Reading: Analysis I by Terence Tao

Hanson Char

May 21, 2025

Contents

Chapter 2 Starting at the Beginning: The Natural Numbers

2.1 The Peano axioms

How are we to define what the natural numbers are?

Axiom 2.1 (Zero) *0 is a natural number.*

Axiom 2.2 (Successor) *If n is a natural number, then n++ is also a natural number.*

(How do we prevent this number system from wrapping around?)

Axiom 2.3 (Zero not a successor) *0 is not the successor of any natural number; i.e., we have $n\text{++} \neq 0$ for every natural number n.*

Axiom 2.4 (Unique successor) *Different natural numbers must have different successors; i.e., if n, m are natural numbers and $n \neq m$, then $n\text{++} \neq m\text{++}$. Equivalently, if $n\text{++} = m\text{++}$, then we must have $n = m$.*

(How do we prevent rouge elements from being included in this number system?)

Axiom 2.5 (Mathematical Induction) (Principle of mathematical induction.) *Let $P(n)$ be any property pertaining to a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n{+}{+})$ is also true. Then $P(n)$ is true for every natural number n.*

Proposition Template 2.1.11 (Property P(n)) *A certain property $P(n)$ is true for every natural number n.*

Proof Template We use induction. We first verify the base case $n = 0$, i.e., we prove $P(0)$. (Insert proof of $P(0)$ here.) Now suppose inductively that n is a natural number, and $P(n)$ has already been proven. We now prove $P(n{+}{+})$. (Insert proof of $P(n{+}{+})$, assuming that $P(n)$ is true, here.) This closes the induction, and thus $P(n)$ is true for all numbers n.

Assumption 2.6 (Natural Numbers) (Informal) There exists a number system $\boldsymbol{N}$, whose elements we will call *natural numbers*, for which Axioms 2.1-2.5 are true.

Proposition 2.1.16 (Recursive definitions) *Suppose for each natural number n, we have some function $f_n : \boldsymbol{N} \to \boldsymbol{N}$ from the natural numbers to the natural numbers. Let c be a natural number. Then we can assign a unique natural number a_n to each natural number n, such that $a_0 = c$ and $a_{n++} = f_n(a_n)$ for each natural number n.*

- In a system which had some sort of wrap-around, recursive definitions would not work because some elements of the sequence would constantly be redefined.

- In a system which had superfluous elements such as 0.5, the element 0.5 would never be defined.

My View

1. Since a unique natural nubmer a_n is assigned to each n, the assignment $n \to a_n$ is injective. However, a_n may not span the entire domain of $\boldsymbol{N}$, so the assignment is not surjective.

2. The Recursive definitions look naively obvious, but is actually quite subtle. In particular, all the Peano axioms had to be used to prove it.

2.2 Addition

Definition 2.2.1 (Addition of natural numbers) Let m be a natural number. To add zero to m, we define $0 + m := m$. Now suppose inductively that we have defined how to add n to m. Then we can add $n{+}{+}$ to m by defining $(n{+}{+}) + m := (n + m){+}{+}$.

Exercise 2.2.1a. Prove using Axioms 2.1, 2.2, and induction (Axiom 2.5), that the sum of two natural numbers is again a natural number.

Attempt: We use induction. Let n and m be natural numbers. By definition (2.2.1 of addition), $0 + m = m$. The base case holds since both 0 (by Peano Axiom 2.1) and m (given) are natural numbers. Suppose $n + m$ is a natural number, we wish to show that $(n{+}{+}) + m$ is also a natural number. By definition (2.2.1 of addition), $(n{+}{+}) + m = (n + m){+}{+}$. Since $n + m$ is a natural number by the inductive hypothesis, $(n + m){+}{+}$ is also a natural number by Peano Axiom 2.2. Therefore, $(n{+}{+}) + m$ is a natural number. This closes the induction. □

Lemma 2.2.2 (Adding zero) *For any natural number n, $n + 0 = n$.*

Lemma 2.2.3 (Adding successor) *For any natural number n and m, $n + (m{+}{+}) = (n + m){+}{+}$.*

Exercise 2.2.3a. As a particular corollary of Lemma 2.2.2 and Lemma 2.2.3 we see that $n{+}{+} = n + 1$. Why?

Attempt: By Lemma 2.2.2, $n{+}{+} = (n + 0){+}{+}$, which in turn equals $n + (0{+}{+})$ by Lemma 2.2.3. But $0{+}{+}$ is just 1 by notation. Therefore $n{+}{+} = n + 1$ as claimed. □

Proposition 2.2.4 (Addition is commutative) *For any natural number n and m, $n + m = m + n$.*

Proposition 2.2.5 (Addition is associative) *For any natural number a, b, c, we have $(a + b) + c = a + (b + c)$.*

Proposition 2.2.6 (Cancellation law) *Let a, b, c be natural numbers such that $a + b = a + c$. Then we have $b = c$.*

Definition 2.2.7 (Positive natural numbers) A natural number n is said to be positive iff it is not equal to 0. ("iff" is shorthand for "if and only if" - see Section A.1).

Proposition 2.2.8 (Adding two positive natural numbers) *If a is positive and b is a natural number, then $a + b$ is positive (and hence $b + a$ is also, by Proposition 2.2.4).*

Corollary 2.2.9 (When sum equals zero) *If a and b are natural numbers such that $a + b = 0$, then $a = 0$ and $b = 0$.*

Proof Attempt: By Proposition 2.2.8, if either a or b is positive, then $a + b$ must be positive. Therefore, if $a + b$ is zero, then a and b must both be zeros by contrapositive. □

Lemma 2.2.10 (Unique predecessor) *Let a be a positive number. Then there exists exactly one natural number b such that $b{+}{+} = a$.*

Definition 2.2.11 (Ordering of the natural numbers) Let n and m be natural numbers. We say that n is *greater than or equal to* m, and write $n \geq m$ or $m \leq n$, iff we have $n = m + a$ for some natural number a. We say that n is *strictly greater than* m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.

Proposition 2.2.12 (Basic properties of order for natural numbers)
Let a, b, c be natural numbers. Then

(a) (Order is reflexive) $a \geq a$.

(b) (Order is transitive) If $a \geq b$ and $b \geq c$, then $a \geq c$.

(c) (Order is anti-symmetric) If $a \geq b$ and $b \geq a$, then $a = b$.

(d) (Addition preserves order) $a \geq b$ if and only if $a + c \geq b + c$.

(e) $a < b$ if and only if $a{+}{+} \leq b$.

(f) $a < b$ if and only if $b = a + d$ for some positive number d.

Proposition 2.2.13 (Trichotomy of order for natural numbers) *Let a and b be natural numbers. Then exactly one of the following statements is true: $a < b, a = b$, or $a > b$.*

(Remark: Seemingly too obvious a proposition, but the proof is anything but obvious - it involves both "maximum one" and "at least one" with induction!)

Proof. This is only a sketch of the proof; the gaps will be filled in Exercise 2.2.4. First we show that we cannot have more than one of the statements $a < b, a = b, a > b$ holding at the same time. If $a < b$ then $a \neq b$ by definition, and if $a > b$ then $a \neq b$ by definition. If $a > b$ and $a < b$ then by Proposition 2.2.12 we have $a = b$, a contradiction. Thus no more than one of the statements is true. Now we show that at least one of the statements is true. We keep b fixed and induct on a. When $a = 0$ we have $0 \leq b$ for all b (why?), so we have either $0 = b$ or $0 < b$, which proves the base case. Now suppose we have proven the proposition for a, and now we prove the proposition for a++. From the trichotomy for a, there are three cases: $a < b, a = b$, and $a > b$. If $a > b$, then $a\text{++} > b$ (why?). If $a = b$, then $a\text{++} > b$ (why?). Now suppose that $a < b$. Then by Proposition 2.2.12, we have $a\text{++} \leq b$. Thus either $a\text{++} = b$ or $a\text{++} < b$, and in either case we are done. This closes the induction.

Proposition 2.2.14 (Strong principle of induction) *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 $m \geq m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leq m' < m$, 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 $m \geq m_0$.*

— Exercises —

Exercise 2.2.1. Prove Proposition 2.2.5. (Hint: fix two of the variables and induct on the third.)

Attempt: We shall induct on a (keeping b and c fixed). The base case holds since $(0+b)+c = b+c = 0+(b+c)$ by definition of addition. Now suppose inductively that $(a+b)+c = a+(b+c)$, we wish show that $((a\text{++})+b)+c = (a\text{++})+(b+c)$. By definition of addition, $((a\text{++})+b)+c = (a+b)\text{++}+c = ((a+b)+c)\text{++}$. By the inductive hypothesis, $((a+b)+c)\text{++} = (a+(b+c))\text{++}$, which in turn is equal to $(a\text{++})+(b+c)$ by definition of addition. This completes the induction. □

Exercise 2.2.2. Prove Lemma 2.2.10. (Hint: use induction.)

Attempt 1: We shall induct on a. The base case $a = 0$ is vacuously true since a is not positive. Assume inductively that there exists exactly one natural number b such that $b\text{++} = a$ where a is a positive number. We wish to show that there exists exactly one natural number c such that $c\text{++} = a\text{++}$. By inductive hypothesis a is a positive number. By Exercise 2.2.3a, a++ is equal to $a+1$, which is positive by Proposition 2.2.8. But c must be equal to a such that $c\text{++} = a\text{++}$ by Peano Axiom 2.4. This completes the induction.

Attempt 2: Let a be a positive natural number. By Definition 2.2.7 of Positive natural numbers, a is not zero and Axiom 2.2 and Axiom 2.3 implies a is of the form $b\text{++} = a$ for some natural number b. By Axiom 2.4, b must be unique. This completes the proof. □

Exercise 2.2.3. Prove Proposition 2.2.12. (Hint: you will need many of the preceding propositions, corollaries and lemmas.)

Attempt:

(a) (Order is reflexive) 0 is a natural number by Axiom 2.1, and $a = a + 0$ by Lemma 2.2.2. Therefore, $a \leq a$ by Definition 2.2.11. □

(b) (Order is transitive) Since $a \geq b$ and $b \geq c$, by definition, $a = b + \delta$ and $b = c + \gamma$ for some natural number δ and γ. So $a = (c + \gamma) + \delta = c + (\gamma + \delta)$ by substitution and associativity. Therefore $a \geq c$ by definition. □

(c) (Order is anti-symmetric). Since $a \geq b$ and $b \geq a$, $a = b + c$ and $b = a + d$ for some natural numbers c and d. By substitution, $a = (a+d)+c$ which is equal to $a+(d+c)$ by associativity. By cancellation, $a = a+(d+c)$ iff $0 = d+c$, but this is possible only if both c and d are zeros by Axiom 2.3 and Corollary 2.2.9. We have $a = b + c$, and $b + c = b + 0 = b$ by substitution and Lemma 2.2.2. Therefore $a = b$. □

(d) (Addition preserves order). We start from the left hand side, and make use of iff in every step to get to the right-hand side. Since $a \geq b$, $a = b + \delta$ for some natural number δ by definition (2.2.11 of ordering). Now $a = b + \delta$ iff $a + c = (b + \delta) + c$ by the equality axiom of substitution (in the forward direction) and cancellation law (in the reverse direction). Then $a + c = (b + \delta) + c = b + \delta + c = (b + c) + \delta$ by associativity and commutativity. Therefore $a + c \geq b + c$ by definition. □

(e) We start from the right-hand side, and make use of iff in every step to get to the left hand side. Since $a\text{++} \leq b$, $a\text{++} + c = b$ for some natural number c by definition (2.2.11 of ordering). Then $(a + c)\text{++} = b$ by definition (2.2.1 of addition), $(a + c + 0)\text{++} = b$ by Lemma 2.2.2 and associativity, and $a + c + 0\text{++} = b$ by Lemma 2.2.3. But $c + 0\text{++}$ cannot possibly be equal to zero by Axiom 2.3. Therefore $a \neq b$ by Axiom 2.3, and $a < b$ by definition (2.2.11 of ordering). □

(f) By definition (2.2.11 of ordering), $a < b$ iff $a + d = b$ and $a \neq b$. But this is possible iff $d \neq 0$ by definition (2.2.1 of addition) and Axiom 2.3. Therefore d is positive by definition (2.2.11 of positive natural numbers). □

Exercise 2.2.4. Justify the three statements marked (why?) in the proof of Proposition 2.2.13.

