteq X$. In particular, this is true for any singleton $S = \{x_0\}$, with $x_0 \in S$. In such a case, we obtain $f^{-1}(f(\{x_0\})) = \{x_0\}$. For any element $x \in X$, if $x \neq x_0$, we have $x \notin \{x_0\}$ by definition of a singleton, thus $x \notin f^{-1}(f(\{x_0\}))$, and thus $f(x) \neq f(x_0)$. This means that f is injective.

   The second equivalence is proved.

EXERCISE 3.4.6. — *Prove lemma 3.4.9. (Hint: start with the set $\{0,1\}^X$ and apply the replacement axiom, replacing each function f with the object $f^{-1}(\{1\})$.)*

First, let's recall the main propositions involved in this exercise:

- **Replacement axiom**. Let A be a set. For any object $x \in A$, and any object y, suppose we have a statement $P(x, y)$ pertaining to x and y, such that for each $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y \mid P(x, y) \text{ is true for some } x \in A\}$, such that for any object z,

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

- **Power set axiom**. Let X and Y be sets. There there exists a set, denoted Y^X, which consists of all the function from X to Y:

$$f \in Y^X \iff (f \text{ is a function from } X \text{ to } Y\}$$

- **Lemma 3.4.9**. Let X be a set. Then the set $\{Y \mid Y \text{ is a subset of X}\}$ is a set.

The aim is to prove this lemma using the two axioms recalled here.

1. Let X be a set, and $Y = \{0, 1\}$. Per the power set axiom, $\{0,1\}^X$ is a set, and it contains all the functions $f : X \to \{0, 1\}$.

2. Let A be a subset of X. One can define the function $f_A : X \to \{0, 1\}$, such that for all $x \in X$, $f(x) = 1$ if $x \in A$, and $f(x) = 0$ otherwise. We can even say more:

[9] If S is empty, the statement is vacuously true, so that we can suppose $S \neq \varnothing$.

- If A is a subset of X, then there exists an element $f \in \{0,1\}^X$ such that $A = f^{-1}(\{1\})$: this is precisely f_A as defined above.
- Conversely, if $f \in \{0,1\}^X$, then $A = f^{-1}(\{1\})$ is by definition a subset of X.

Thus, the two statements "A is a subset of X" and "there exists $f \in \{0,1\}^X$ such that $A = f^{-1}(\{1\})$" are equivalent.

3. Finally, let be $A \subset X$ and $f \in \{0,1\}^X$. Let's define $P(f, A)$ the statement "$A = f^{-1}(\{1\})$". For each f, there is at most one A (in fact, *exactly* one A) such that $P(f, A)$ is true. Thus, per the axiom of replacement, there exists a set:

$$\mathcal{P} = \{A \mid A = f^{-1}(\{1\}) \text{ for some } f \in \{0,1\}^X\}$$

And, thanks to the equivalence demonstrated in 2.:

$$\mathcal{P} = \{A \mid A \text{ is a subset of } X\}$$

is a well-defined set, which we wanted to prove.

EXERCISE 3.4.7. — *Let X, Y be sets. Define a partial function from X to Y to be any function $f : X' \to Y'$ with $X' \subseteq X$ and $Y' \subseteq Y$. Show that the collection of all partial functions from X to Y is itself a set.*

- Let be $X' \subseteq X$ and $Y' \subseteq Y$. If both X' and Y' are fixed, then per the power set axiom (3.10), there exists a set $Y'^{X'}$ which consists of all the functions from X' to Y'.
- By lemma 3.4.9, there exist a set 2^X which consists of all the subsets of X, and a set 2^Y which consists of all the subsets of Y.
- Now we *fix* an element X' of 2^X. Let be Y' an element of the set 2^Y, A a set, and P the property "$P(Y', A)$: $A = Y'^{X'}$". Per the replacement axiom, there exists exactly one (and thus, at most one) set:

$$\begin{aligned}\{A \mid P(Y', A) \text{ is true for some } Y' \in 2^Y\} &= \{A \mid A = Y'^{X'} \text{ for some } Y' \in 2^Y\} \\ &= \{Y'^{X'} \mid Y' \in 2^Y\}\end{aligned}$$

- Each element of this set is itself a set. Thus we can apply the axiom of union (3.11): there exists a set $\bigcup\{Y'^{X'} \mid Y' \in 2^Y\}$ whose elements are those objects which are elements of elements of $\{Y'^{X'} \mid Y' \in 2^Y\}$, i.e.:

$$\bigcup\{Y'^{X'} \mid Y' \in 2^Y\} = \{f | f : X' \to Y' \text{ for some } Y' \in 2^Y\}$$

This set is obtained for one given *fixed* subset $X' \subseteq X$, so let's denote this set:

$$S_{X'} = \{f | f : X' \to Y' \text{ for some } Y' \in 2^Y\}$$

- Now we apply once again the union set (3.11), especially in its second formulation. If we denote $I = 2^X$, then for each element $X' \in I$ we do have one set $S_{X'}$, which is defined above. Thus, there exists a set $\bigcup_{X' \in 2^X} S_{X'} := \bigcup\{S_{X'} \mid X' \in 2^X\}$. And, for every function f, we have $f \in \bigcup\{S_{X'} \mid X' \in 2^X\}$ iff there exists $X' \in 2^X$ such that $f \in S_{X'}$, i.e. if there exists $X' \subset X$ and $Y' \subset Y$ such that $f : X' \to Y'$.

- Consequently, we have proved that there exists a set which consists of the collection of all partial functions from X to Y.

EXERCISE 3.4.8. — *Prove that Axiom 3.4 can be deduced from Axiom 3.1, Axiom 3.3 and Axiom 3.11.*

Let's recall very briefly the four axioms involved here :

- Axiom 3.4 (to be proved) says that if A and B are sets, then there exists a union set $A \cup B$ such that $x \in A \cup B$ iff $x \in A$ or $x \in B$.
- Axiom 3.1 essentially says that sets are objects.
- Axiom 3.3 says that singletons are pair sets do exist.
- Axiom 3.11: let A be a set, whose all elements are themselves sets. Then there exists a set $\bigcup A$ whose elements are those objects which are elements of elements of A, i.e., $x \in \bigcup A$ iff $x \in S$ for some $S \in A$.

Here is a sketch of proof for Axiom 3.4. Let A and B be sets. According to Axiom 3.1, A and B are themselves objects: they can be elements of other sets. Consequently, according to Axiom 3.3, it makes sense to talk about the singleton sets $\{A\}$ and $\{B\}$, and the set $\{A, B\}$.

Now we consider this latter set, which we denote $\mathcal{A} = \{A, B\}$. According to axiom 3.11, there exists a set $\bigcup \mathcal{A}$ whose elements those objects which are the elements of $\mathcal{A}$, i.e., $x \in \mathcal{A}$ iff there exists $S \in \mathcal{A}$ such that $x \in S$. But $\mathcal{A}$ is a pair set with only two elements, so that S must necessarily be equal to A or B.

This leads to the following conclusion: if A and B are sets, then there exists a set $\mathcal{A}$ such that $x \in \mathcal{A}$ iff $x \in A$ or $x \in B$. This is precisely the Axiom 3.4.

EXERCISE 3.5.1. — *Suppose we define the ordered pair (x, y) for any objects x and y by the formula $(x, y) := \{\{x\}, \{x, y\}\}$. Show that this definition obeys the property (3.5), and also whenever X and Y are sets, the cartesian product $X \times Y$ is also a set.*

Recall that property (3.5) says that $(x, y) = (x', y')$ iff $x = x'$ and $y = y'$. The proof below is heavily inspired by the sketch given by Paul Halmos in his famous book, *Naive Set Theory*. (The proof below is just immensely more verbose.)

1. First, we go back to Remark 3.1.9 by Terence Tao (page 37). In this remark, Tao says that for any object a, the pair set $\{a, a\}$ is in fact the singleton $\{a\}$. Tao asks *why?* to the reader. This is easy to prove using the Definition 3.1.4 (equality of sets): both sets have the same elements, thus they are equal. This fact is a crucial point for the current proof.

   Indeed, first note that for any object x, the ordered pair (x, x) will be (by definition) equal to $\{\{x\}, \{x, x\}\}$. Applying twice the Remark 3.1.9 made by Terence Tao, we can conclude that $(x, x) = \{\{x\}\}$ for any object x.

   Conversely, if any ordered pair (x, y) is a singleton, this means that $\{\{x\}, \{x, y\}\}$ is a singleton. This implies that both elements of this pair set are equal, i.e. $\{x\} = \{x, y\}$. Thus, (by Definition 3.1.4,) $y \in \{x\}$, i.e. $x = y$.