1. When $a = 0$ we have $0 \leq b$ for all b (why?)

   Attempt. We shall induct on b. Let $b = 0$, and $0 \leq 0$ estbalishes the base case. Assume $0 \leq x$ for all natural numbers from 0 to b, we want to show $0 \leq x$ for all natural numbers from 0 to b++. Since $0 \leq b$, by definition (of ordering), $0 + c = b$ for some natural number c. Then $(0 + c)\text{++} = b\text{++}$ by the axiom of equality substitution, and $0 + c\text{++} = b\text{++}$ by Lemma 2.2.3. Given c is a natural number, so is c++ by Axiom 2.2. It follows $0 \leq b\text{++}$ by definition (of ordering). By the inductive hypothesis, $0 \leq x$ for all natural numbers from 0 to b, and we now know $0 \leq b\text{++}$. Therefore, $0 \leq x$ for all natural numbers from 0 to b++. This closes the induction. □

2. If $a > b$, then $a\text{++} > b$ (why?)

   Attempt. By definition (of ordering) $a > b$ iff $a = b + c$ and $a \neq b$ for some natural number c. Then $a\text{++} = (b + c)\text{++} = b + c\text{++}$ by axiom of equality substitution and by Lemma 2.2.3. By definition (of ordering) we see $a\text{++} \geq b$, and we want to show $a\text{++} \neq b$. Suppose the opposite that $a\text{++} = b$. Since $a = b + c$, $(b + c)\text{++} = b$ by substitution, and $b + c\text{++} = b$ by Lemma 2.2.3. By cancellation, $c\text{++} = 0$ which violates Axiom 2.3. Therefore the supposition is false and $a\text{++} \neq b$. Since $a\text{++} \geq b$ and $a\text{++} \neq b$, $a\text{++} > b$ by definition (of ordering). □

3. If $a = b$, then $a\text{++} > b$ (why?)

   Attempt. Given $a = b$, $a\text{++} = b\text{++} = (b + 0)\text{++} = b + 0\text{++}$ by axiom of equality substitution, Lemma 2.2.2 and Lemma 2.2.3. Hence $a\text{++} \geq b$ by definition of ordering. Also, $a\text{++} \neq a$. (Suppose otherwise that $a = a\text{++}$. So $a = a\text{++} = (a + 0)\text{++} = a + 0\text{++}$ by Lemma 2.2.2 and Lemma 2.2.3. By law of cancellation $0 = 0\text{++}$ which is impossible by Axiom 2.3.) Since $a = b$ and $a\text{++} \neq a$, $a\text{++} \neq b$. Since $a\text{++} \geq b$ and $a\text{++} \neq b$, $a\text{++} > b$. □

Exercise 2.2.5. Prove Proposition 2.2.14. (Hint: define $Q(n)$ to be the property that $P(m)$ is true for all $m_0 \leq m < n$; note that $Q(n)$ is vacuously true when $n < m_0$.)

Attempt. Let $Q(n)$ be the property that $P(m)$ is true for all $m_0 \leq m < n$. We shall induct on n. For the base case, $Q(0)$ is true iff $P(m)$ is true for all $m_0 \leq m < 0$. Since there is no natural number less than zero, Proposition 2.2.14 is vacuously true. Assume inductively the proposition holds for $Q(n)$. We wish to show that it also holds for $Q(n + 1)$. There are two possibilities: $n + 1 \leq m_0$ or $m_0 < n + 1$. In the first case, Proposition 2.2.14 is vacuously true since there is no element m in the interval $m_0 \leq m < n+1 \leq m_0$. For the second case, since Proposition 2.2.14 holds for $Q(n)$, $P(m)$ is true for $m_0 \leq m < n$, which implies $P(n)$ is true by the inductive hypothesis. So $P(m)$ is true for $m_0 \leq m < n+1$. Thus $Q(n+1)$ is true. This closes the 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 $m \leq n$; this is known as the *principle of backwards induction*. (Hint: apply induction to the variable n.)

Attempt. We shall induct on n. For the base case, let $n = 0$. $P(0)$ is true by supposition, and $m \leq 0$ iff $m = 0$, so $P(m)$ is trivially true for all $m \leq 0$. Assume inductively for a fixed n that if $P(n)$ is true, then $P(m)$ is true for all $m \leq n$. We want to show that if $P(n+1)$ is true, then $P(m)$ is true for all $m \leq n+1$. But if $P(n+1)$ is true, $P(n)$ must be true by the given property. By the inductive property, $P(m)$ is true for all $m \leq n$. Therefore, $P(m)$ is true for all $m \leq n+1$. This closes the induction. □

Exercise 2.2.7. 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, $P(m{+}{+})$ is true. Show that if $P(n)$ is true, then $P(m)$ is true for all $m \geq n$. (This principle is sometimes referred to as the *principle of induction starting from the base case n*.)

Attempt by contradiction. We shall prove by contradiction. Assume $P(n)$ is true and there exists $P(m)$ that is false for $m \geq n$. Let a be the smallest such m. Since $P(n)$ is true and $P(a)$ is false, we know that $a \neq n$. Thus, $a > n$. By Lemma 2.2.10, there exists exactly one natural number b such that $b{+}{+} = a$. Since $P(b)$ is true, $P(b{+}{+})$ is also true by the given property. Therefore, $P(a)$ is true, a contradiction. Note $P(b)$ cannot be false as that would contradict a being the smallest counter example. Hence the assumption must be false. We conclude that if $P(n)$ is true, then $P(m)$ is true for all $m \geq n$. □

Attempt by induction. Let $Q(n) = P(m+n)$ for some natural number m and n. Assume $P(m)$ is true, we want to show $Q(n)$ is true for all natural numbers. The base case when $n = 0$ holds since $Q(0) = P(m)$ which is true by assumption. Suppose inductively that $Q(n)$ is true. We wish to show $Q(n+1)$ is also true. By definition, $Q(n) = P(m+n)$. Since $Q(n)$ is true by the inductive hypothesis, $P(m+n)$ is true which implies $P((m+n){+}{+})$ is true by the given property. By Lemma 2.2.3, $P((m+n){+}{+}) = P(m+(n{+}{+}))$, which is equal to $P(m+(n+1))$ by Exercise 2.2.3a. Thus $Q(n+1)$ is true. This closes the induction. □

2.3 Multiplication

Definition 2.3.1 (Multiplication of natural numbers) Let m be a natural number. To multiply zero to m, we define $0 \times m := 0$. Now suppose inductively that we have defined how to multiply n to m. Then we can multiply $n{+}{+}$ to m by defining $(n{+}{+}) \times m := (n \times m) + m$.

Lemma 2.3.2 (Multiplication is commutative)
Let n,m be natural numbers. Then $n \times m = m \times n$.

Lemma 2.3.3 (Positive natural numbers have no zero divisors) *Let* n, m *be natural numbers. Then* $n \times m = 0$ *if and only if at least one of* n, m *is equal to zero. In particular, if* n *and* m *are both positive, then* nm *is also positive.*

Lemma 2.3.4 (Distributive law) *For any natural numbers* a, b, c, *we have* $a(b+c) = ab + ac$ *and* $(b+c)a = ba + ca$.

Proof Attempt. Since multiplication is commutative, we only need to show the first identity $a(b+c) = ab + ac$. We keep b and c fixed, and use induction on a. Let's prove the base case $0(b+c) = 0 \times b + 0 \times c$. By Exercise 2.2.1a (the sum of two natural numbers is again a natural number), $b + c$ is a natural number, so the left-hand side is zero by definition of multiplication (2.3.1). The right-hand side is also zero by definition of multiplication and addition, so we are done with the base case. Suppose inductively that $a(b+c) = ab + ac$. We wish to show that $(a{+}{+})(b+c) = (a{+}{+})b+(a{+}{+})c$. By definition of multiplication, $(a{+}{+})(b+c)$ is equal to $a(b+c)+(b+c)$, which is equal to $ab + ac + (b+c)$ by applying the inductive hypothesis. Then $ab + ac + (b+c)$ is equal to $(ab+b) + (ac+c)$ by rearranging terms, and $(ab+b)+(ac+c) = (a{+}{+})b + (a{+}{+})c$ by definition of multiplication. This closes the induction.

Proposition 2.3.5 (Multiplication is associative) *For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.*

Proposition 2.3.6 (Multiplication preserves order) *If a, b are natural numbers such that $a < b$, and c is positive, then $ac < bc$.*

Corollary 2.3.7 (Cancellation law) *Let a, b, c be natural numbers such that $ac = bc$, and c is non-zero. Then $a = b$.*

Proposition 2.3.9 (Euclid's division lemma) *Let n be a natural number, and let q be a positive number. Then there exist natural numbers m,r such that $0 \le r < q$ and $n = mq + r$.*

Definition 2.3.11 (Exponentiation for natural numbers) Let m be a natural number. To raise m to the power 0, we define $m^0 := 1$; in particular, we define $0^0 := 1$. Now suppose recursively that m^n has been defined for some natural number n, then we define $m^{n{+}{+}} := m^n \times m$.

— Exercises —

Exercise 2.3.1. Prove Lemma 2.3.2. (Hint: modify the proofs of Lemmas 2.2.2, 2.2.3 and Proposition 2.2.4.)

Attempt. We shall make use of two additional lemmas to prove Lemma 2.3.2.

Lemma 2.3.1a: $m \times 0 = 0$. Note that we cannot deduce this immediately from $0 \times m = 0$ because we do not know yet that $0 \times m = m \times 0$. We use induction. The base case $0 \times 0 = 0$ follows sine we know that $0 \times m = 0$ for every natural number m, and 0 is a natural number. Now suppose inductively that $m \times 0 = 0$. We wish to show that $(m{+}{+}) \times 0 = 0$. By definition of multiplication, $(m{+}{+}) \times 0 = (m \times 0) + 0$, which is equal to $0 + 0$ since $m \times 0 = 0$ by the inductive hypothesis. Finally, $0 + 0 = 0$ by definition (of addition). This closes the induction.

Lemma 2.3.1b: $m \times (n{+}{+}) = (m \times n) + m$. We shall induct on m. The base case follows since the left-hand side $0 \times (n{+}{+}) = 0$ by definition of multiplication, and the right-hand side $(0 \times n) + 0 = 0{+}0 = 0$ by definition of multiplication and addition. Now we assume inductively that $m \times (n{+}{+}) = (m \times n) + m$, we wish to show that $(m{+}{+}) \times (n{+}{+}) = ((m{+}{+}) \times n) + (m{+}{+})$. The left-hand side is $(m \times (n{+}{+})) + (n{+}{+})$ by definition of multiplication, which is equal to $((m \times n) + m) + (n{+}{+})$ by the inductive hypothesis. Then $((m \times n) + m) + (n{+}{+}) = (m \times n) + m + (n{+}{+})$ by associativity. Similarly, the right-hand side is $((m \times n) + n) + (m{+}{+})$ by definition of multiplication, which is equal to $(m \times n) + [n + (m{+}{+})]$ by associativity. But we know that $[n + (m{+}{+})] = (n+m){+}{+} = (m+n){+}{+} = m + (n{+}{+})$ by Lemma 2.2.3 and commutativity. Therefore the right-hand side is equal to $(m \times n) + m + (n{+}{+})$. Thus both sides are equal to each other, and we have closed the induction.

We are now ready to prove $n \times m = m \times n$ by induction on n. By Lemma 2.3.1a, the base case $0 \times m = 0 = m \times 0$ follows. Now suppose inductively that $n \times m = m \times n$. We wish to show $(n{+}{+}) \times m = m \times (n{+}{+})$. The left-hand side is equal to $(n \times m) + m$ by definition of multiplication, and is equal to $(m \times n) + m$ by the inductive hypothesis. But the right-hand side is equal to $(m \times n) + m$ by Lemma 2.3.1b. Thus both sides are equal to each other, and we have closed the induction. □

Exercise 2.3.2. Prove Lemma 2.3.3. (Hint: prove the second statement first.)

Attempt. We want to prove that $n \times m = 0$ iff $n = 0$ or $m = 0$. We start with the reverse direction. If $n = 0$, then $0 \times m = 0$ by definition of multiplication. If $m = 0$, then $n \times 0 = 0$ by Lemma 2.3.1a. So the reverse direction holds. For the forward direction, we shall prove by contradiction. Assume the opposite that $n \times m = 0$, but both n and m are positive natural numbers. Let $n = \nu{+}{+}$ and $m = \mu{+}{+}$ for some natural numbers ν and μ. Then $n \times m = (\nu{+}{+}) \times (\mu{+}{+}) = (\nu \times (\mu{+}{+})) + (\mu{+}{+})$ by definition of multiplication, which is equal to $((\nu \times (\mu{+}{+})) + \mu){+}{+}$ by Lemma 2.2.3. So $n \times m = k{+}{+}$ where $k = ((\nu \times (\mu{+}{+})) + \mu)$. Since k is a natural number, $k{+}{+}$ must be positive; and therefore $n \times m$ is positive. But this contradicts the assumption that $n \times m$ is zero. Therefore, if $n \times m = 0$, then $n = 0$ or $m = 0$. This completed the proof. □

Exercise 2.3.3. Prove Proposition 2.3.5. (Hint: modify the proof of Proposition 2.2.5 and use the distributive law.)

Attempt. We keep b and c fixed, and induct on a. Let's prove the base case $(0 \times b)c = 0(bc)$. The left-hand side is zero, since $(0 \times b)c = 0 \times c = 0$ by definition of multiplication (2.3.1). The right-hand side is also zero, since bc is a natural number, so $0(bc) = 0$ by definition of multiplication. We are done with the base case. Suppose inductively that $(ab)c = a(bc)$. We wish to show $((a{+}{+})b)c = (a{+}{+})(bc)$. On the left-hand side, $((a{+}{+})b)c = a(bc) + bc$ by definition of multiplication. By the distributive law (2.3.4), $(ab + b)c$ is equal to $(ab)c + bc$, which is equal to $a(bc) + bc$ by the inductive hypothesis. On the right-hand side, $(a{+}{+})(bc) = a(bc) + bc$ by definition of multiplication. Thus the two sides are equal to each other, and we can close the induction. □

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

Attempt.

$$\begin{aligned}
(a+b)^2 &= (a+b)(a+b) && \text{(Exponentiation 2.3.11)}\\
&= a(a+b) + b(a+b) && \text{(Distributive law 2.3.4)}\\
&= a^2 + ab + ba + b^2 && \text{(Distributive law and Addition is associative 2.2.5)}\\
&= a^2 + ab + ab + b^2 && \text{(Multiplication is commutative 2.3.2)}\\
&= a^2 + (1+1)ab + b^2 && \text{(Distributive law)}\\
&= a^2 + 2ab + b^2 && \text{(Definition of addition 2.2.1)}
\end{aligned}$$

□

Exercise 2.3.5. Prove Proposition 2.3.9. (*Hint*: fix q and induct on n.)

Attempt. Let q be fixed and we induct on n. Let $n = 0$, we see $0 = mq + r$ only if the right-hand side is zero. Since $q \neq 0$, m and r must be zero, and the base case holds. Suppose inductively that $n = mq + r$ for $0 \leq r < q$. We wish to show that $n + 1 = m'q + r'$ for some natural number m' and $0 \leq r' < q$. Based on the inductive hypothesis, the left-hand side is equal to $(mq + r) + 1 = mq + (r + 1)$. There are two possibilities. If $r + 1 < q$, then $r' = r + 1$ and $m' = m$. If $r + 1 = q$, then $n + 1 = mq + q = (m + 1)q + 0$, so $m' = m + 1$ and $r' = 0$. In both cases, the hypothesis holds for $n + 1$, and the induction is closed. □

Chapter 3 Set Theory

3.1 Fundamentals

Definition 3.1.1 (Set) (*Informal*) We define a *set* A to be any unordered collection of objects, e.g., $\{3, 8, 5, 2\}$ is a set. If x is an object, we say that x is an element of A or $x \in A$ if x lies in the collection; otherwise we say that $x \notin A$. For instance, $3 \in \{1, 2, 3, 4, 5\}$ but $7 \notin \{1, 2, 3, 4, 5\}$.

Axiom 3.1 (Sets are objects) If A is a set then A is also an object. In particular, given two sets A and B, it is meaningful to ask whether A is also an element of B.

Axiom 3.2 (Equality of Sets) Two sets A and B are equal, $A = B$, iff every element of A is an element of B and vice versa. To put it another way, $A = B$ if and only if every element x of A belongs also to B, and every element y of B belongs also to A.

Axiom 3.3 (Empty Set) There exists a set $\emptyset$, known as the empty set, which contains no elements, i.e., for every object x we have $x \notin \emptyset$.

Exercise 3.3a If there were two sets $\emptyset$ and $\emptyset'$ which were both empty, then by Axiom 3.2 they would be equal to each other (why?).

Attempt. Since there is no element in both sets, it is vacuously true that every element in one set belongs to the other set. □

Lemma 3.1.5 (Single choice) *Let A be a non-empty set. Then there exists an object x such that $x \in A$.*

Axiom 3.4 (Singleton sets and pair sets) If a is an object, then there exists a set $\{a\}$ whose only element is a, i.e., for every object y, we have $y \in \{a\}$ if and only if $y = a$; we refer to $\{a\}$ as the singleton set whose element is a. Furthermore, if a and b are objects, then there exists a set $\{a, b\}$ whose only elements are a and b; i.e., for every object y, we have $y \in \{a, b\}$ if and only if $y = a$ or $y = b$; we refer to this set as the pair set formed by a and b.

Axiom 3.5 (Pairwise union) Given any two sets A, B, there exists a set $A \cup B$, called the *union* of A and B, which consists of all the elements which belong to A or B or both. In other words, for any object x,

$$x \in A \cup B \iff (x \in A \text{ or } x \in B).$$

Lemma 3.1.12 (Set as union of singletons) *If a and b are objects, then $\{a, b\} = \{a\} \cup \{b\}$. If A, B, C are sets, then the union operation is commutative (i.e., $A \cup B = B \cup A$) and associative (i.e., $(A \cup B) \cup C = A \cup (B \cup C)$). Also, we have $A \cup A = A \cup \emptyset = \emptyset \cup A = A$.*

Definition 3.1.14 (Subsets) Let A, B be sets. We say that A is a *subset* of B, denoted $A \subseteq B$, iff every element of A is also an element of B, i.e.,

$$\text{For any object } x, \quad x \in A \implies x \in B.$$

We say that A is a proper subset of B, denoted $A \subsetneq B$, if $A \subseteq B$, and $A \neq B$.

Proposition 3.1.17 (Sets are partially ordered by set inclusion) Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. If $A \subseteq B$ and $B \subseteq A$, then $A = B$. Finally, if $A \subsetneq B$ and $B \subsetneq C$ then $A \subsetneq C$.

Axiom 3.6 (Axiom of specification) Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x (i.e., for each $x \in A, P(x)$ is either a true statement or a false statement). Then there exists a set, called $\{x \in A : P(x) \text{ is true}\}$ (or simply $\{x \in A : P(x)\}$ for short), whose elements are precisely the elements x in A for which $P(x)$ is true. In other words, for any object y,

$$y \in \{x \in A : P(x) \text{ is true}\} \iff (y \in A \text{ and } P(y) \text{ is true}).$$

This axiom is also known as the *axiom of separation.*

Definition 3.1.22 (Intersections) The intersection $S_1 \cap S_2$ of two sets is defined to be the set

$$S_1 \cap S_2 := \{x \in S_1 : x \in S_2\}.$$

In other words, $S_1 \cap S_2$ consists of all the elements which belong to both S_1 and S_2. Thus, for all objects x,

$$x \in S_1 \cap S_2 \iff x \in S_1 \text{ and } x \in S_2.$$

Two sets A, B are said to be *disjoint* if $A \cap B = \emptyset$. Note that this is not the same concept as being *distinct*, $A \neq B$.

Definition 3.1.26 (Difference sets) Given two sets A and B, we define the set $A - B$ or $A \setminus B$ to be the set A with any elements of B removed:

$$A \setminus B := \{x \in A : x \notin B\};$$

Proposition 3.1.27 (Sets form a boolean algebra) *Let A, B, C be sets, and let X be a set containing A, B, C as subsets.*

(a) (Minimal element) We have $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

(b) (Maximal element) We have $A \cup X = X$ and $A \cap X = A$.

(c) (Identity) We have $A \cap A = A$ and $A \cup A = A$.

(d) (Commutativity) We have $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

(e) (Associativity) We have $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.

(f) (Distributivity) We have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(g) (Partition) We have $A \cup (X \setminus A) = X$ and $A \cap (X \setminus A) = \emptyset$.

(h) (De Morgan laws) We have $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ and $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Axiom 3.7 (Replacement) 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 $\{y : P(x, y) \text{ is true for some } x \in A\}$, such that for any object z,

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

Axiom 3.8 (Infinity) There exists a set $\boldsymbol{N}$, whose elements are called natural numbers, as well as an object 0 in $\boldsymbol{N}$, and an object n++ assigned to every natural number $n \in \boldsymbol{N}$, such that the Peano axioms (Axioms 2.1-2.5) hold.

This is the more formal version of Assumption 2.6.

— Exercises —

Exercise 3.1.1 Let a, b, c, d be objects such that $\{a, b\} = \{c, d\}$. Show that at least one of the two statements "$a = c$ and $b = d$" and "$a = d$ and $b = c$" hold.

Attempt. Given the two sets are equal, by Axiom 3.2, every element of $\{a, b\}$ is an element of $\{c, d\}$ and vice-versa. Let's first consider the case when a, b are distinct objects from each other, and c, d are distinct from each other. Since $a \in \{a, b\}$, $a \in \{c, d\}$ by Axiom 3.2. Suppose $a = c$, then b must be equal to d for otherwise $b = c = a$ which implies $d \notin \{a, b\}$, a contradiction that the two sets are equal. So the first statement holds. Similar argument applies if $a = d$, so the second statement holds. If a, b or c, d were not distinct objects from each other, then necessarily $a = b = c = d$, and the two statements would both hold trivially. In all cases, at least one of the two statements is true, as desired. □

Exercise 3.1.2 Using only Axiom 3.2, Axiom 3.1, Axiom 3.3, and Axiom 3.4, prove that the sets $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}$ and $\{\emptyset, \{\emptyset\}\}$ are all distinct (i.e., no two of them are equal to each other).

Attempt. One way to prove this is to compare pairwise between any two of the four given sets, and see that they all violate Axiom 3.2 with respect to set equality. Another way is to note that $\{\emptyset\}$ is a singleton set of $\emptyset$ by Axiom 3.4. Then $\{\{\emptyset\}\}$ is a singleton set of $\{\emptyset\}$, and $\{\emptyset, \{\emptyset\}\}$ is a pair set of both $\emptyset$ and $\{\emptyset\}$. Every set is formulated with different elements during the process. Hence no two sets are equal. □

Exercise 3.1.3 Prove the remaining claims in Lemma 3.1.12.

Attempt. We want to prove that

(a) Set union operation is commutative i.e., $A \cup B = B \cup A$.

Attempt. By Axiom 3.5, both the left-hand side and right-hand side is a set by union. Every object that belongs to either set A or set B on the left-hand side belongs to either set B or set A on the right-hand side. Hence the two sides are equal by Axiom 3.2.

(b) $A \cup A = A \cup \emptyset = \emptyset \cup A = A$.

Attempt. By Axiom 3.5, the union of two sets is a set. Also, every object that belongs to either set A or set A belongs to set A, and vice-versa. Similarly, every object that belongs to either set A or the empty set belongs to set A, and vice-versa. Since union of sets is commutative by Lemma 3.1.12, $A \cup \emptyset = \emptyset \cup A$. By Axiom 3.2, we conclude all these sets are equal to each other.

□

Exercise 3.1.4 Prove the remaining claims in Proposition 3.1.17.

Attempt. We want to prove that

(a) if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Attempt. By definition of subsets (3.1.14), since $A \subseteq B$, every element of A is also an element of B, and vice-versa since $B \subseteq A$. The two sets are therefore equal by Axiom 3.2.

(b) if $A \subsetneq B$ and $B \subsetneq C$ then $A \subsetneq C$.

Attempt. By definition of subsets (3.1.14), since $A \subsetneq B$, every element of A is also an element of B, and since $B \subsetneq C$, every element of B is also an element of C. Therefore, every element of A is also an element of C i.e., $A \subseteq C$. What remains is to show $A \neq C$. Assume the opposite that $A = C$, so every element of C is also an element of A by Axiom 3.2. But since every element of A is also an element of B, every element of C is also an element of B, contradicting $B \subsetneq C$. Hence the assumption is false, and $A \subsetneq C$ as desired.

□

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

Attempt. Let x be an object.

1. By definition of subsets (3.1.14), $A \subseteq B$ is logically equivalent to

$$x \in A \implies x \in B.$$

2. By axiom of pairwise union (3.5), $A \cup B = B$ is logically equivalent to

$$(x \in A \text{ or } x \in B) \iff x \in B.$$

3. By definition of intersections (3.1.22), $A \cap B = A$ is logically equivalent to

$$(x \in A \text{ and } x \in B) \iff x \in A.$$

For each of these three statements,

- If $x \in A$ is true, the statement is true only if $x \in B$ is true.
- If $x \in A$ is false, the statement is always true.

Therefore we conclude the three statements are logically equivalent to each other. □

Exercise 3.1.6 Prove Proposition 3.1.27. (Hint: one can use some of these claims to prove others. Some of the claims have also appeared previously in Lemma 3.1.12.)

Attempt. Let A, B, C be sets, and let X be a set containing A, B, C as subsets. We want to prove that

(a) (Minimal element) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

Since an empty set has no element by axiom 3.3, for any object x, $A \cup \emptyset$ is equivalent to

$$(x \in A \text{ or } x \in \emptyset) \iff x \in A$$

by axiom 3.5 of pairwise union. Therefore, $A \cup \emptyset = A$ by axiom 3.2 of equality of sets.