   This gives a handy conclusion, that we can write as a lemma:

Lemma. *An ordered pair (x, y) is a singleton if and only if $x = y$ (and in this case, this singleton is $\{\{x\}\} = \{\{y\}\}$).*

We can now prove more easily that property (3.5) is met.

2. Let's prove that the property (3.5) is satisfied.

   - First, let be two ordered pairs $(a, b) = \{\{a\}, \{a, b\}\}$ and $(x, y) = \{\{x\}, \{x, y\}\}$. If $a = x$ and $y = b$, then we obviously have $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$.
   - For the reciprocal, suppose that $(a, b) = (x, y)$, and let's show that $a = x$ and $b = y$. We will consider two distinct cases.
     (a) First consider the case where $a = b$ (note that this also covers the case $x = y$, since they play symmetrical roles). Thus $(a, b) = \{\{a\}\}$. Since $(a, b) = (x, y)$, we have $\{\{x\}, \{x, y\}\} = \{\{a\}\}$.
     This means that $\{x\} \in \{\{a\}\}$, i.e. $a = x$.
     But we also have $\{x, y\} \in \{\{a\}\}$, i.e. $\{x, y\} = \{a\}$. This means in particular that $\{x, y\}$ is a singleton, which is only possible if $x = y$ according to the lemma introduced above.
     Thus, $a = b$ by hypothesis, and $a = x$, and $x = y$. This finally means that all four elements are equal: $a = b = x = y$.
     We can insist: if we have either $a = b$ or $x = y$, then all four elements are equal, and property (3.5) is met.
     (b) The other case is $a \neq b$ (which also implies $x \neq y$, otherwise all four elements would be equal). Since $(a, b) = (x, y)$, we have $\{a\} \in \{\{x\}, \{x, y\}\}$, so that we have either $\{a\} = \{x\}$ or $\{a\} = \{x, y\}$. The latter case can be excluded: $\{a\} = \{x, y\}$ would mean that $\{x, y\}$ is a singleton, thus $x = y$, a contradiction with our hypothesis. Thus, the only possibility is $\{a\} = \{x\}$, i.e. $a = x$.
     We also have $\{a, b\} \in \{\{x\}, \{x, y\}\}$, and for the same reason, the only possibility is $\{a, b\} = \{x, y\}$. But we have showed that $a = x$, so that $\{a, b\} = \{a, y\}$. The conclusion is $y = b$.
   - Conclusion: in both cases, (a, b) implies both $a = x$ and $y = b$, which is our initial goal. Property (3.5) is met.

3. Finally, if we adopt this definition, $X \times Y$ is a set. Indeed, for every $x \in X$ and $y \in Y$, both x and y are elements of $X \cup Y$. Thus, the singleton $\{x\}$ and the pair set $\{x, y\}$ are elements of the power set of $X \cup Y$ (which is indeed a set, by Lemma 3.4.9: see Exercise 3.4.6). In other words, if $\mathcal{P}(A)$ denotes the power set of a set A, we have $\{x\} \in \mathcal{P}(X \cup Y)$ and $\{x, y\} \in \mathcal{P}(X \cup Y)$.

   Thus, for every objects $x \in X$ and $y \in Y$, $\{\{x\}, \{x, y\}\} \subset \mathcal{P}(X \cup Y)$. This latter statement is equivalent to $\{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(X \cup Y))$, which is also a well-defined set by a (recursive) application of Lemma 3.4.9.

   Then, for any element $S \in \mathcal{P}(\mathcal{P}(X \cup Y))$, let $P(S)$ be the property "There exists $x \in X$ and $y \in Y$ such that $S = \{\{x\}, \{x, y\}\}$". By the axiom of specification (Axiom 3.5), there exists a set $\{S \in \mathcal{P}(\mathcal{P}(X \cup Y)) \mid P(S) \text{ is true}\}$: this set is precisely the cartesian product $X \times Y$ we were looking for.

4. Integers and rationals

Exercise 4.1.1. — *Verify that the definition of equality on the integers is both reflexive and symmetric.*

Recall the Definition 4.1.1 of equality on integers: two integers $a--b$ and $c--d$ are equal iff $a+d=c+b$. This defines a binary relation on $\mathbb{Z}$, denoted "=". Let's show that this relation is reflexive and symmetric.

- Reflexivity: let a and b be natural numbers, so that $a--b$ is an integer. We know that, on natural numbers, equality is reflexive, i.e. $a+b=a+b$. This equality means precisely that $a--b=a--b$.
- Symmetry: let a,b,c,d be natural numbers. If $a--b=c--d$, do we also have $c--d=a--b$?

$$\begin{array}{rrcl} & a--b & = & c--d \\ \iff & a+d & = & c+b \\ \iff & c+b & = & a+d \text{ (equality is symmetric on naturals)} \\ \iff & c--d & = & a--b \end{array}$$

Exercise 4.1.2. — *Show that the definition of negation on the integers is well-defined in the sense that if $(a--b)=(a'--b')$, then $-(a--b)=-(a'--b')$ (so equal integers have equal negations).*

Since $a--b=a'--b'$, we have $a+b'=a'+b$.
Also, by Definition 4.1.4 of negation, we have:

$$\begin{aligned} -(a--b) &= b--a \\ -(a'--b') &= b'--a' \end{aligned}$$

Then, we have successively:

$$\begin{aligned} b+a' &= a'+b \text{ (addition is commutative on naturals, Prop. 2.2.4)} \\ &= a+b' \text{ (initial hypothesis)} \\ &= b'+a \text{ (by commutativity on naturals once again)} \end{aligned}$$

and this equality $b+a'=b'+a$ precisely means that $b--a=b'--a'$, i.e. that $-(a--b)=-(a'--b')$.

Exercise 4.1.3. — *Show that $(-1)\times a=-a$ for every integer a.*

Since a is an integer, there exist two natural numbers n and m such that $a=m--n$.
On the one hand, by Definition 4.1.4, $-a=n--m$.
On the other hand, using once again Definition 4.1.4 and Definition 4.1.2,

$$\begin{aligned} (-1)\times a &= (0--1)\times(m--n) \\ &= (0\times m+1\times n)--(0\times n+1\times m) \\ &= n--m \end{aligned}$$

Thus, we have indeed $(-1) \times a = -a$.

EXERCISE 4.1.4. — *Prove the remaining identities in Proposition 4.1.6.*

Let $x = a -\!\!- b$, $y = c -\!\!- d$ and $z = e -\!\!- f$ be three integers. Those identities are the following:

1. $x + y = y + x$, i.e., we must prove that addition is commutative on the integers. We have:

$$\begin{aligned} x + y &= (a -\!\!- b) + (c -\!\!- d) \\ &= (a + c) -\!\!- (b + d) \text{ (by Definition 4.1.2)} \\ &= (c + a) -\!\!- (d + b) \text{ (addition is commutative on naturals)} \\ &= (c -\!\!- d) + (a -\!\!- b) \text{ (by Definition 4.1.2 again)} \\ &= y + x \end{aligned}$$

2. $(x + y) + z = x + (y + z)$, i.e. prove that addition is associative on the integers. This is a very similar proof, and this is a direct consequence of associativity of addition on the naturals.

3. $x + 0 = 0 + x = x$. We have already showed that addition is commutative on the integers, so we just have to prove that $x + 0 = x$.

$$\begin{aligned} x + 0 &= (a -\!\!- b) + (0 -\!\!- 0) \\ &= (a + 0) -\!\!- (b + 0) \\ &= a -\!\!- b = x. \end{aligned}$$

4. $x+(-x) = (-x)+x = 0$. Once again, thanks to the previous result about commutativity, we just have to prove that $x + (-x) = 0$.

$$\begin{aligned} x + (-x) &= (a -\!\!- b) + (b -\!\!- a) \text{ (by Definition 4.1.4)} \\ &= (a + b) -\!\!- (b + a) \text{ (by Definition 4.1.2)} \\ &= (a + b) -\!\!- (a + b) \text{ (addition is commutative on naturals)} \\ &= 0 \text{ (because } m -\!\!- m = 0 -\!\!- 0 \text{ for all integer } m) \end{aligned}$$

5. $xy = yx$, i.e. multiplication is commutative on the integers.

$$\begin{aligned} xy &= (a -\!\!- b) \times (c -\!\!- d) \\ &= (ac + bd) -\!\!- (ad + bc) \text{ (by Definition 4.1.2)} \\ &= (ca + db) -\!\!- (da + cb) \text{ (multiplication is commutative on the naturals)} \\ &= yx \text{ (by Definition 4.1.2)} \end{aligned}$$

6. $(xy)z = x(yz)$, i.e. multiplication is associative on the integers. This is actually the only identity proved in the main text by Terence Tao.