By definition 3.1.22 of intersections, $A \cap \emptyset = \{x \mid x \in A : x \in \emptyset\}$ which is equal to an empty set by axiom 3.2 of equality of sets. Hence $A \cap \emptyset = \emptyset$. □

(b) (Maximal element) $A \cup X = X$ and $A \cap X = A$.

$A \cup X$ is equal to the set $\{x \in A \text{ or } x \in X\}$ by axiom 3.5 of pairwise union. Given $A \subseteq X$, every element of A is also an element of X by definition 3.1.14 of subsets. Therefore,

$$\{x \in A \text{ or } x \in X\} = \{x \in X\} = X.$$

Hence $A \cup X = X$ by axiom 3.2 of equality of sets.

On the other hand, $A \cap X$ is equal to the set $\{x \in A : x \in X\}$ by definition 3.1.22 of intersections. Given $A \subseteq X$, every element of A is also an element of X by definition 3.1.14 of subsets. Therefore,

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

Hence $A \cap X = A$ by axiom 3.2 of equality of sets. □

(c) (Identity) $A \cap A = A$ and $A \cup A = A$.

By definition 3.1.22 of intersections, and axiom 3.2 of equality of sets,

$$A \cap A = \{x \in A : x \in A\} = \{x \in A\} = A.$$

By axiom 3.5 of pairwise union, and axiom 3.2 of equality of sets,

$$A \cup A = \{x \in A \text{ or } x \in A\} = \{x \in A\} = A.$$

□

(d) (Commutativity) $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

By axiom 3.5 of pairwise union, commutativity of logical or, and axiom 3.2 of equality of sets,

$$A \cup B = \{x \in A \text{ or } x \in B\} = \{x \in B \text{ or } x \in A\} = B \cup A$$

By definition 3.1.22 of intersections, commutativity of logical and, and axiom 3.2 of equality of sets,

$$A \cap B = \{x \in A : x \in B\} = \{x \in B : x \in A\} = B \cap A$$

□

(e) (Associativity) $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.

$$\begin{aligned}
(A \cup B) \cup C &= \{x \in A \cup B \text{ or } x \in C\} && \text{(axiom 3.5 of pairwise union)}\\
&= \{(x \in A \text{ or } x \in B) \text{ or } x \in C\} && \text{(axiom 3.5 of pairwise union)}\\
&= \{x \in A \text{ or } (x \in B \text{ or } x \in C)\} && \text{(associativity of logical-or)}\\
&= A \cup (B \cup C) && \text{(axiom 3.5 of pairwise union)}
\end{aligned}$$

$$\begin{aligned}
(A \cap B) \cap C &= \{x \in A \cap B : x \in C\} && \text{(definition 3.1.22)}\\
&= \{(x \in A \text{ and } x \in B) \text{ and } x \in C\} && \text{(definition 3.1.22)}\\
&= \{x \in A \text{ and } (x \in B \text{ and } x \in C)\} && \text{(associativity of logical-and)}\\
&= \{x \in A : x \in B \cap C\} && \text{(definition 3.1.22)}\\
&= A \cap (B \cap C) && \text{(definition 3.1.22)}
\end{aligned}$$

□

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

$$\begin{aligned}
A \cap (B \cup C) &= \{x \in A \text{ and } x \in B \cup C\} && \text{(definition 3.1.22)}\\
&= \{x \in A \text{ and } (x \in B \text{ or } x \in C\}) && \text{(axiom 3.5 of pairwise union)}\\
&= \{(x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\} && \text{(distributivity of logical-and)}\\
&= (A \cap B) \cup (A \cap C) && \text{(definition 3.1.22, axiom 3.5)}
\end{aligned}$$

$$\begin{aligned}
A \cup (B \cap C) &= \{x \in A \text{ or } x \in B \cap C\} && \text{(axiom 3.5 of pairwise union)}\\
&= \{x \in A \text{ or } (x \in B \text{ and } x \in C)\} && \text{(definition 3.1.22)}\\
&= \{(x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C)\} && \text{(distributivity of logical-or)}\\
&= \{x \in A \cup B : x \in A \cup C\} && \text{(axiom 3.5 of pairwise union)}\\
&= (A \cup B) \cap (A \cup C) && \text{(definition 3.1.22, axiom 3.5)}
\end{aligned}$$

□

(g) (Partition) $A \cup (X \setminus A) = X$ and $A \cap (X \setminus A) = \emptyset$.

$$\begin{aligned}
A \cup (X \setminus A) &= \{x \in A \text{ or } x \in (X \setminus A)\} && \text{(axiom 3.5 of pairwise union)}\\
&= \{x \in A \text{ or } (x \in X \text{ and } x \notin A)\} && \text{(definition 3.1.26)}\\
&= \{(x \in A \text{ or } x \in X) \text{ and } (x \in A \text{ or } x \notin A)\} && \text{(distributivity of logical-or)}\\
&= \{x \in A \text{ or } x \in X\} && \text{(tautology of } x \in A \text{ or } x \notin A)\\
&= A \cup X && \text{(axiom 3.5 of pairwise union)}\\
&= X && ((b) \text{ maximal element})
\end{aligned}$$

$$\begin{aligned}
A \cap (X \setminus A) &= \{x \in A \text{ and } x \in X \setminus A\} && \text{(definition 3.1.22)}\\
&= \{x \in A \text{ and } (x \in X \text{ and } x \notin A\}) && \text{(definition 3.1.26)}\\
&= \{x \in A \text{ and } x \notin A \text{ and } x \in X\} && \text{(associativity of logical-and)}\\
&= \emptyset && \text{contradiction of } x \in A \text{ and } x \notin A
\end{aligned}$$

□

(h) (De Morgan laws) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ and $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

$$\begin{aligned}
X \setminus (A \cup B) &= \{x \in X : x \notin A \cup B\} && \text{(definition 3.1.26)}\\
&= \{x \in X \text{ and } \neg(x \in A \text{ or } x \in B)\} && \text{(definition of } \notin)\\
&= \{x \in X \text{ and } (x \notin A \text{ and } x \notin B\}) && \text{(De Morgan's law on logical-or)}\\
&= \{x \in X \text{ and } x \notin A \text{ and } x \notin B\} && \text{(associative of logical-and)}\\
&= \{x \in X \text{ and } x \notin A \text{ and } x \in X \text{ and } x \notin B\} && (x \in X = x \in X \text{ and } x \in X)\\
&= \{x \in X \setminus A \text{ and } x \in X \setminus B\} && \text{(definition 3.1.26)}\\
&= (X \setminus A) \cap (X \setminus B) && \text{(definition 3.1.22)}
\end{aligned}$$

$$
\begin{aligned}
X \setminus (A \cap B) &= \{x \in X : x \notin A \cap B\} && \text{(definition 3.1.26)}\\
&= \{x \in X \text{ and } \neg(x \in A \text{ and } x \in B)\} && \text{(definition of } \notin\text{)}\\
&= \{x \in X \text{ and } (x \notin A \text{ or } x \notin B)\} && \text{(De Morgan's law on `and')}\\
&= \{(x \in X \text{ and } x \notin A) \text{ or } (x \in X \text{ and } x \notin B)\} && \text{(logical-and is distributive)}\\
&= (X \setminus A) \cup (X \setminus B) && \text{(definition 3.1.26)}
\end{aligned}
$$

□

Exercise 3.1.7 Let A, B, C be sets. Show that $A \cap B \subseteq A$ and $A \cap B \subseteq B$. Furthermore, show that $C \subseteq A$ and $C \subseteq B$ if and only if $C \subseteq A \cap B$. In a similar spirit, show that $A \subseteq A \cup B$ and $B \subseteq A \cup B$, and furthermore that $A \subseteq C$ and $B \subseteq C$ if and only if $A \cup B \subseteq C$.

Attempt. We want to show that

(a) $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

By definition 3.1.22 of itersections, $A \cap B = \{x \in A \text{ and } x \in B\}$. Therefore any object that belongs to both A and B must also belong to A, but any object that belongs to A does not necessarily belong to B. Hence $A \cap B \subseteq A$ by definition 3.1.14 of subsets. By exchanging the set names, we have $B \cap A \subseteq B$, which is equivalent to $A \cap B \subseteq B$ since set intersection is commutative by Proposition 3.1.27. □

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

For any object x,

$$
\begin{aligned}
C \subseteq A \text{ and } C \subseteq B &= (x \in C \implies x \in A) \text{ and } (x \in C \implies x \in B) && \text{(def. 3.1.14 of subsets)}\\
&= x \in C \implies (x \in A \text{ and } x \in B)\\
&= x \in C \implies x \in A \cap B && \text{(def. 3.1.22)}\\
&= C \subseteq A \cap B && \text{(def. 3.1.14 of subsets)}
\end{aligned}
$$

□

(c) $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

If an object x belongs to A, it must also belong to either A or B, i.e.,

$$x \in A \implies (x \in A \text{ or } x \in B).$$

Therefore, $A \subseteq A \cup B$ by Axiom 3.5 of pairwise union. By exchanging the set names, we have $B \subseteq B \cup A$, which is equivalent to $B \subseteq A \cup B$ since set union is commutative by Proposition 3.1.27. □

(d) $A \subseteq C$ and $B \subseteq C$ if and only if $A \cup B \subseteq C$. Let's start from the right-hand side. For any object x,

$$
\begin{aligned}
A \cup B \subseteq C &= (x \in A \text{ or } x \in B) \implies x \in C && \text{(def. 3.1.14 subsets)}\\
&= \neg(x \in A \text{ or } x \in B) \text{ or } x \in C && \text{(def. implication)}\\
&= (x \notin A \text{ and } x \notin B) \text{ or } x \in C && \text{(De Morgan's law)}\\
&= (x \notin A \text{ or } x \in C) \text{ and } (x \notin B \text{ or } x \in C) && \text{(distribute or over and)}\\
&= (x \in A \implies x \in C) \text{ and } (x \in B \implies x \in C) && \text{(def. implication)}\\
&= A \subseteq C \text{ and } B \subseteq C && \text{(def. 3.1.14 subsets)}
\end{aligned}
$$

□

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

Attempt. Let $X = A \cup B$. Since X contains A, $A \cap X = A$ by maximal element of Proposition 3.1.27. Therefore, $A \cap (A \cup B) = A$.

Now let $X = A$. Since X contains $A \cap B$, $(A \cap B) \cup X = X$ by maximal element. By commutativity of Proposition 3.1.27, $(A \cap B) \cup X = X \cup (A \cap B) = X$. Therefore, $A \cup (A \cap B) = A$. □

Exercise 3.1.9 Let A, B, X be sets such that $A \cup B = X$ and $A \cap B = \emptyset$. Show that $A = X \setminus B$ and $B = X \setminus A$.

Attempt. We will first show that $A \setminus B = A$ (i).

$$\begin{aligned}
A \cap B &= \emptyset && \text{(given)}\\
(A \cap B)^c &= X && \text{(duality)}\\
A^c \cup B^c &= && \text{(De Morgan's law)}\\
A \cap (A^c \cup B^c) &= A \cap X && \text{(intersect both sides with } A\text{)}\\
&= A && \text{(maximal element 3.1.27(b))}\\
(A \cap A^c) \cup (A \cap B^c) &= && \text{(distributivity)}\\
\{x \in A \text{ and } \notin A\} \cup \{x \in A \text{ and } x \notin B\} &= && \text{(definition)}\\
(A \setminus A) \cup (A \setminus B) &= && \text{(definition)}\\
\emptyset \cup (A \setminus B) &= && \text{(contradiction)}\\
(A \setminus B) \cup \emptyset &= && \text{(commutativity 3.1.27(d))}\\
A \setminus B &= A && \text{(minimal element 3.1.27(a))}
\end{aligned}$$

Now we will show that $X \setminus B = A$.

$$\begin{aligned}
X \setminus B &= (A \cup B) \setminus B && \text{(given)}\\
&= \{(x \in A \text{ or } x \in B) \text{ and } x \notin B\} && \text{(definition)}\\
&= (A \setminus B) \cup (B \setminus B) && \text{(distributivity and definition)}\\
&= A \cup \emptyset && \text{(by (i) and contradiction)}\\
&= A && \text{(minimal element 3.1.27(a))}
\end{aligned}$$

Therefore $A = X \setminus B$. Finally, swapping A and B in the argument gives $B = X \setminus A$. □

(Note in particular De Morgan laws 3.1.27(h) cannot be applied to $(A \cup B) \setminus B$ in this case.)

Exercise 3.1.10 Let A and B be sets. Show that the three sets $A \setminus B, A \cap B$, and $B \setminus A$ are disjoint, and that their union is $A \cup B$.

Attempt. Let X be the universal set that contains both A and B. By definition, two sets are disjoint if their intersection is empty. First, let's check the intersection of $A \setminus B$ and $A \cap B$.

$$\begin{aligned}
(A \setminus B) \cap (A \cap B) &= (A \cap B^c) \cap (A \cap B) && \text{(definition 3.1.26)}\\
&= (A \cap A) \cap (B \cap B^c) && \text{(associativity 3.1.27(e))}\\
&= A \cap (B \setminus B) && \text{(identity 3.1.27(c) and definition 3.1.26)}\\
&= A \cap \emptyset && \text{(contradiction)}\\
&= \emptyset && \text{(minimal element 3.1.27(a))}
\end{aligned}$$

Hence $A \setminus B$ and $A \cap B$ are disjoint. Similarly, it follows that $B \setminus A$ and $A \cap B$ are disjoint by swapping A and B and then applying the same argument. By definition, $A \setminus B$ and $B \setminus A$ are disjoint iff their intersection is empty.

$$\begin{aligned}
(A \setminus B) \cap (B \setminus A) &= (A \cap B^c) \cap (B \cap A^c) && \text{(definition 3.1.26)}\\
&= (A \setminus A) \cap (B \setminus B) && \text{(associativity 3.1.27(e) and definition 3.1.26)}\\
&= \emptyset \cap \emptyset && \text{(contradiction)}\\
&= \emptyset && \text{(minimal element 3.1.27(a))}
\end{aligned}$$

Therefore all three sets are disjoint to each other.

For the final part, we first want to show the equality $A \cup (B \setminus A) = A \cup B$, and $B \cup (A \setminus B) = A \cup B$.

$$\begin{aligned} A \cup (B \setminus A) &= A \cup (B \cap A^c) && \text{(definition)} \\ &= (A \cup B) \cap (A \cup A^c) && \text{(distributivity 3.1.27(f))} \\ &= (A \cup B) \cap X \\ &= A \cup B && \text{(maximal element 3.1.27(b) as } (A \cup B) \subseteq X) \end{aligned}$$

Similarly, the equality $B \cup (A \setminus B) = A \cup B$ follows if we swap A and B and apply the same argument. Let's label this equality as Lemma 1:

$$A \cup (B \setminus A) = A \cup B = B \cup (A \setminus B).$$

We are now ready to show that the union of all three sets, namely $A \setminus B$, $A \cap B$, and $B \setminus A$, is $A \cup B$. In fact, we only need to show that the union of the first two sets is equal to A, because the union of A and the third set $B \cup (A \setminus B)$ is equal to $A \cup B$ by Lemma 1.

$$\begin{aligned} (A \setminus B) \cup (A \cap B) &= \big[(A \setminus B) \cup A \setminus big] \cap \big[(A \setminus B) \cup B\big] && \text{(distributivity 3.1.27)} \\ &= A \cap \big[(A \setminus B) \cup B\big] && \text{(maximal element 3.1.27(b) as } (A \setminus B) \subseteq A) \\ &= A \cap \big[B \cup (A \setminus B)\big] && \text{(commutativity 3.1.27(d))} \\ &= A \cap (A \cup B) && \text{(lemma 1)} \\ &= A && \text{(maximal element 3.1.27(b) as } A \subseteq (A \cup B)) \end{aligned}$$

□

Exercise 3.1.11 Show that the axiom of replacement implies the axiom of specification.

Attempt. Starting from axiom 3.7 of replacement:

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 $\{y : P(x, y) \text{ is true for some } x \in A\}$, such that for any object z,

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

Since y can be any object, we set $y = x$, so that the axiom reduces to:

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

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

Note in particular that

1. the statement "for any object $x \in A$" is equivalent to "for each $x \in A$".
2. the statement "for each $x \in A$ there is at most one x for which $P(x)$ is true" is equivalent to "for each $x \in A$, $P(x)$ can either be true or false"; or equivalently "for each $x \in A, P(x)$ is either a true statement or a false statement".
3. $\{x : P(x) \text{ is true for some } x \in A\}$ is the same as $\{x \in A : P(x) \text{ is true}\}$.
4. ($P(x)$ is true for some $x \in A$) is equivalent to ($x \in A$ and $P(x)$ is true), which is the same as ($y \in A$ and $P(y)$ is true) by renaming variable.

Substituting these equiavlent statements into axiom 3.7 of replacement, we get

Let A be a set. For each $x \in A$, suppose we have a statement $P(x)$ pertaining to x, such that for each $x \in A, P(x)$ is either a true statement or a false statement. Then there exists a set $\{x \in A : P(x) \text{ is true}\}$, such that for any object z,

$$z \in \{x \in A : P(x) \text{ is true}\} \iff (y \in A \text{ and } P(y) \text{ is true}).$$

Compare this to axiom 3.6 of specification:

Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x (i.e., for each $x \in A, P(x)$ is either a true statement or a false statement). Then there exists a set, called $\{x \in A : P(x) \text{ is true}\}$ (or simply $\{x \in A : P(x)\}$ for short), whose elements are precisely the elements x in A for which $P(x)$ is true. In other words, for any object y,

$$y \in \{x \in A : P(x) \text{ is true}\} \iff (y \in A \text{ and } P(y) \text{ is true}).$$

We see the two axioms become equivalent. We conclude that axiom 3.6 of specification is a special case of applying axiom 3.7 of replacement when the object is replaced by itself. Hence axiom 3.7 of replacement implies axiom 3.6 of specification. □

Exercise 3.1.12. Suppose that A, B, A', B' are sets such that $A' \subseteq A$ and $B' \subseteq B$.

(i) Show that $A' \cup B' \subseteq A \cup B$ and $A' \cap B' \subseteq A \cap B$.

(ii) Given a counterexample to show that the statement $A' \setminus B' \subseteq A \setminus B$ is false. Can you find a modification of this statement involving the set difference operation $\setminus$ which is true given the stated hypothesis? Justify your answer.

Attempt.

(i) First we want to show $(A' \cup B') \subseteq (A \cup B)$. Given $A' \subseteq A$ and $B' \subseteq B$, we have $A' \subseteq (A \cup B)$ and $B' \subseteq (B \cup A)$, by enlarging the set on each of the right-hand sides. It follows that for every object x, by definition 3.1.14 of subsets,

$$\begin{aligned}
&(x \in A' \implies x \in (A \cup B)) \text{ and } (x \in B' \implies x \in (B \cup A)) \\
\iff &(x \notin A' \text{ or } x \in A \text{ or } x \in B) \text{ and } (x \notin B' \text{ or } x \in A \text{ or } x \in B) \\
\iff &(x \notin A' \text{ and } x \notin B') \text{ or } (x \in A \text{ or } x \in B) && \text{(distributivity)} \\
\iff &x \notin (A' \cup B') \text{ or } x \in (A \cup B) \\
\iff &x \in (A' \cup B') \implies x \in (A \cup B) \\
\iff &(A' \cup B') \subseteq (A \cup B) && \text{(def. 3.1.14 of subsets)}
\end{aligned}$$

Therefore, $(A' \subseteq A)$ and $(B' \subseteq B)$ implies $(A' \cup B') \subseteq (A \cup B)$.

Now we want to show $A' \cap B' \subseteq A \cap B$. Given $A' \subseteq A$ and $B' \subseteq B$, we have $(A' \cap B') \subseteq A$ and $(B' \cap A') \subseteq B$, by shrinking the subset on each of the left-hand sides. It follows that for every object x, by definition 3.1.14 of subsets,

$$\begin{aligned}
&(x \in (A' \cap B') \implies x \in A) \text{ and } (x \in (B' \cap A') \implies x \in B) \\
\iff &(x \notin (A' \cap B') \text{ or } x \in A) \text{ and } (x \notin (A' \cap B') \text{ or } x \in B) \\
\iff &(x \notin A' \text{ or } x \notin B' \text{ or } x \in A) \text{ and } (x \notin A' \text{ or } x \notin B' \text{ or } x \in B) \\
\iff &(x \notin A' \text{ or } x \notin B') \text{ or } (x \in A \text{ and } x \in B) && \text{(distributivity)} \\
\iff &(x \in A' \text{ and } x \in B') \implies (x \in A \text{ and } x \in B) \\
\iff &A' \cap B' \subseteq A \cap B && \text{(def. 3.1.14 of subsets)}
\end{aligned}$$

Therefore, $(A' \subseteq A)$ and $(B' \subseteq B)$ also implies $A' \cap B' \subseteq A \cap B$. □

Remark: The presentation of the solution is in reverse order of how the solution was discovered.

(ii) We want to find a counterexample to show that the statement $A' \setminus B' \subseteq A \setminus B$ is false. Let a, b be two distinct objects, and let $A = B = \{a, b\}, A' = \{a\}$ and $B' = \{b\}$. Then $A' \setminus B' = A'$ whereas $A \setminus B = \emptyset$. This proves the statement is false.

The second question is more interesting – how can we find a modification of the statement involving the set difference operation $\setminus$ which is true given the stated hypothesis?

Starting from the left-hand side, for every object x, if $x \in A'$ and $x \notin B'$, then it must also be the case that $x \in A$ and $x \notin B'$, since $A' \subseteq A$. Therefore,

$$(x \in A' \text{ and } x \notin B') \implies (x \in A \text{ and } x \notin B')$$

i.e.,

$$A' \setminus B' \subseteq A \setminus B'$$

Note that, given $A' \subseteq A$, $x \in A' \implies x \in A$. In contrast, $x \notin B'$ does *not* imply $x \notin B$, given $B' \subseteq B$. This is why the statement $A' \setminus B' \subseteq A \setminus B$ is false. □

Exercise 3.1.13. Euclid famously defined a point to be "that which has no part". This exercise should be reminiscent of that definition. Define a *proper subset* of a set A to be a subset B of A with $B \neq A$. Let A be a non-empty set. Show that A does not have any non-empty proper subsets if and only if A is of the form $A = \{x\}$ for some object x.

Attempt. We prove the equivalence in both directions.

($\Rightarrow$ direction via contrapositive) Suppose A does not have any non-empty proper subsets. We aim to show that A is of the form $A = \{x\}$ for some object x. Since A is non-empty, there exists $x \in A$. Assume, for contradiction, that there exists $y \in A$ with $y \neq x$. Then the set $B = A \setminus \{y\}$ is a non-empty proper subset of A. This contradicts the assumption that A does not have any non-empty proper subsets. Therefore A is of the form $A = \{x\}$ for some object x.

($\Leftarrow$ direction) Suppose A is of the form $A = \{x\}$ for some object x. Then the empty set is the only proper subset of A. Thus A does not have any non-empty proper subsets. □

3.2 Russell's Paradox (Optional)

Axiom 3.9 (Universal Specification) (Dangerous!) Suppose for every object x we have a property $P(x)$ pertaining to x (so that for every $x, P(x)$ is either a true statement or a false statement). Then there exists a set $\{x : P(x) \text{ is true}\}$ such that for every object y,

$$y \in \{x : P(x)\text{is true}\} \iff P(y) \text{ is true.}$$

This axiom is also known as the *axiom of comprehension.* It asserts that every property corresponds to a set; if we assumed that axiom, we could talk about the set of all blue objects, the set of all natural numbers, the set of all sets, and so forth. Unfortunately, this axiom cannot be introduced into set theory, because it creates a logical contradiction known as *Russell's paradox.*

Axiom 3.10 (Regularity) If A is a non-empty set, then there is at least one element x of A which is either not a set, or is disjoint from A.

This axiom ensures that absurdities such as Russell's paradox do not occur. The point of this axiom (which is also known as the *axiom of foundation*) is that it is asserting that at least one of the elements of A is so low on the hierarchy of objects that it does not contain any of the other elements of A.

— Exercises —

Exercise 3.2.1. Show that the universal specification axiom, Axiom 3.9, if assumed to be true, would imply Axioms 3.3, 3.4, 3.5, 3.6, and 3.7. (If we assume that all natural numbers are objects, we also obtain Axiom 3.8.) Thus, this axiom, if permitted, would simplify the foundations of set theory tremendously (and can be viewed as one basis for an intuitive model of set theory known as "naive set theory"). Unfortunately, as we have seen, Axiom 3.9 is "too good to be true"!

Attempt. We aim to show Axiom 3.9, if assumed to be true, would imply

(i) Axioms 3.3 (Empty Set). Let $P(x)$ be false for every object x. By Axiom 3.9, there exists a set $\{x : P(x)\} = \{\} = \emptyset$ such that for every object y, the statement $y \in \emptyset \iff P(y)$ is vacuously true in both directions. Therefore Axiom 3.9 implies Axiom 3.3 i.e., there exists a set $\emptyset$ which contains no elements.

(ii) Axioms 3.4 (Singleton sets and pair sets). Let a, b be objects, and $P(x)$ be true if $x = a$. By Axiom 3.9, there exists a set $\{x : P(x)\} = \{a\}$ such that for every object y, $y \in \{a\} \iff P(y)$. Likewise, let $P(x)$ be true if $x = a$ or $x = b$. By Axiom 3.9, there exists a set $\{x : P(x)\} = \{a, b\}$ such that for every object y, $y \in \{a, b\} \iff P(y)$. Therefore Axiom 3.9 implies Axiom 3.4.