7. $x1 = 1x = x$. The equality between the first two terms is a direct consequence of commutativity of multiplication on the integers. We just have to prove that $x1 = x$. And indeed, $x1 = (a -\!\!- b) \times (1 -\!\!- 0) = (a1 + b0) -\!\!- (b1 + a0) = a -\!\!- b = x$.

8. $x(y + z) = xy + xz$, i.e. show distributivity on the integers. On the left side, we have:

$$\begin{aligned} x(y+z) &= (a -\!\!- b)\,((c -\!\!- d) + (e -\!\!- f)) \\ &= (a -\!\!- b)\,((c+e) -\!\!- (d+f)) \\ &= (a(c+e) + b(d+f)) -\!\!- (a(d+f) + b(c+e)) \\ &= ((ac + ae + bd + bf)) -\!\!- ((ad + af + bc + be)) \end{aligned}$$

   and then on the left side:

$$\begin{aligned} xy + xz &= (a -\!\!- b)(c -\!\!- d) + (a -\!\!- b)(e -\!\!- f) \\ &= ((ac + bd) -\!\!- (ad + bc)) + ((ae + bf) -\!\!- (af + be)) \\ &= ((ac + ae + bd + bf)) -\!\!- ((ad + af + bc + be)) \end{aligned}$$

9. $(y + z)x = yx + zx$. This latter identity is a direct consequence of commutativity of multiplication on the integers, and distributivity on the integers, both being already proved earlier in this exercise.

Exercise 4.1.5. — *Prove Proposition 4.1.8, i.e.: let x and y be integers such that $xy = 0$, then either $x = 0$ or $y = 0$ (or both).*

We will use here Lemma 4.1.5 (trichotomy of integers, which says that any integer is either zero, or equal to a positive natural number, or the negation of a positive natural number), and Lemma 2.3.3 (which provides an equivalent of Proposition 4.1.8 for natural numbers only). We will prove the proposition for (all) three possible cases: $x = 0$, x is a positive natural number, $-x$ is a positive natural number.

y will be considered as a fixed integer, $y = c -\!\!- d$ with c, d natural numbers.

1. First let's take the case $x = 0$. There is nothing to prove here, the proposition is obviously true.

2. Then let's take the case where x is a positive natural number (and, consequently, is not equal to zero). In this case, as an integer, x can be written $n -\!\!- 0$ with n a positive natural number.

   We have $xy = (n -\!\!- 0) \times (c -\!\!- d) = (nc + 0d) -\!\!- (nd + 0c) = nc -\!\!- nd$.

   Thus, $xy = 0$ iff $nc -\!\!- nd = 0 -\!\!- 0$, and by Definition 4.1.1, this means that $nc = nd$. But since all three n, c, d are natural numbers, we can use the cancellation law for natural numbers and conclude that $c = d$.

   This means that $y = c -\!\!- c = 0 -\!\!- 0 = 0$. Thus, in this case, if $xy = 0$ with x non-zero, we have showed that y is necessarily equal to 0.

3. Finally, let's take the case where x is the opposite of a positive natural number n, i.e. $x = 0 -\!\!- n$. A very similar proof also leads to $c = d$, and to $y = 0$.

Exercise 4.1.6. — *Prove Corollary 4.1.9, i.e. if a, b, c are integers such that $ac = bc$ and c is non-zero, then $a = b$.*

If $ac = bc$, then $ac + (-bc) = bc + (-bc) = 0$. Thus, $ac - bc = 0$.

Let's use the property of distributivity (Proposition 4.1.6): we obtain $(a - b)c = 0$. According to Proposition 4.1.8 (see also the previous exercise), this implies either $c = 0$ or $a - b = 0$. The first option ($c = 0$) must be discarded since it does not fit the initial hypothesis. The only possibility is thus $a - b = 0$, and adding b to both sides finally leads to $a = b$.

Exercise 4.1.7. — *Prove Lemma 4.1.11.*

The statements to prove are the following:

1. Show that $a > b$ if and only if $a - b$ is a positive natural number.

   First suppose that $a > b$. This means (Definition 4.1.10) that there exists a natural number n such that $a = b + n$, and $a \neq b$. Then, we add to both sides the opposite of b, and we get $a + (-b) = b + n + (-b)$, i.e. $a - b = n$. In this latest equality, n cannot be zero, otherwise we would have $a = b$, which is excluded. The first implication is proved.

   Then suppose that $a - b = n$ with n a positive natural number. Adding b to both sides leads to $a = b + n$, i.e. $a \geqslant b$. We cannot have $a = b$, because this would be a contradiction with the fact that $n \neq 0$. Thus, $a > b$.

2. Show that addition preserves order, i.e. if $a > b$, then $a + c > b + c$.

   Suppose that $a > b$. According to the previous point, this means that $a - b = n$, with n a positive natural number. Then, we get successively:

   $$\begin{array}{rcll} a & = & b + n & \text{(by adding } b \text{ to both sides)} \\ a + c & = & b + c + n & \text{(by adding } c \text{ to both sides)} \\ a + c - b - c & = & n & \text{(by adding } (-b) + (-c) \text{ to both sides)} \\ a + c - (b + c) & = & n & \text{(by using the distributive law and Exercise 4.1.3)} \end{array}$$

   Using again the previous point, since $(a + c) - (b + c)$ is equal to a positive natural number, we can conclude that $a + c > b + c$.

3. Show that positive multiplication preserves order, i.e. if $a > b$ and c is positive, then $ac > bc$.

   Since $a > b$, according to the first point of this exercise, we have $a - b = n$, with n a positive natural number. According to the distributive law, $(a - b)c = ac - bc$. But we also have $(a - b)c = nc$, and nc is a positive natural number (as product of two positive numbers, see Lemma 2.3.3). Thus, $ac - bc$ is equal to a positive number, which means that $ac > bc$.

4. Show that negation reverses order, i.e. if $a > b$, then $-a < -b$.

   Here, we will need a small lemma, which says that for any natural number n, we have $n = -(-n)$. There are several ways to show this result: either by proving that $(-1) \times (-1) = 1$ and using Exercise 4.1.3, or simply by noting that $n + (n) = 0$ for all n, which means that n is the opposite of $-n$ (i.e., $n = -(-n)$).

Now this point is easy to prove. $a > b$ means that $a - b$ is a positive number, as shown earlier in this exercise. We want to prove that $-a < -b$, and proving this assertion requires to show that $-b-(-a)$ is a positive number. But $-b-(-a) = -b+a = a-b$, which is a positive natural number. Thus we are done.

5. Show that order is transitive, i.e. if $a > b$ and $b > c$, then $a > c$.

   Still using the first point of this exercise, we have $a-b = n$ and $b-c = m$, with n, m two positive natural numbers. We know that $n + m$ is positive as the sum of two positive numbers, thus $n + m = a - b + b - c = a - c$ is positive. This means that $a > c$.

6. Show order trichotomy, i.e.: exactly one of the statements $a > b$, $a < b$, or $a = b$ is true.

   - If $a = b$, then obviously (exactly) one of those statements is true.
   - Now consider the case $a \neq b$, and let's show that we have either $a > b$ or $a < b$ (and cannot have both).

     Let's consider the integer $a-b$. By trichotomy of integers (Lemma 4.1.5), we know that we have either $a-b = 0$ (which is excluded here), or $a-b = n$ with n positive, or $a - b = -n$ with n positive.

     If $a - b = n$, then $a > b$ according to the first point of this exercise. If $a - b = -n$, then $-n = -(a - b) = b - a$, thus $b > a$.

     Finally, we just have to show that we cannot have both $a > b$ and $b > a$ at the same time. If $a > b$, then the integer $a - b$ is positive. If $b > a$, then $b - a$ is positive, i.e. $-(b - a) = a - b$ is the opposite of a positive natural. Thus, $a - b$ is both positive and the opposite of a positive number, which is excluded by the trichotomy of integers.

Exercise 4.1.8. — *Show that the principle of induction (Axiom 2.5) does not apply directly to the integers. More precisely, give an example of a property $P(n)$ pertaining to an integer n such that $P(0)$ is true, and that $P(n)$ implies $P(n{+}{+})$ for all integers n, but that $P(n)$ is not true for all integers n.*

According to Lemma 4.1.5, an integer is either equal to 0, or equal to a positive natural number, or equal to the negation of a positive natural number.