(iii) Axioms 3.5 (Pairwise union). Given any two sets A, B, let $P(x)$ be true if $x \in A$ or $x \in B$. By Axiom 3.9, there exists a set $\{x : P(x)\} = \{x \in A \text{ or } x \in B\}$ such that for every object y, $y \in \{x \in A \text{ or } x \in B\} \iff P(y)$, i.e., $y \in A \cup B \iff P(y)$. Therefore Axiom 3.9 implies Axiom 3.5.

(iv) Axioms 3.6 (Axiom of specification). Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x. Furthermore, let $Q(x) = (x \in A \text{ and } P(x))$. By Axiom 3.9, there exists a set $\{x : Q(x) \text{ is true}\}$ such that for every object y, $y \in \{x : Q(x) \text{ is true}\} \iff Q(y)$ is true, which is equivalent to $y \in \{x \in A : P(x)\} \iff (y \in A \text{ and } P(y) \text{ is true})$. Therefore Axiom 3.9 implies Axiom 3.6.

(v) Axioms 3.7 (Replacement). 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. Suppose for every object y, we have a property $Q(y) = P(x, y)$ pertaining to y for some $x \in A$. By Axiom 3.9, there exists a set $\{y : Q(y) \text{ is true}\}$ such that for every object z,

$$z \in \{y : Q(y) \text{ is true}\} \iff Q(z) \text{ is true}$$

which is equivalent to

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

Therefore Axiom 3.9 implies Axiom 3.7.

(vi) Axioms 3.8, if we assume that all natural numbers are objects. Suppose for every object x, we have a property $P(x)$ pertaining to x so that $P(x)$ is true iff x is a natural number, i.e, such that the Peano axioms (Axioms 2.1-2.5) hold. By Axiom 3.9, there exists a set $\{x : P(x) \text{ is true}\}$ such that for every object y, $y \in \{x : P(x) \text{ is true}\} \iff P(y)$ is true. Since the set $\{x : P(x) \text{ is true}\}$ is equal to the set $\boldsymbol{N}$, whose elements are the natural numbers, we conclude that Axiom 3.9 implies Axiom 3.8.

□

Exercise 3.2.2. Use the axiom of regularity (and the singleton set axiom) to show that if A is a set, then $A \notin A$. Furthermore, show that if A and B are two sets, then either $A \notin B$ or $B \notin A$ (or both). (One corollary of this exercise is worth noting: given any set A, there exists a mathematical object that is not an element in A, namely A itself. Thus one can always "add one more element" to a set A to create a larger set, namely $A \cup \{A\}$.)

Attempt. Let A be a set. By axiom 3.4 of singleton sets, there exists $A' = \{A\}$. Assume, for contradiction, that $A \in A$. Since A is the only element of A', by axiom 3.10 of regularity, we need $A' \cap A = \emptyset$. Given $A \in A$, we have $A' \cap A = \{A\} = A' \neq \emptyset$, a contradiction. Hence the assumption is false, and we conclude $A \notin A$.

For the second part, let A, B be sets. By axiom 3.4 of pair sets, there exists $C = \{A, B\}$. Assume, for contradiction, that $A \in B$ and $B \in A$. Since A and B are the only two elements of C, by axiom 3.10 of regularity, we need either $C \cap A = \emptyset$ or $C \cap B = \emptyset$. Since $A \in C$ and $A \in B$, we have $C \cap B = \{A\} \neq \emptyset$, and similarly $C \cap A = \{B\} \neq \emptyset$; both are contradictions. Hence the assumption is false, and we conclude that either $A \notin B$ or $B \notin A$.

Remark. Initially I got stuck on mistakenly trying to show $A = \{A\}$, but that is false and in fact unnecessarily for the proof.

Exercise 3.2.3. Show (assuming the other axioms of set theory) that the universal specification axiom, Axiom 3.9, is equivalent to an axiom postulating the existence of a "universal set" Ω consisting of all objects (i.e., for all objects x, we have $x \in \Omega$). In other words, if Axiom 3.9 is true, then a universal set exists, and conversely, if a universal set exists, then Axiom 3.9 is true. (This helps explain why Axiom 3.9 is called the axiom of *universal* specification.) Note that if a universal set Ω existed, then we would have $\Omega \in \Omega$ by Axiom 3.1, contradicting Exercise 3.2.2. Thus the axiom of foundation specifically rules out the axiom of universal specification.

Attempt. ($\Rightarrow$) We want to show that if Axiom 3.9 is true, then a universal set exists. Let $P(x)$ be a statement that is always true for every object x. By Axiom 3.9, there exists $\{x : P(x) \text{ is true}\}$ such that for every object y,

$$y : \{x : P(x)\} \iff P(y).$$

Let $\Omega = \{x : P(x)\}$. We conclude Ω is the universal set as it contains every object.

($\Leftarrow$) We want to show that if a universal set exists, then Axiom 3.9 is true. Let Ω be a universal set that contains every object. For each $x \in \Omega$, let $P(x)$ be a property pertaining to x. By Axiom 3.6 of specification, there exists a set $\{x \in \Omega : P(x) \text{ is true}\}$ such that for any object y,

$$y \in \{x \in \Omega : P(x) \text{ is true}\} \iff (y \in \Omega \text{ and } P(y) \text{ is true}).$$

This is equivalent to forming a set $\{x : P(x) \text{ is true}\}$ for every object x such that for every object y,

$$y \in \{x : P(x) \text{ is true}\} \iff P(y) \text{ is true}.$$

Therefore we conclude that if a universal set exists, then Axiom 3.9 is true.

Remark. The tricky part is proving the reverse direction, and the key is to make use of Axiom 3.6 of specification.

3.3 Functions

Definition 3.3.1 (Functions) Let X, Y be sets, and let $P(x, y)$ be a property pertaining to an object $x \in X$ and an object $y \in Y$, such that for every $x \in X$, there is exactly one $y \in Y$ for which $P(x, y)$ is true (this is sometimes known as the *vertical line test*). Then we define the *function* $f : X \to Y$ *defined by* P *on the domain* X *and codomain* Y to be the object which, given any input $x \in X$, assigns an output $f(x) \in Y$, defined to be the unique object $f(x) \in Y$ for which $P(x, f(x))$ is true. Thus, for any $x \in X$ and $y \in Y$,

$$y = f(x) \iff P(x, y) \text{ is true}.$$

Functions are also referred to as *maps* or *transformations*, depending on the context.

One common way to define a function is simply to specify its domain, its range, and how one generates the output $f(x)$ from each input; this is known as an *explicit* definition of a function. Example: f has domain and codomain equal to $\boldsymbol{N}$, and $f(x) := x{+}{+}$ for all $x \in \boldsymbol{N}$.

In other cases we only define a function f by specifying what property $P(x, y)$ links the input x with the output $f(x)$; this is an *implicit* definition of a function. Example: $\sqrt{} : [0, +\infty) \to [0, +\infty)$ using the property (or relation) $P(x, y)$ defined by $y^2 = x$.

Definition 3.3.8 (Equality of functions) Two functions $f : X \to Y, g : X' \to Y'$ are said to be equal if their domains and codomains agree (i.e., $X = X'$ and $Y = Y'$), and furthermore that $f(x) = g(x)$ for all $x \in X$. If $f(x)$ and $g(x)$ agree for some values of x in the domain, but not others, then we do not consider f and g to be equal. If two functions f, g have different domains, or different ranges, we also do not consider them to be equal.

Definition 3.3.13 (Composition) Let $f : X \to Y$ and $g : Y \to Z$ be two functions, such that the codomain of f is the same set as the domain of g. We then define the *composition* $g \circ f : X \to Z$ of the two functions g and f to be the function defined explicitly by the formula

$$(g \circ f)(x) := g(f(x)).$$

If the codomain of f does not match the domain of g, we leave the composition $g \circ f$ undefined.

Lemma 3.3.15 (Composition is associative) *Let $f : Z \to W, g : Y \to Z$, and $h : X \to Y$ be functions. Then $f \circ (g \circ h) = (f \circ g) \circ h$.*

Definition 3.3.17 (One-to-one functions) A function f is *one-to-one* (or *injective*) if different elements map to different elements:

$$x \neq x' \implies f(x) \neq f(x').$$

Equivalently, a function is one-to-one if

$$f(x) = f(x') \implies x = x'.$$

Definition 3.3.20 (Onto functions) A function f is *onto* (or *surjective*) if every element in Y comes from applying f to some element in X:

$$\text{For every } y \in Y, \text{ there exists } x \in X \text{ such that } f(x) = y.$$

Definition 3.3.23 (Bijective functions) Functions $f : X \to Y$ which are both one-to-one and onto are also called *bijective* or *invertible*.

If a function $x \mapsto f(x)$ is bijective, then we sometimes call f a *perfect matching* or a *one-to-one correspondence* (not to be confused with the notion of a one-to-one function) and denote the action of f using the notation $x \leftrightarrow f(x)$ instead of $x \mapsto f(x)$. Examples: $0 \leftrightarrow 3, 1 \leftrightarrow 4, 2 \leftrightarrow 5$.

If f is bijective, then for every $y \in Y$, there is exactly one x such that $f(x) = y$ (there is at least one because of surjectivity, and at most one because of injectivity). This value of x is denoted $f^{-1}(y)$; thus f^{-1} is a function from Y to X . We call f^{-1} the inverse of f.

— Exercises —

Exercise 3.3.1. Show that the definition of equality in Definition 3.3.8 is reflexive, symmetric, and transitive. Also verify the substitution property: if $f, \tilde{f} : X \to Y$ and $g, \tilde{g} : Y \to Z$ are functions such that $f = \tilde{f}$ and $g = \tilde{g}$, then $g \circ f = \tilde{g} \circ \tilde{f}$. (Of course, these statements are immediate from the axioms of equality in Appendix A.7 applied directly to the functions in question, but the point of the exercise is to show that they can also be established by instead applying the axioms of equality to elements of the domain and codomain of these functions, rather than to the functions itself.)

Attempt. Given any three functions $f : X \to Y$, $g : X' \to Y'$ and $h : W \to Z$.

- Reflexivity. By Axiom 3.2 of equality of sets, $X = X$ and $Y = Y$. For every object $x \in X$, by the Reflexive axiom A.7 of Equality, $f(x) = f(x)$. Hence the equality of functions is reflexive.
- Symmetry. By Axiom 3.2 of equality of sets, if $X = X'$, then $X' = X$, and similarly, if $Y = Y'$, then $Y' = Y$. For every object $x \in X$, by the Symmetry axiom A.7 of Equality, if $f(x) = g(x)$, then $g(x) = f(x)$. Hence the equality of functions is symmetric.
- Transitivity. If $X = X'$ and $X' = W$, then $X \subseteq X'$ and $X' \subseteq W$ by Definition 3.1.14 of Subsets. By Proposition 3.1.17, $X \subseteq W$. Now by Axiom 3.2 of equality of sets, $W = X'$ and $X' = X$, so applying the same argument we have $W \subseteq X$. Therefore, if $X = X'$ and $X' = W$, then $X = W$. For every object $x \in X$, by the Transitive axiom A.7 of Equality, if object $f(x) = g(x)$ and $g(x) = h(x)$, then $f(x) = h(x)$. Hence the equality of functions is transitive.

We now verify the substitution property. For every object $x \in X$

$$\begin{aligned}
(g \circ f)(x) &= g(f(x)) && \text{(def. 3.3.13)}\\
&= g(\tilde{f}(x)) && \text{(substitution axiom A.7 and } f = \tilde{f})\\
&= \tilde{g}(\tilde{f}(x)) && \text{(substitution axiom A.7 and } g = \tilde{g})\\
&= (\tilde{g} \circ \tilde{f})(x) && \text{(def. 3.3.13)}
\end{aligned}$$

□

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 $g \circ f$.

Attempt.

- Injectivity. If f and g are both injective, by Definition 3.3.17 of One-to-one functions, $f(x) = f(x') \implies x = x'$ for all $x, x' \in X$, and $g(y) = g(y') \implies y = y'$ for all $y, y' \in Y$. By Definition 3.3.13 of Composition, $(g \circ f)(x) = (g \circ f)(x') \iff g(f(x)) = g(f(x'))$. Hence $(g \circ f)(x) = (g \circ f)(x') \iff g(f(x)) = g(f(x')) \implies f(x) = f(x') \implies x = x'$ for all $x, x' \in X$. Therefore, if f and g are both injective, then so is $g \circ f$.
- Surjectivity. If f and g are both surjective, by Definition 3.3.20 of Onto functions, for every $z \in Z$, there exists $y \in Y$ such that $g(y) = z$, and for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$. Hence, for every $z \in Z$, there exists $x \in X$ such that $g(f(x)) = z$. By Definition 3.3.13 of Composition, $g(f(x)) = (g \circ f)(x)$. Therefore, if f and g are both surjective, then so is $g \circ f$.