Let's define $P(n)$ as the property "The integer n is a natural number, i.e. is either equal to 0 or equal to a positive natural number". Obviously, $P(0)$ is true. Furthermore, if n is a natural number, then $n{+}{+}$ is also a natural number (Axiom 2.2), so that if $P(n)$ is true, then $P(n{+}{+})$ is true. Thus, $P(n)$ matches the required condtions.

However, $P(-1)$ is obviously false.

Exercise 4.2.1. — *Show that the definition of equality for the rational numbers is reflexive, symmetric, and transitive.*

This exercise ressembles Exercise 4.1.1, and the same approach applies. Recall the Definition 4.2.1: two rational numbers $a /\!/ b$ and $c /\!/ d$ are equal iff $ad = bc$. This defines a binary relation on $\mathbb{Q}$, denoted "=". Let's show that this relation is reflexive, symmetric and transitive.

Hereafter, a, b, c, d, e, f are integers (and b, d, f are non-zero).

- Reflexivity: here we must prove that $a // b = a // b$. This is the case iff $ab = ba$, with is true because of (commutativity of multiplication on $\mathbb{Z}$ and) reflexivity of equality on $\mathbb{Z}$.
- Symmetry: here we must prove that if $a // b = c // d$, we also have $c // d = a // b$. We have successively:

$$\begin{array}{rrcl} & a // b & = & c // d \\ \iff & ad & = & bc \\ \iff & da & = & cb \ (\times \text{ is commutative on } \mathbb{Z}) \\ \iff & cb & = & da \ (= \text{ is symmetric on } \mathbb{Z}) \\ \iff & c // d & = & a // b \end{array}$$

- Transitivity: here we must prove that if $a // b = c // d$ and $c // d = e // f$, then $a // b = e // f$. I.e., we must prove that if $ad = bc$ and $cf = de$, then $af = be$.

  Let's multiply by e both sides of the equality $ad = bc$: we get $ade = bce$. Since $de = cf$, we also get $acf = bce$.

  In this latest equality, using the cancellation law (Corollary 4.1.9) for c would lead to $af = be$, which would close the proof. However, unlike b, d or f, the integer c may be equal to 0, and in this case we cannot use the cancellation law. There are thus two different cases:

  - If $c \neq 0$, we simply use the cancellation law: since $acf = bce$, then $af = be$, which means that $a // b = e // f$.
  - If $c = 0$, then $bc = 0$. But since $ad = bc$, we also have $ad = 0$, and we know that $d \neq 0$. According to Proposition 4.1.8, this leads to $a = 0$. A similar reasoning leads to $e = 0$. Thus, $a = c = e = 0$, and $0 = af = be$, which means $a // b = e // f$.

Exercise 4.2.2. — *Prove the remaining components of Lemma 4.2.3.*

Let $a // b = a' // b'$ be two rationals; let $c // d = c' // d'$ be two rationals. The remaining claims are the following:

- Prove that $-(a' // b') = -(a // b)$. This equality holds iff $(-a') // b' = (-a) // b$, i.e. iff $(-a')b = b'(-a)$. We have successively:

$$\begin{aligned} (-a')b &= (-1)a'b \text{ (see Exercise 4.1.3)} \\ &= (-1)ab' \text{ (because } a // b = a' // b') \\ &= (-a)b' \text{ (using Exercise 4.1.3 one again)} \end{aligned}$$

  Thus we are done.

- Prove that $(a // b) \times (c // d) = (a' // b') \times (c // d)$. To prove this equality, we must show that $(ac) // (bd) = (a'c) // (b'd)$. By definition of equality between rationals, this holds iff $acb'd = bda'c$. Since $ab' = ba'$, the claim follows (using commutativity of multiplication on integers[10]).

[10] This kind of precision about very basic properties of naturals and integers will not be mentioned anymore.

- Prove that $(a // b) \times (c // d) = (a // b) \times (c' // d')$. To prove this equality, we must show that $(ac) // (bd) = (ac') // (bd')$. By definition of equality between rationals, this holds iff $acbd' = bdac'$. Since $cd' = dc'$, the claim follows.

EXERCISE 4.2.3. — *Prove the remaining components of Proposition 4.2.4.*

Let $x = a // b$, $y = c // d$, and $z = e // f$ be rational numbers, with a, c, e integers, and b, d, f non-zero integers. The remaining claims are the following:

1. $x + y = y + x$, i.e. addition is commutative for the rationals.

   On the one hand, we have $x + y = a // b + c // d = (ad + bc) // bd$.

   On the other hand, $y + x = c // d + a // b = (cb + da) // db = (ad + bc) // bd$ using the commutativity of addition and multiplication on the integers. Thus, the two expressions are equal.

2. $(x + y) + z = x + (y + z)$: already proved in the book.

3. $x+0 = 0+x = x$. By the first point of this exercise, we already know that $x+0 = 0+x$, so we have just to show that $x+0 = x$. We have $x+0 = a//b+0//1 = (a1+b0)//(b1) = a // b = x$, which is the required result.

4. $x + (-x) = (-x) + x = 0$. Once again, the part $x + (-x) = (-x) + x$ comes from the first point of this exercise, so we just have to prove that $x + (-x) = 0$. We have $x + (-x) = a // b + -(a // b) = a // b + (-a) // b = (ab - ba) // b^2 = 0 // b^2$. But we know that $0 // m = 0 // 1 = 0$ for all non-zero integer m, since $0 \times 1 = m \times 0$. Thus, $x + (-x) = 0 // b^2 = 0$, as required.

5. $xy = yx$, i.e. multiplication is commutative on the rationals. Indeed, $xy = (a // b) \times (c // d) = (ac) // (bd)$ by definition. On the other hand, $yx = (c // d) \times (a // b) = (ca) // (db) = (ac) // (bd)$ by commutativity of multiplication on the integers. Thus, $xy = yx$.

6. $(xy)z = x(yz)$, i.e. multiplication is associative on the rationals. We have $(xy)z = (ace) // (bdf) = x(yz)$ by associativity of multiplication on the integers.

7. $x1 = 1x = x$. Once again, we already know that $x1 = 1x$, thanks to the fifth point of this exercise. So we just have to show that $x1 = x$. We have $x1 = (a // b) \times (1 // 1) = (a1) // (b1) = a // b = x$.

8. $x(y + z) = xy + xz$, i.e. distributivity of multplication for the rationals. On the one hand, we have:

$$\begin{aligned} x(y+z) &= (a // b)(c // d + e // f) \\ &= (a // b)((cf + de) // (df)) \\ &= (acf + ade) // (bdf) \end{aligned}$$

On the other hand[11]:

$$\begin{aligned} xy + xz &= (a // b)(c // d) + (a // b)(e // f) \\ &= (ac) // (bd) + (ae) // (bf) \\ &= (acbf + bdae) // (b^2df) \\ &= (acf + ade) // (bdf) \end{aligned}$$

Thus we have indeed $x(y + z) = xy + xz$.

9. $(y + z)x = yx + zx$. This can be deduced immediately from commutativity of multiplication and the eighth point of this exercise.

10. For all $x \neq 0$, $xx^{-1} = x^{-1}x = 1$. Once again, the part $xx^{-1} = x^{-1}x$ comes from the fifth point of this exercise, so that we just have have to show that $xx^{-1} = 1$.

$$\begin{aligned} xx^{-1} &= (a // b) \times (b // a) \\ &= (ab) // (ba) \\ &= 1 // 1 = 1 \end{aligned}$$

Exercise 4.2.4. — *Prove Lemma 4.2.7. (trichotomy of rationals), i.e., if x is a rational number, then exactly one of the following three statements is true: (a) x is equal to 0, (b) x is a positive rational number, or (c) x is a negative rational number.*

Following the hint given by Terence Tao, we'll first prove that *at least* one of those statements is true, and then that *at most* one of them is true. Let be $x = a // b$, where a is an integer and b a non-zero integer.