□

Exercise 3.3.3. When is the empty function into a given set X injective? surjective? bijective?

Attempt.

- The empty function into a given set is vacuously injective iff the domain is empty.
- The empty function into a given set is vacuously surjective iff the codomain $X = \emptyset$.
- The empty function into a given set is vacuously bijective iff both the domain and codomain are empty.

□

Exercise 3.3.4. In this section we give some cancellation laws for composition. Let $f : X \to Y, \tilde{f} : X \to Y, g : Y \to Z$, and $\tilde{g} : Y \to Z$ be functions. Show that if $g \circ f = g \circ \tilde{f}$ and g is injective, then $f = \tilde{f}$. Is the same statement true if g is not injective? Show that if $g \circ f = \tilde{g} \circ f$ and f is surjective, then $g = \tilde{g}$. Is the same statement true if f is not surjective?

Attempt. By Definition 3.3.13 of Composition, $(g \circ f)(x) = (g \circ \tilde{f})(x)$ is equivalent to $g(f(x)) = g(\tilde{f}(x))$. If g is injective, then by Definition 3.3.17 of One-to-one functions, $(g \circ f)(x) = (g \circ \tilde{f})(x) \iff g(f(x)) = g(\tilde{f}(x)) \implies f(x) = \tilde{f}(x)$ for every $x \in X$. It follows that $f = \tilde{f}$. The same statement does not remain true if g is not injective, since we can have $(g \circ f)(x) = (g \circ \tilde{f})(x)$ but $f(x) \neq \tilde{f}(x)$ for $x \in X$.

By Definition 3.3.13 of Composition, $(g \circ f)(x) = (\tilde{g} \circ f)(x)$ is equivalent to $g(f(x)) = \tilde{g}(f(x))$. If f is surjective, then by Definition 3.3.20 of Onto functions, for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$. Therefore if $g(f(x)) = \tilde{g}(f(x))$ for every $x \in X$, then $g(y) = \tilde{g}(y)$ for every $y \in Y$. It follows that $g = \tilde{g}$. The same statement does not remain true if f is not surjective, since there can exists $y' \in Y$ such that $g(y') \neq \tilde{g}(y')$ and $y' \neq f(x)$ for every $x \in X$. □

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 also be surjective?

Attempt. Suppose $g \circ f$ is injective, we aim to show that f must be injective. By Definition 3.3.17 of One-to-one functions, $x \neq x' \implies (g \circ f)(x) \neq (g \circ f)(x')$ for some $x, x' \in X$. Assume, for contradiction, that f is not injective. Let $x, x' \in X$ such that $x \neq x'$ and $f(x) = f(x')$, which implies $g(f(x)) = g(f(x'))$. By Definition 3.3.13 of Composition, $g(f(x)) = g(f(x'))$ is equivalent to $(g \circ f)(x) = (g \circ f)(x')$, contradicting $(g \circ f)(x) \neq (g \circ f)(x')$. Hence the assumption is false. We conclude that if $g \circ f$ is injective, then f must be injective.

Suppose $g \circ f$ is injective so f must also be injective. We aim to show by counter example that g is not necessarily injective. For example, let $X = \{1, 2\}, Y = \{a, b, c\}, Z = \{\alpha, \beta\}$, and let $f(1) = a, f(2) = b, g(a) = \alpha, g(b) = g(c) = \beta$. In particular, $g(b) = g(c)$ so g is not injective. We conclude that if $g \circ f$ is injective, then f must be injective, but not necessarily g.

Suppose $g \circ f$ is surjective, we aim to show that g must be surjective. By Definition 3.3.20 of Onto functions, for every $z \in Z$, there exists $x \in X$ such that $(g \circ f)(x) = z$. By Definition 3.3.13 of Composition, $(g \circ f)(x) = z \iff g(f(x)) = z$. Therefore, for every $z \in Z$, there must exist $y \in Y$ such that $g(y) = z$. We conclude that if $g \circ f$ is surjective, then g must also be surjective.

Suppose $g \circ f$ is surjective so g must also be surjective. We aim to show by counter example that f is not necessarily surjective. For example, let $X = \{1\}, Y = \{a, b\}, Z = \{\alpha\}$, and let $f(1) = a, g(a) = g(b) = \alpha$. In particular, b is outside the image of f so f is not surjective. We conclude that if $g \circ f$ is surjective, then g must be surjective, but not necessarily f. □

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 (thus $(f^{-1})^{-1} = f$).

Attempt. Given f is bijective, for every $x \in X$, there exists a unique $y \in Y$ such that $y = f(x)$. Let f^{-1} be the inverse of f so that $f^{-1}(y) = x$. Substituting y by $f(x)$, we get

$$f^{-1}(y) = f^{-1}(f(x)) = x \text{ for every } x \in X.$$

Also, given f is bijective, for every $y \in Y$, there exists a unique $x \in X$ such that $y = f(x)$. Since f^{-1} is defined as the inverse of f so that $f^{-1}(y) = x$, we apply f to both sides and get

$$f(f^{-1}(y)) = f(x) = y \text{ for every } y \in Y.$$

We aim to show that f^{-1} is invertible, i.e., bijective:

- Surjectivity. For every $x \in X$, there exists $y \in Y$, namely $y = f(x)$, such that $f^{-1}(y) = x$. Hence f^{-1} is surjective.
- Injectivity. Let $y, y' \in Y$ and $y \neq y'$. Assume, for contradiction, that $f^{-1}(y) = f^{-1}(y') = x$. But this is absurd, since $f(x)$ cannot be equal to both y and y'. Hence the assumption is false. If $y \neq y'$, then $f^{-1}(y) \neq f^{-1}(y')$. Therefore f^{-1} is injective.

We conclude that f^{-1} is also invertible and has f as its inverse (thus $(f^{-1})^{-1} = f$). □

Remark. This one turned out to be quite challenging in getting the presentation right.

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 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Attempt. (Injectivity.) Let $x, x' \in X$ and $x \neq x'$. If f is injective, then $f(x) \neq f(x')$. If g is injective, then $g(f(x)) \neq g(f(x'))$. Therefore $g \circ f$ is also injective. (Surjectivity.) If g is surjective, then for every $z \in Z$, there exists $y \in Y$ such that $g(y) = z$. If f is surjective, then for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$. So then for every $z \in Z$, there must exist $x \in X$ such that $(g \circ f)(x) = z$, i.e., $(g \circ f)$ is surjective. We conclude that if f and g are bijective, then so is $g \circ f$.

Since g, f and $g \circ f$ are bijective, they are all invertible. So, for every $z \in Z$, $z = (g \circ f \circ f^{-1} \circ g^{-1})(z)$, and for every $x \in X, x = (f^{-1} \circ g^{-1} \circ g \circ f \circ)(x)$. By Lemma 3.3.15 of associativity, $g \circ f \circ f^{-1} \circ g^{-1} = (g \circ f) \circ (f^{-1} \circ g^{-1})$, and $f^{-1} \circ g^{-1} \circ g \circ f = (f^{-1} \circ g^{-1}) \circ (g \circ f)$. In both cases, $(f^{-1} \circ g^{-1})$ is the inverse of $(g \circ f)$. Also, both $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ share the same domain Z and codomain X. By definition 3.3.8 of equality of functions, we conclude $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Remark. For the second part, it's important to show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ holds on both left and right sides.

Exercise 3.3.8. If X is a subset of Y , let $\iota_{X \to Y} : X \to Y$ be the *inclusion map* from X to Y , defined by mapping $x \mapsto x$ for all $x \in X$, i.e., $\iota_{X \to Y}(x) := x$ for all $x \in X$. The map $\iota_{X \to X}$ is in particular called the *identity map* on X.

(a) Show that if $X \subseteq Y \subseteq Z$ then $\iota_{Y \to Z} \circ \iota_{X \to Y} = \iota_{X \to Z}$.

(b) Show that if $f : A \to B$ is any function, then $f = f \circ \iota_{A \to A} = \iota_{B \to B} \circ f$.

(c) Show that, if $f : A \to B$ is a bijective function, then $f \circ f^{-1} = \iota_{B \to B}$ and $f^{-1} \circ f = \iota_{A \to A}$.

(d) Show that if X and Y are disjoint sets, and $f : X \to Z$ and $g : Y \to Z$ are functions, then there is a unique function $h : X \cup Y \to Z$ such that $h \circ \iota_{X \to X \cup Y} = f$ and $h \circ \iota_{Y \to X \cup Y} = g$.

(e) Show that the hypothesis that X and Y are disjoint can be dropped in (d) if one adds the additional hypothesis that $f(x) = g(x)$ for all $x \in X \cap Y$.

Attempt.

(a) Given $X \subseteq Y \subseteq Z$, $\iota_{X \to Y}$ maps $x \mapsto x$ from domain X to codomain Y for all $x \in X$, and $\iota_{Y \to Z}$ maps $y \mapsto y$ from domain Y to codomain Z for all $y \in Y$, $\iota_{Y \to Z} \circ \iota_{X \to Y}$ maps $x \mapsto x$ from domain X to codomain Z for all $x \in X$. Let $\iota_{X \to Z}$ maps $x \mapsto x$ from domain X to codomain Z for all $x \in X$. By definition 3.3.8 of equality of functions, we conclude $\iota_{X \to Z} = \iota_{Y \to Z} \circ \iota_{X \to Y}$.

(b) $\iota_{A \to A}$ maps $a \mapsto a$ from domain A to codomain A for all $a \in A$. Thus $(f \circ \iota_{A \to A})(a) = f(\iota_{A \to A}(a)) = f(a)$ for all $a \in A$. Since both $f \circ \iota_{A \to A}$ and f also have the same domain A and codomain B, they are equal by Definition 3.3.8 of equality of functions.

Similarly, $\iota_{B \to B}$ maps $b \mapsto b$ from domain B to codomain B for all $b \in B$. Thus $(\iota_{B \to B} \circ f)(a) = \iota_{B \to B}(f(a)) = f(a)$ for all $a \in A$. Since both $\iota_{B \to B} \circ f$ and f also have the same domain A and codomain B, they are equal by Definition 3.3.8 of equality of functions.

We conclude that $f = f \circ \iota_{A \to A} = \iota_{B \to B} \circ f$.

(c) Since $f : A \to B$ is bijective, it has an inverse $f^{-1} : B \to A$. For every $b \in B$, $(f \circ f^{-1})(b) = f(f^{-1}(b)) = b = \iota_{B\to B}(b)$. Since both $f \circ f^{-1}$ and $\iota_{B\to B}$ also have the same domain B and codomain B, they are equal by Definition 3.3.8 of equality of functions.

Similarly, for every $a \in A$, $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a = \iota_{A\to A}(a)$. Since both $f^{-1} \circ f$ and $\iota_{A\to A}$ also have the same domain A and codomain A, they are equal by Definition 3.3.8 of equality of functions.

We conclude that $f \circ f^{-1} = \iota_{B\to B}$ and $f^{-1} \circ f = \iota_{A\to A}$.

(d) First we want to verify the function $h : X \cup Y \to Z$ exists. Since X and Y are disjoint, for every $w \in X \cup Y$, $h(w) = f(w)$ if $w \in X$, and $h(w) = g(w)$ if $w \in Y$. We conclude that h is well defined.

Suppose another function $i : X \cup Y \to Z$ satisfies the same conditions. Given X and Y are disjoint, either $w \in X$ or $w \in Y$ but not both. If $w \in X$, $i(w) = (i \circ \iota_{X\to X\cup Y})(w) = f(w) = h(w)$. If $w \in Y$, $i(w) = (i \circ \iota_{Y\to X\cup Y})(w) = g(w) = h(w)$. Thus, $i = h$.

Therefore, if X and Y are disjoint sets, and $f : X \to Z$ and $g : Y \to Z$ are functions, then there is a unique function $h : X \cup Y \to Z$ such that $h \circ \iota_{X\to X\cup Y} = f$ and $h \circ \iota_{Y\to X\cup Y} = g$.

(e) Given $h : X \cup Y \to Z$ is defined as

$$h(w) = \begin{cases} f(w) & \text{for w} \in \text{X} \\ g(w) & \text{for w} \in \text{Y} \end{cases}$$

If X and Y are not disjoint, then h is well defined only if $f(w) = g(w)$ for every $w \in X \cap Y$. Otherwise, it would be absurd if there exists $w \in X \cap Y$ such that $h(w) = f(w)$ and $h(w) = g(w)$ but $f(w) \neq g(w)$. Conversely, if $f(w) = g(w)$ for every $w \in X \cap Y$, then h is well defined, and X and Y do not need to be disjoint.

□

3.4 Images and Inverse Images

Definition 3.4.1 (Images of sets) If $f : X \to Y$ is a function from X to Y, and S is a subset of X, we define $f(S)$ to be the set

$$f(S) := \{f(x) : x \in S\};$$

this set is a subset of Y and is sometimes called the *image* of S under the map f. We sometimes call $f(S)$ the *forward image* of S to distinguish it from the concept of the *inverse image* $f^{-1}(S)$ of S, which is defined below.