1. Let's prove that at least one of those statements is true.

   First, an obvious case: if $a = 0$, then $x = a // b = 0$, thus one of the statements is true. Now consider the case where $a \neq 0$. By the trichotomy of integers, a can be either positive or negative. Similarly, b can also be either positive or negative (it cannot be null, by definition). Thus, there are four main cases:

   - $a > 0$ and $b > 0$. Here, by Definition 4.2.6, $x = a // b$ is positive.
   - $a > 0$ and $b < 0$. Here, $b = -m$, with m a positive natural number. Thus, $x = a // (-m)$. But $a // (-m) = (-a) // m$ (this is easy to verify: $am = (-a)(-m)$). This means that $x = (-a) // m$, with both a and m positive, i.e. x is negative.
   - $a < 0$ and $b > 0$. Here, $x = a // b$ is negative by Definition 4.2.6.
   - $a < 0$ and $b < 0$. Here, we can say that $a = -n$ and $b = -m$, with n, m positive natural numbers. Thus, $x = (-n) // (-m) = n // m$ (once again, this latest equality is easy to verify). Thus, x is positive.

   Conclusion: if all four cases, at least one of the three properties is true.

2. Now prove that at most one of those statements is true.

[11] We use implicitly here the fact that $(nm) // n = m // 1$ for all integers n, m with $m \neq 0$, which is straightforward to prove.

- Suppose, for the sake of contradiction, that we have both $x = 0$ and x positive. On the one hand, "$x = a // b = 0$" implies that $a = 0$ (see Terence Tao's remark, page 83). On the other hand, "x is positive" implies that $a > 0$. So we would have both $a = 0$ and a positive, which is not compatible with the trichotomy of integers.
- A similar argument holds if we suppose both $x = 0$ and x negative.
- Now suppose that we have both x positive and x negative, i.e. $x = c // d = (-n) // m$, with c, d, n, m positive natural numbers. Thus, we should have $cm = (-n)d$. On the one hand, cm is positive, as the multiplication of two positive natural numbers. On the other hand, $(-n)d = -(nd)$ is negative. The equality $cm = -nd$ is thus impossible.

Conclusion: all three statements are mutually exclusive.

Exercise 4.2.5. — *Prove Proposition 4.2.9.*

Let x, y, z be rational numbers. This proposition includes the following statements:

1. Prove that exactly one of the three statements $x = y$, $x < y$, or $x > y$ is true.

   This statement is very close to Lemma 4.2.7, proved in the previous exercise. Let's consider the rational number $x - y$. According to the trichotomy of rationals, this number can be either zero, positive or negative (exactly one of these statements is true).

   If $x - y = 0$, then $x = y$. If $x - y$ is positive, then $x > y$. And if $x - y$ is negative, then $x < y$. Thus, the order trichotomy is a direct consequence of the ordering of rationals.

2. Prove that one has $x < y$ if and only if $y > x$.

   Since $x < y$, the rational number $x - y$ is negative, and can be written $(-a) // b$ for positive integers a, b. And since $x - y = -a // b$, we have $a // b = y - x$, i.e. $y - x$ is positive, i.e. $y > x$.

3. Prove that if $x < y$ and $y < z$, then $x < z$.

   Since $x < y$, $x - y$ is negative. Similarly, $y - z$ is negative. This means that $x - y$ can be written $(-a) // b$, and $y - z$ can be written $(-c) // d$, with a, b, c, d positive integers.

   On the one hand, their sum is $x - z$. On the other hand, their sum is $((-ad) + (-cb)) // (bd)$. This latest expression is a negative rational, thus we have $x < z$.

4. Prove that if $x < y$, then $x + z < y + z$.

   Suppose that $x < y$. Thus, $x - y$ is negative. But we have, for any rational z, $x - y = (x + z) - (y + z)$, and thus this latter expression is also negative. This means that $x + z < y + z$.

5. Prove that if $x < y$ and z is positive, then $xz < yz$.

   Since $x < y$, the rational number $x - y$ is negative. Furthermore, we know (by Proposition 4.2.4) that $xz - yz = (x - y)z$. In the expression $(x - y)z$, z is supposed to

be positive and $x - y$ is negative, thus their product is negative[12]. This means that $xz < yz$.

EXERCISE 4.2.6. — *Show that if x, y, z are rational numbers such that $x < y$ and z is negative, then $xz > yz$.*

If $x < y$, then $x - y$ is negative. Thus, $(x - y)z$ is the product of two negative rationals: it is a positive rational[13].

But $(x-y)z = xz-yz$ by Proposition 4.2.4. And since we have showed that this number is positive, we have $xz > yz$.

Note: in particular, this exercise says that if $x > y$, then $-x < -y$ (with $z = -1$).

EXERCISE 4.3.1. — *Prove Proposition 4.3.3.*

Let x, y, z be rational numbers. The statements to prove are the following:

1. Show that $|x| \geqslant 0$ for all x, and that $|x| = 0$ iff $x = 0$.

   There are three cases:

   - if $x = 0$, then $|x| := 0$, thus we have in particular $|x| \geqslant 0$.
   - if $x > 0$, then $|x| := x$, thus $|x| > 0$. And in particular, this means that $|x| \geqslant 0$.
   - if $x < 0$, then $|x| := -x$, thus $|x| > 0$. And in particular, $|x| \geqslant 0$.

   We can note that the only case where $|x| = 0$ is when $x = 0$. Thus, by trichotomy of rationals, $|x| = 0$ iff $x = 0$.

2. Show that $|x + y| \leqslant |x| + |y|$.

   - If $x = 0$ or $y = 0$, this is immediate.
   - If $x > 0$ and $y > 0$, $x + y$ is positive, thus $|x + y| = x + y = |x| + |y|$.
   - If $x < 0$ and $y < 0$, $x + y$ is negative, thus $|x + y| = -(x + y) = -x - y$. On the other hand, $|x| + |y| = -x - y$.
   - Finally, the case where x and y are of opposite signs. Say that x is positive and y negative, but they are exchangeable. On the one hand, $|x| + |y| = x - y > 0$. On the other hand, $|x + y|$ can be either equal to $x + y$ if $x + y > 0$, i.e. if $x > -y$; or equal to $-x - y$ if $x + y < 0$, i.e. if $x < -y$.

     In the first case, since $-y < 0 < y$ by hypothesis, we have $|x+y| = x+y < x-y = |x| + |y|$.

     In the second case, since $-x < 0 < x$ by hypothesis, we have $|x + y| = -x - y < x - y = |x| + |y|$.

   Conclusion: in all cases, we have indeed $|x + y| \leqslant |x| + |y|$.

[12] This is never explicitly mentioned in the book. However, using Exercise 4.1.3, we know that for every integer a, we have $-a = (-1) \times a$. So let's consider the product $n(-m)$ where n, m are positive integers: this product is $(-1)nm = -(nm)$, and thus is negative.

[13] Similarly, if x and y are negative, then $-x$ and $-y$ are positive, and their product $(-x)(-y) = (-1)(-1)xy = xy$ is positive by definition. This can also be deduced from Proposition 4.2.9(e), by choosing $x = 0$.

3. Show that $-y \leqslant x \leqslant y$ iff $y \geqslant |x|$. (Thus, in particular, $-|x| \leqslant x \leqslant |x|$.)

   - First suppose that $y \geqslant |x|$. Note that, whatever could be the value of x, we have necessarily $y \geqslant 0$ according to the first point of this exercise. Now we can split into three cases.

     If $x = 0$ then $y \geqslant 0$ and the claim is immediate.

     If $x > 0$, then $|x| = x$, and the part $y \geqslant x$ is immediate. Furthermore, the other part $-y \leqslant x$ is also immediate since $-y$ is negative and x is positive.

     If $x < 0$, then $|x| = -x$, thus we have $y \geqslant -x$, i.e. $-y \leqslant x$ according to Exercise 4.2.6. Additionally, the part $x \leqslant y$ is immediate since x is negative and y is positive.
   - Conversely, suppose that $-y \leqslant x \leqslant y$. If $x \geqslant 0$, then $|x| = x$, thus the rightmost inequality gives $x = |x| \leqslant y$. In the other case, if $x < 0$, then $|x| = -x$. The leftmost inequality $-y \leqslant x$ leads (according to Exercise 4.2.6) to $y \geqslant -x$, i.e. $y \geqslant |x|$.

4. Show that $|xy| = |x| \times |y|$. (In particular, $|-x| = |x|$.)

   Once again, we can split into several cases, as in the second point of this exercise.

   - If $x = 0$ or $y = 0$, both sides of the equality are zero (cf. the first point of this exercise), thus the claim is immediate.
   - If $x > 0$ and $y > 0$, the product xy is also positive. Thus, $|xy| = xy$, and $|x| \times |y| = xy$, and the claim follows.
   - If $x < 0$ and $y < 0$, then the product xy is positive, and $|xy| = xy$. On the other hand, $|x| \times |y| = (-x)(-y) = xy$, and the claim follows.
   - If x and y are of opposite signs (say x positive and y negative, but they are exchangeable), then xy is negative, and $|xy| = -xy$. On the other hand, $|x| \times |y| = -xy$, thus the claim follows.

5. Show that $d(x, y) \leqslant 0$ for all x, y, and that $d(x, y) = 0$ iff $x = y$.

   We have $d(x, y) = |x - y| \geqslant 0$ according to the first point of this exercise. Furthermore, still according to the first point, $d(x, y) = |x - y| = 0$ iff $x - y = 0$, i.e. $x = y$.

6. Show that $d(x, y) = d(y, x)$.

   We have $d(x, y) = |x - y|$ and $d(y, x) = |y - x|$ by definition. But $|y - x| = |-(x - y)| = |x - y|$ according to the fourth point of this exercise.

7. Show that $d(x, z) = d(x, y) + d(y, z)$.

   We have $d(x, z) = |x - z| = |(x - y) + (y - z)| \leqslant |x - y| + |y - z|$ according to the second point of this exercise. The claim follows.

Exercise 4.3.2. — *Prove the remaining claims in Proposition 4.3.7.*

Let x, y, z, w be rational numbers.

1. If $x = y$, then $d(x, y) = 0$ according to Proposition 4.3.3(e). Thus, $d(x, y) \leqslant \varepsilon$ for any positive number ε.

   Conversely, suppose that $d(x, y) \leqslant \varepsilon$ for any $\varepsilon > 0$, and let's prove that $x = y$. Suppose, for the the sake of contradiction, that $x \neq y$; and let be $\varepsilon = |x - y|/2$. Since $x \neq y$, we have $|x - y| > 0$, thus ε is a positive number. Furthermore, $d(x, y) = \varepsilon + \varepsilon$, thus $d(x, y) > \varepsilon$, which is a contradiction.

2. This is a direct consequence from Proposition 4.3.3(f). Indeed, since $d(x, y) = d(y, x)$, we obviously have $d(y, x) \leqslant \varepsilon$ when $d(x, y) \leqslant \varepsilon$.

3. Suppose that $d(x, y) \leqslant \varepsilon$ and $d(y, z) \leqslant \delta$. Thus, by triangle inequality, $d(x, z) \leqslant d(x, y + d(y, z) \leqslant \varepsilon + \delta$.

4. Suppose that $d(x, y) \leqslant \varepsilon$ and $d(z, w) \leqslant \delta$. Thus,

$$\begin{aligned} d(x + z, y + w) &= |(x + z) - (y + w)| \\ &= |(x - y) + (z - w)| \\ &\leqslant |x - y| + |z - w| \\ &\leqslant \varepsilon + \delta \end{aligned}$$

   which means that $x + z$ and $y + w$ are $(\varepsilon + \delta)$-close.

   Similarly, $d(x - z, y - w) = |(x - y) + (w - z)|$, and using just the symmetry of distance, we can conclude that $x - z$ and $y - w$ are $(\varepsilon + \delta)$-close according to the previous result.

5. This is clear: we have $d(x, y) \leqslant \varepsilon < \varepsilon'$.

6. Since $d(x, y) \leqslant \varepsilon$, we have $-\varepsilon \leqslant y - x \leqslant \varepsilon$. Similarly, we have $-\varepsilon \leqslant z - x \leqslant \varepsilon$.

   y and z are exchangeable here, so we can suppose that $y \leqslant w \leqslant z$. From this inequality, we can get $y - x \leqslant w - x \leqslant z - x$. Extending this with the former inequalities, we have:

$$-\varepsilon \leqslant y - x \leqslant w - x \leqslant z - x \leqslant \varepsilon$$

   and in particular $-\varepsilon \leqslant w - x \leqslant \varepsilon$, which means $d(w, x) \leqslant \varepsilon$.

7. We have $d(x, y) = |x - y| \leqslant \varepsilon$. Since z is positive, we have $|z| > 0$, thus $|x - y||z| \leqslant \varepsilon|z|$. But according to Proposition 4.3.3(d), $|x - y|z = |(x - y)z| = |xz - yz|$. Thus, $|xz - yz| \leqslant \varepsilon|z|$, i.e., xz and yz are $\varepsilon|z|$-close.

Exercise 4.3.3. — *Prove Proposition 4.3.10.*

Let x, y be rationals, and n, m be natural numbers. The claims to prove are the following (they are re-ordered and re-numbered here):

1. Show that $x^n x^m = x^{n+m}$. We induct on n while keeping m fixed.

   For the base case $n = 0$, we have on the one hand $x^n x^m = x^0 x^m = 1 \cdot x^m = x^m$. On the other hand, $x^{n+m} = x^{0+m} = x^m$. Thus, both sides are equal, and the base case is done.

Now suppose that $x^n x^m = x^{n+m}$, and let's show that $x^{n+1}x^m = x^{(n+1)m}$. We have:

$$\begin{aligned} x^{n+1}x^m &= (x^n x)x^m && \text{(by Definition 4.3.9)} \\ &= x^n x^m x && \text{(by associativity and commutativity of multiplication)} \\ &= x^{n+m}x && \text{(by induction hypothesis)} \\ &= x^{n+m+1} && \text{(by Definition 4.3.9 once again)} \end{aligned}$$

This closes the induction.

2. Show that $(xy)^n = x^n y^n$. Let's induct on n. The base case $n = 0$ is obvious, since both sides are equal to 1. Now suppose inductively that $(xy)^n = x^n y^n$. Thus we have:

$$\begin{aligned} (xy)^{n+1} &= (xy)^n(xy) && \text{(by Definition 4.3.9)} \\ &= x^n y^n xy && \text{(by inductive hypothesis)} \\ &= x^n x y^n y && \text{(by commutativity of multiplication)} \\ &= x^{n+1}y^{n+1} && \text{(by Definition 4.3.9 once again)} \end{aligned}$$

3. Show that $(x^n)^m = x^{nm}$. We induct on n while keeping m fixed.

   For the base case $n = 0$, we have $(x^n)^m = 1^m = 1$, since $1^m = 1$ for all natural number m[14]. On the other hand, $x^{nm} = x^{0m} = 1$. Thus, both sides are equal, and the base case is done.

   Now suppose inductively that $(x^n)^m = x^{nm}$. Then we have:

$$\begin{aligned} (x^{n+1})^m &= (x^n x)^m && \text{(by Definition 4.3.9)} \\ &= (x^n)^m x^m && \text{(proved in 2. from this exercise)} \\ &= x^{nm}x^m && \text{(by inductive hypothesis)} \\ &= x^{nm+m} && \text{(proved in 1. from this exercise)} \\ &= x^{(n+1)m} \end{aligned}$$

   This closes the induction.

4. Show that if $n > 0$, then $x^n = 0$ iff $x = 0$. For that, let's induct on n. Here the base case starts with $n = 1$ since we suppose $n > 0$. For $n = 1$, $x^1 = x$, thus we obviously have $x^1 = 0 \Leftrightarrow x = 0$ since both objects are equal.

   Now suppose inductively that $x^n = 0$ iff $x = 0$. We must show that $x^{n+1} = 0$ iff $x = 0$. Here we'll need the following lemma:

   Lemma. *Let x, y be rational numbers. Then, if $xy = 0$, we have either $x = 0$ or $y = 0$.*

   Proof. Let's denote $x = a /\!/ b$ and $y = c /\!/ d$. By Definition 4.2.2, $xy = (ac) /\!/ (bd)$. Thus, since $xy = 0$, we have $ac = 0$ (see Tao's remark p. 83). And, by Proposition 4.1.8, we have either $a = 0$ or $c = 0$. In the first case, this means that $x = 0$; in the second case this means that $y = 0$. □

   Now go back to the main proof. First, if $x = 0$, we have $x^{n+1} = x^n x = 0^n \times 0 = 0$. Conversely, if $x^{n+1} = 0$, then $x^n x = 0$. According to the previous lemma, this means that either $x^n = 0$ or $x = 0$. In the second case, we are done. In the first case, the induction hypothesis also allows to conclude that $x^n = 0$. This closes the induction.

[14] This can easily be proved by induction, which we'll not write formally here.

5. Show that if $x \geqslant y \geqslant 0$, then $x^n \geqslant y^n \geqslant 0$. Let's induct on n.

   For the base case $n = 0$, $x^0 = y^0 = 1$. Thus in particular we have indeed $x^0 \geqslant y^0 \geqslant 0$.

   Now suppose inductively that $x^n \geqslant y^n \geqslant 0$, and show that $x^{n+1} \geqslant y^{n+1} \geqslant 0$. We start from $x^n \geqslant y^n \geqslant 0$ and multiply all terms by x (which preserves inequality since x is supposed to be positive): we get $x^{n+1} \geqslant xy^n \geqslant 0$. If we start from $x \geqslant y \geqslant 0$ and multiply all terms by y^n (which is also positive by induction hypothesis), we get $y^n x \geqslant y^{n+1} \geqslant 0$. Now combine all those inequalities:

   $$x^{n+1} \geqslant xy^n \geqslant y^{n+1} \geqslant 0$$

   This closes the induction.

6. Show that $|x^n| = |x|^n$. Let's induct on n.

   For the base case $n = 0$, we have $|x^n| = |x^0| = |1| = 1$; and $|x|^n = |x|^0 = 1$. Thus both sides are equal, and the base case is done.

   Now suppose that $|x^n| = |x|^n$ and show that $|x^{n+1}| = |x|^{n+1}$. We have:

   $$\begin{array}{rcll} |x^{n+1}| & = & |x^n x| & \text{(by Definition 4.3.9)} \\ & = & |x^n| \cdot |x| & \text{(by Proposition 4.3.3d)} \\ & = & |x|^n \cdot |x| & \text{(by inductive hypothesis)} \\ & = & |x|^{n+1} & \end{array}$$

   This closes the induction.

Exercise 4.3.4. — *Prove Proposition 4.3.12.*

This is essentially the same exercise as 4.3.3, but dealing with integer exponents (instead of natural exponents). The claims to prove are the following (and once again, they are relabeled):

1. Prove that $x^n x^m = x^{n+m}$. Let's distinguish three cases:

   - If $n, m \geqslant 0$, then this is simply Proposition 4.3.10(a).
   - If $n, m < 0$, then $n = -p$ and $m = -q$ with p, q positive natural numbers. Thus, $x^n x^m = (1/x^p) \cdot (1/x^q) = 1/(x^p x^q)$ by Definition 4.2.2. But since p, q are positive, this is also equal to $1/(x^{p+q})$ according to Proposition 4.3.10(a). This can also be written $x^{-(p+q)}$ by Definition 4.3.11, which is finally equal to x^{n+m}.
   - If $n \geqslant 0$ and $m < 0$ (or inversely, since they are exchangeable), then $m = -q$ with q a positive natural number. Thus, $x^n x^m = x^n \times (1/x^q) = x^n/x^q$. We will (once again) split into two cases:
     - if $n \geqslant -m$, i.e. if $n - q \geqslant 0$, then we can note that $x^{n-q} \cdot x^q = x^n$ according to Proposition 4.3.10(a). Thus, let's multiply both sides of this equality by x^{-q} to get $x^{n-q} = x^n x^{-q}$; which can be rewritten $x^{n+m} = x^n x^m$ as required.
     - if $n < -m$, i.e. $q - n > 0$, then we can note that $x^{q-n} x^n = x^q$ according to Proposition 4.3.10(a). Also, since $n - q < 0$, according to Definition 4.3.11, we have $x^{n-q} = 1/x^{q-n}$. Let's multiply both sides by $1/x^n$, to get $x^{n-q}/x^n = 1/(x^{q-n}x^n) = 1/x^q = x^{-q}$. Finally, multiply both sides by x^n to get $x^{n+m} = x^n x^m$.

2. Prove that $(x^n)^m = x^{nm}$.

3. Show that $(xy)^n = x^n y^n$. If $n \geqslant 0$, this is simply Proposition 4.3.10(a). So let's consider the case $n < 0$. In this case, $n = -p$, with p a positive natural number. Thus we have successively:

$$\begin{array}{rcll} (xy)^n & = & (xy)^{-p} & \\ & = & 1/(xy)^p & \text{(by Definition 4.3.11)} \\ & = & 1/(x^p y^p) & \text{(Proposition 4.3.10(a))} \\ & = & 1/(x^p) \times 1/(y^p) & \text{(Definition 4.2.2)} \\ & = & x^{-p} \times y^{-p} & \text{(by Definition 4.3.11)} \\ & = & x^n \times y^n & \end{array}$$

4. Show that if $x \geqslant y > 0$, then $x^n \geqslant y^n > 0$ if n is positive, and $0 < x^n \leqslant y^n$ if n is negative.

   - If $n > 0$, according to Proposition 4.3.10(c), we already have $x^n \geqslant y^n \geqslant 0$, so that we just have to show that the rightmost inequality is strict, i.e. that $y^n > 0$. To show that, we only need to prove $y^n \neq 0$. For the sake of contradiction, let's suppose that $y^n = 0$. Our starting hypothesis was $x \geqslant y > 0$, thus we know that $y \neq 0$. According to Proposition 4.3.10(b), we can't have both $y \neq 0$ and $y^n = 0$, this is a contradiction. Thus, we indeed have $y^n \neq 0$, which shows the inequality $x^n \geqslant y^n > 0$ as required.
   - If $n < 0$, this includes an important result, which is that taking the inverse reverses order. Indeed, let's begin by proving that if $x \geqslant y > 0$, then $1/x \leqslant 1/y$. Since both x and y are positive, their product xy is also positive, and $1/(xy)$ is also positive. Following Proposition 4.2.9(e), we can multiply both sides of $x \geqslant y$ by $1/(xy)$ to get $1/y \geqslant 1/x$. Then, we immediately get $(1/y)^p \geqslant (1/x)^p$ for any positive number p by Proposition 4.3.10(c), which can be rewritten $y^n \geqslant x^n$ with $n = -p$ negative. And since both numbers are positive (because x and y are positive), the claim follows.

5. Prove that if $x, y > 0$ and $n \neq 0$, then $x^n = y^n \implies x = y$. Let's consider two cases: $n > 0$ and $n < 0$.

   First, if $n > 0$, suppose for the sake of contradiction that we have both $x^n = y^n$ and $x \neq y$. According to the trichotomy of rationals (Lemma 4.2.7), this last claim means that we have either $x > y$ or $y > x$. Since x and y are exchangeable, we only prove the first case here, $x > y$. In this case, Proposition 4.3.10(c) leads to $x^n > y^n$, which is obviously not compatible with our initial hypothesis $x^n = y^n$. A similar contradiction follows in the case $y > x$. Thus, both $x > y$ and $y > x$ are impossible, and the only possibility is $x = y$.

   Now, if $n < 0$, then $n = -p$, with p a positive natural number. Suppose that $x^n = y^n$, i.e. that $x^{-p} = y^{-p}$, or finally $1/x^p = 1/y^p$. From this last equality, by multiplying both sides by $x^p y^p$, we get $y^p = x^p$. We are thus back in the previous case, and obtain $x = y$.

6. Prove that $|x^n| = |x|^n$. If $n \geqslant 0$, this is simply Proposition 4.3.10(d). So let's consider the case $n < 0$. We'll need a quick lemma:

Lemma. *For all rationals $x \neq 0$, we have $|1/x| = 1/|x|$.*

Proof. If $x > 0$, there is nothing to show. If $x < 0$, then $1/x$ is also negative[15]. Thus, $1/|x| = 1/(-x)$; and $|1/x| = -(1/x)$. And we have clearly $1/(-x) = -(1/x)$ because $1/(-x) + 1/x = 0$. □

In this case, $n = -p$, with p a positive natural number. We have successively:

$$\begin{array}{rcll} |x^n| & = & |x^{-p}| & \\ & = & |1/(x^p)| & \text{(by Definition 4.3.11)} \\ & = & |(1/x)^p| & \text{(Proposition 4.3.12(a))} \\ & = & |1/x|^p & \text{(Proposition 4.3.10(d))} \\ & = & (|1|/|x|)^p & \text{(lemma introduced just above)} \\ & = & 1/|x|^p & \text{(Proposition 4.3.12(a))} \\ & = & |x|^{-p} & \text{(Definition 4.3.11)} \\ & = & |x|^n & \end{array}$$

Exercise 4.3.5. — *Prove that $2^N \geqslant N$ for all positive integers N.*

Let's use induction on N. Since we only consider positive integers, we have here $N \geqslant 1$, and in particular, the base case starts at $N = 1$.

For the base case $N = 1$, the assertion is true, since we have indeed $2^1 \geqslant 1$.

Now suppose inductively that $2^N \geqslant N$, and show that $2^{N+1} \geqslant N + 1$. We have $2^{N+1} = 2^N \times 2 \geqslant N \times 2$ by induction hypothesis. But we know that $2N = N + N$ (recall Definition 2.3.1 for instance), thus we can rewrite this as $2^{N+1} \geqslant N + N$. And since $N \geqslant 1$, we finally get $2^{N+1} \geqslant N + 1$.

Exercise 4.4.1. — *Prove Proposition 4.4.1.*

We have to prove that, for any rational number x, there exists an integer n such that $n \leqslant x < n + 1$. Let's proceed through the following four steps:

- Suppose that $x \in \mathbb{Q}_+$. Thus, $x = a/b$, with a and b natural numbers. According to Proposition 2.3.9, there exists $n, r \in \mathbb{N}$ such that $a = bn + r$, with $0 \leqslant r < b$. By dividing all terms by b, this also means that $x = a/b = n + r/b$, with $0 \leqslant r/b < 1$.

  Since $0 \leqslant r/b < 1$, we have $n \leqslant n + r/b < n + 1$, i.e. $n \leqslant x < n + 1$, as required.

- Now suppose that $x \in \mathbb{Q}^\star_-$. Consequently, $-x \in \mathbb{Q}_+$, and we are back in the previous case: there exists a natural number n such that $n \leqslant -x < n + 1$, i.e. $-n - 1 < x \leqslant -n$. Now we have two possible cases:

  - if $x = -n$, then let be $m = -n$. Thus, $m - 1 < x \leqslant m$, and then $m \leqslant x < m + 1$, as required.
  - if $x \neq -n$, then let be $m = -n - 1$. Thus, $m < x \leqslant m + 1$, i.e. $m - 1 \leqslant x < m$. And by denoting $p = m - 1$, we have $p \leqslant x < p + 1$ as required.

[15] Formally, see Definition 4.2.6, and note that $a \mathbin{//} (-b) = (-a) \mathbin{//} b$ if a and b are positive integers.

- Let's prove that this integer n is unique. Suppose that we have two integers m, n such that:

$$n \leqslant x < n+1 \tag{3}$$
$$m \leqslant x < m+1 \tag{4}$$

From (4), we also have $-m-1 < -x \leqslant -m$. And, by adding this inequality to (3), we get $n-m-1 < 0 < n-m+1$. The left-hand side says that $n < m+1$, i.e. that $n \leqslant m$ (recall Proposition 2.2.12 (e)). Similarly, the right-hand side says that $n > m-1$, i.e. that $n \geqslant m$. Thus, we have both $n \leqslant m$ and $n \geqslant m$, which means that $n = m$.

- Finally, this means in particular that there exists a natural number N such that $N > x$. Indeed, if x is negative, then $N = 0$ is suitable; and if x is positive, then N is directly given by $N = \lfloor x \rfloor + 1$.

Exercise 4.4.2. — *A sequence $a_0, a_1, a_2, \ldots$ of numbers (natural numbers, integers, rationals, or reals) is said to be in* infinite descent *if we have $a_n > a_{n+1}$ for all natural numbers n (i.e., $a_0 > a_1 > a_2 > \ldots$).*

1. *Prove the principle of infinite descent: that it is not possible to have a sequence of natural numbers which is in infinite descent.*
2. *Does the principle of infinite descent work if the sequence $a_1, a_2, a_3, \ldots$ is allowed to take integer values instead of natural number values? What about if it is allowed to take positive rational values instead of natural numbers? Explain.*

We follow the hints given by Terence Tao.

1. Assume for the sake of contradiction that we have a sequence of natural numbers (a_n) which is in infinite descent. Let k be a natural number, and P_k be the property "$a_n \geqslant k$ for all natural numbers n". Let's induct on k.

   For the base case, P_0 is true since a_n are natural numbers for all n, so that $a_n \geqslant 0$ for all n by definition.

   Now let's suppose inductively that P_k is true, i.e. that $a_0 > a_1 > a_2 > \ldots \geqslant k$. If we had $a_p = k$ for one given natural number p, then we would have $k = a_p > a_{p+1}$. But also, $a_{p+1} > a_{p+2} > ... > k$ by induction hypothesis. However, the inequality $k \geqslant a_{p+1} > k$ is a contradiction, so that $a_n \neq k$ for all n. Thus, P_{k+1} is also true: we have $a_n > k+1$ for all n.

   However, having $a_n > k$ for all natural numbers k, n is a contradiction. Indeed, for $k = a_0$ and $n = 1$, we have $a_1 > a_0$, which contradicts the fact that (a_n) is in infinite descent.

   Thus, there are no such sequence of natural numbers.

2. A general note: to prove that the infinite descent principle does not work for integers or rationals, it is enough to find *one* sequence of such numbers which is actually in infinite descent. Instead of a formal proof as in the previous case, a simple counterexample will do the trick.

- If the sequence $a_0 > a_1 > \dots$ can take integer values, lets define the sequence by $a_n = -n$. By definition, we have $a_n > a_{n+1}$ for all natural number n (since $-n > -n-1$, as a simple induction will show).
- If the sequence $a_0 > a_1 > \dots$ can take rational values, lets define the sequence by $a_n = 1/n$. Thus, we have $a_n > a_{n+1}$ for all natural number n, since $1/n > 1/(n+1)$. (This can be shown as follows: $1/n - 1/(n+1) = 1/(n(n+1)) > 0$.)

5. The real numbers

Exercise 5.1.1. — *Prove Lemma 5.1.15, i.e. that every Cauchy sequence is bounded.*

Let $(a_n)_{n=1}^{\infty}$ be a Cauchy sequence.

- By definition 5.1.8, for every rational $\varepsilon > 0$, there exists a natural number N such that if $j, k \geqslant N$, then $d(a_j, a_k) \leqslant \varepsilon$. In particular, let's rephrase this statement with the arbitrary value $\varepsilon = 1$ (valid, since 1 is a positive rational): there exists a natural number N such that if $j, k \geqslant N$, then $|a_j - a_k| \leqslant 1$.

  Since $N \geqslant N$, we can take in particular $k = N$ to get yet another particular formulation: if $j \geqslant N$, then $|a_j - a_N| \leqslant 1$.

  According to Proposition 4.3.3(b), we have $|x + y| \leqslant |x| + |y|$ for all rationals x, y. Let's consider $x = a_j - a_N$ and $y = a_N$: this leads to $|a_j| \leqslant |a_j + a_N| + |a_N|$, i.e. $|a_j| - |a_N| \leqslant |a_j - a_N|$.

  Thus, this means that $|a_j| - |a_N| \leqslant |a_j - a_N| \leqslant 1$ as soon as $j \geqslant N$, i.e. that $|a_j| \leqslant 1 + |a_N|$ for $j \geqslant N$. We have bounded part of the infinite sequence.

- The other part is simply the finite sequence $a_0, a_1, \cdots, a_{N-1}$. By Lemma 5.1.14, this finite sequence is necessarily bounded by a rational number M.

- Finally, let's consider the rational number $B = 1 + |a_N| + M$. Since we have both $B \geqslant M$ and $B \geqslant 1 + |a_N|$, both the infinite sequence $(a_n)_{n=N}^{\infty}$ and the finite sequence $a_0, \cdots, a_{N-1}$ are bounded by B. Thus, the whole Cauchy sequence $(a_n)_{n=1}^{\infty}$ is bounded by B.

Exercise 5.2.1. — *Show that if $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ are eventually ε-close, then $(a_n)_{n=1}^{\infty}$ is a Cauchy sequence if and only if $(b_n)_{n=1}^{\infty}$ is a Cauchy sequence.*

First note that $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ are exchangeable here, so that showing only one direction ("if $(a_n)_{n=1}^{\infty}$ is Cauchy, then $(b_n)_{n=1}^{\infty}$ is Cauchy") will be enough.

Let be $\varepsilon > 0$ a positive rational. Since $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ are eventually ε-close, there exists a natural number N_1 such that $n \geqslant N_1 \Longrightarrow |a_n - b_n| \leqslant \frac{\varepsilon}{3}$. Furthermore, since $(a_n)_{n=1}^{\infty}$ is a Cauchy sequence, there exists a natural number N_2 such that $j, k \geqslant N_2 \Longrightarrow |a_j - a_k| \leqslant \frac{\varepsilon}{3}$.

Let be $N = \max(N_1, N_2)$. If $j, k \geqslant N$, then we have:

$$\begin{aligned} |b_j - b_k| &= |b_j - a_j + a_j - a_k + a_k - b_k| \\ &\leqslant |b_j - a_j| + |a_j - a_k| + |a_k - b_k| \quad \text{(by triangle inequality)} \\ &\leqslant \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} \\ &\leqslant \varepsilon \end{aligned}$$

which means that $(b_n)_{n=1}^{\infty}$ is a Cauchy sequence.