The image $f(X)$ of the domain is also known as the *range* of the function $f : X \to Y$; it is a subset of the codomain Y.

In general,

$$x \in S \implies f(x) \in f(S)$$

but

$$f(x) \in f(S) \not\Rightarrow x \in S.$$

Rather,

$$y \in f(S) \iff y = f(x) \text{ for some } x \in S.$$

Definition 3.4.5 (Inverse images) If U is a subset of Y, we define the set $f^{-1}(U)$ to be the set

$$f^{-1}(U) := \{x \in X : f(x) \in U\}.$$

In other words, $f^{-1}(U)$ consists of all the elements of X which map into U:

$$f(x) \in U \iff x \in f^{-1}(U).$$

We call $f^{-1}(U)$ the *inverse image* of U.

Note that f does not have to be invertible in order for $f^{-1}(U)$ to make sense.

Functions are not necessarily sets. However, we do consider functions to be a type of object, and in particular we should be able to consider sets of functions. In particular, we should be able to consider the set of all functions from a set X to a set Y. To do this we need to introduce another axiom to set theory:

Axiom 3.11 (Power set axiom) Let X and Y be sets. Then there exists a set, denoted Y^X, which consists of all the functions from X to Y, thus

$$f \in Y^X \iff (f \text{ is a function with domain } X \text{ and codomain } Y).$$

The reason we use the notation Y^X to denote this set is that if Y has n elements and X has m elements, then one can show that Y^X has n^m elements.

Lemma 3.4.10 (Power set) *Let X be a set. Then the set*

$$\{Y : Y \textit{ is a subset of } X\}$$

is a set. That is to say, there exists a set Z such that

$$Y \in Z \iff Y \subseteq X$$

for all objects Y.

Axiom 3.12 (Union) Let A be a set, all of whose elements are themselves sets. Then there exists a set $\bigcup A$ whose elements are precisely those objects which are elements of the elements of A, thus for all objects x

$$x \in \bigcup A \iff (x \in S \text{ for some } S \in A).$$

The axiom of union, combined with the axiom of pair set, implies the axiom of pairwise union. Another important consequence of this axiom is that if one has some set I, and for every element $\alpha \in I$ we have some set A_α, then we can form the union set $\bigcup_{\alpha\in I} A_\alpha$ by defining

$$\bigcup_{\alpha\in I} A_\alpha := \bigcup\{A_\alpha : \alpha \in I\},$$

which is a set thanks to the axiom of replacement and the axiom of unions. More generally, we see that for any object y,

$$y \in \bigcup_{\alpha\in I} A_\alpha \iff (y \in A_\alpha \text{ for some } \alpha \in I). \tag{3.2}$$

In situations like this, we often refer to I as an *index set*, and the elements α of this index set as *labels*; the sets A_α are then called a *family of sets* and are *indexed* by the labels $\alpha \in I$. Note that if I was empty, then $\bigcup_{\alpha\in I} A_\alpha$ would automatically also be empty.

We can similarly form intersections of families of sets, as long as the index set is non-empty. More specifically, given any non-empty set I, and given an assignment of a set A_α to each $\alpha \in I$, we can define the intersection $\bigcap_{\alpha\in I} A_\alpha$ by first choosing some element β of I (which we can do since I is non-empty), and setting

$$\bigcap_{\alpha\in I} A_\alpha := \{x \in A_\beta : x \in A_\alpha \text{ for all } \alpha \in I\}, \tag{3.3}$$

which is a set by the axiom of specification. This definition may look like it depends on the choice of β, but it does not. Observe that for any object y,

$$y \in \bigcap_{\alpha\in I} A_\alpha \iff (y \in A_\alpha \text{ for all } \alpha \in I) \tag{3.4}$$

(compare with (3.2)).

The axioms of set theory that we have introduced (Axioms 3.1 and 3.12, excluding the dangerous Axiom 3.9) are known as the *Zermelo–Fraenkel axioms of set theory.*

— Exercises —

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 set as the inverse image of V under f; thus the fact that both sets are denoted by $f^{-1}(V)$ will not lead to any inconsistency.

Attempt. Given f is bijective, there exists a unique $x \in X$ such that $y = f(x)$ for every $y \in V$. Given V is a subset of Y, by definition 3.4.1 of image of sets, the forward image of V under f^{-1} is

$$\begin{aligned} f^{-1}(V) &= \{f^{-1}(y) : y \in V\} \\ &= \{f^{-1}(f(x)) \in X : f(x) \in V\} && \text{(substitute } y = f(x)) \\ &= \{x \in X : f(x) \in V\} \end{aligned}$$

which is the inverse image of V under f by definition 3.4.5 of inverse images. □

Exercise 3.4.2 Let $f : X \to Y$ be a function from one set X to another set Y, let S be a subset of X, and let U be a subset of Y.

(i) What, in general, can one say about $f^{-1}(f(S))$ and S?

(ii) What about $f(f^{-1}(U))$ and U ?

(iii) What about $f^{-1}(f(f^{-1}(U)))$ and $f^{-1}(U)$?

Attempt.

(i) $S \subseteq f^{-1}(f(S))$. The preimage $f^{-1}(f(S))$ can become larger if f is not injective.

(ii) $f(f^{-1}(U)) \subseteq U$. The image $f(f^{-1}(U))$ can become smaller if U contains elements that are outside the image of X under f.

(iii) $f^{-1}(f(f^{-1}(U))) = f^{-1}(U)$. Based on (ii), $f(f^{-1}(U)) \subseteq U$. The difference is that U may contain additional objects that fall outside the image of X under f, but these objects have no effect on the reverse image of U.

Remark. This one is tricker than it looks at first sight.

Exercise 3.4.3 Let A, B be two subsets of a set X, and let $f : X \to Y$ be a function. Show that $f(A \cap B) \subseteq f(A) \cap f(B)$, that $f(A) \setminus f(B) \subseteq f(A \setminus B)$, $f(A \cup B) = f(A) \cup f(B)$. For the first two statements, is it true that the $\subseteq$ relation can be improved to $=$?

Attempt.

- We aim to show $f(A \cap B) \subseteq f(A) \cap f(B)$.

  By definition 3.4.1 of images of sets, $f(A \cap B) = \{f(x) : x \in A \cap B\}$. By definition 3.1.22 of intersections, $x \in A \cap B \iff x \in A$ and $x \in B$ which implies $f(x) \in f(A)$ and $f(x) \in f(B)$. Equivalently, $f(x) \in f(A) \cap f(B)$. Hence, $f(A \cap B) = \{f(x) : x \in A \cap B\} \subseteq \{f(x) : f(x) \in f(A) \cap f(B)\} = f(A) \cap f(B)$.

  We cannot improve the $\subseteq$ in this case to $=$ because in general $x \in S \implies f(x) \in f(S)$ but not the other way around. For example, if $A = \{1\}, B = \{2\}$, and $f(1) = f(2) = a$, then $f(A \cap B) = \emptyset$ which is not equal to $f(A) \cap f(B) = \{a\}$. □

- We aim to show $f(A) \setminus f(B) \subseteq f(A \setminus B)$. We observe that

$$A \setminus (A \cap B) = A \setminus B \tag{3.4.3a}$$

$$\begin{aligned} A &= (A \setminus (A \cap B)) \cup (A \cap B) \\ &= (A \setminus B) \cup (A \cap B) && \text{(by 3.4.3a)} \end{aligned}$$

$$\therefore f(A) = f(A \setminus B) \cup f(A \cap B) \tag{3.4.3b}$$

We also observe that set difference distributes over union on the left (instead of invoking De Morgan's law when the union is on the right). Namely,

$$(f(A) \cup f(B)) \setminus f(C) = f(A) \setminus f(C) \cup f(B) \setminus f(C) \tag{3.4.3c}$$

So,

$$\begin{aligned}
f(A) \setminus f(B) &= \big(f(A \setminus B) \cup f(A \cap B)\big) \setminus \big(f(B \setminus A) \cup f(A \cap B)\big) && \text{(by 3.4.3b)} \\
&= \big(\big(f(A \setminus B) \cup f(A \cap B)\big) \setminus f(B \setminus A)\big) \cap \\
&\qquad \big(\big(f(A \setminus B) \cup f(A \cap B)\big) \setminus f(A \cap B)\big) && \text{(De Morgan 3.1.27(h))} \\
&= \big(\big(f(A \setminus B) \cup f(A \cap B)\big) \setminus f(B \setminus A)\big) \cap \\
&\qquad (f(A \setminus B) \setminus f(A \cap B)) \cup (f(A \cap B) \setminus f(A \cap B)) && \text{(by 3.4.3c)} \\
&= \big(\big(f(A \setminus B) \cup f(A \cap B)\big) \setminus f(B \setminus A)\big) \cap \\
&\qquad (f(A \setminus B) \setminus f(A \cap B) \cup \emptyset) \\
&\subseteq f(A \setminus B)
\end{aligned}$$

Hence $f(A) \setminus f(B) \subseteq f(A \setminus B)$.

We cannot improve the $\subseteq$ in this case to $=$ in general. For example, if $A = \{1\}, B = \{2\}$, and $f(1) = f(2) = a$, then $f(A) \setminus f(B) = \emptyset$ which is not equal to $f(A \setminus B) = \{a\}$.

For the first part, there is also a simple argument. Let $f(x) \in f(A) \setminus f(B)$. So $f(x) \in f(A)$ and $f(x) \notin f(B)$. By definition 3.4.1 of image of sets, $f(x) \in f(A) \iff y = f(x)$ for some $x \in A$. Then $x \notin B$, for otherwise $x \in B \implies f(x) \in f(B)$, a contradiction. Hence $f(x) \in f(A) \setminus f(B) \implies x \in A \setminus B \implies fx() \in f(A \setminus B)$, i.e., $f(A) \setminus f(B) \subseteq f(A \setminus B)$. □

- We aim to show $f(A \cup B) = f(A) \cup f(B)$.

$$\begin{aligned}
f(A \cup B) &= \{f(x) : x \in A \cup B\} && \text{(def. 3.4.1 images of sets)} \\
&= \{f(x) : x \in A \text{ or } x \in B\} && \text{(axiom 3.5 pairwise union)} \\
&= \{f(x) : x \in A\} \cup \{f(x) : x \in B\} && \text{(axiom 3.5 \& 3.7 replacement)} \\
&= f(A) \cup f(B) && \text{(def. 3.4.1 images of sets)}
\end{aligned}$$

□

Exercise 3.4.4 Let $f : X \to Y$ be a function from one set X to another set Y , and let U, V be subsets of Y . Show that $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$, that $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$, and that $f^{-1}(U \setminus V) = f^{-1}(U) \setminus f^{-1}(V)$.

Attempt.

- We want to show $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$.

$$\begin{aligned}
x \in f^{-1}(U \cup V) &\iff f(x) \in U \cup V && \text{(def. 3.4.5 inverse images)} \\
&\iff f(x) \in U \text{ or } f(x) \in V && \text{(axiom 3.5 pairwise union)} \\
&\iff x \in f^{-1}(U) \text{ or } x \in f^{-1}(V) && \text{(def. 3.4.5 inverse images)} \\
&\iff x \in f^{-1}(U) \cup f^{-1}(V) && \text{(axiom 3.5 pairwise union)}
\end{aligned}$$

- We want to show $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$.

$$\begin{aligned}
x \in f^{-1}(U \cap V) &\iff f(x) \in U \cap V && \text{(def. 3.4.5 inverse images)} \\
&\iff f(x) \in U \text{ and } f(x) \in V && \text{(def. 3.1.22 intersections)} \\
&\iff x \in f^{-1}(U) \text{ and } x \in f^{-1}(V) && \text{(def. 3.4.5 inverse images)} \\
&\iff x \in f^{-1}(U) \cap f^{-1}(V) && \text{(def. 3.1.22 intersections)}
\end{aligned}$$

- We want to show $f^{-1}(U \setminus V) = f^{-1}(U) \setminus f^{-1}(V)$.

$$\begin{aligned}
x \in f^{-1}(U \setminus V) &\iff f(x) \in U \setminus V && \text{(def. 3.4.5 inverse images)}\\
&\iff f(x) \in U \text{ and } f(x) \notin V && \text{(def. 3.1.26 difference sets)}\\
&\iff x \in f^{-1}(U) \text{ and } x \notin f^{-1}(V) && \text{(def. 3.4.5 inverse images)}\\
&\iff x \in f^{-1}(U) \setminus f^{-1}(V) && \text{(def. 3.1.26 difference sets)}
\end{aligned}$$

□

Remark. Initially I tried a set-based approach, but ran into difficulties in justifying transitions. It turns out to be much easier to reason about from the perspective of set membership. For example,

$$\begin{aligned}
f^{-1}(U \setminus V) &= \{x \in X : f(x) \in U \setminus V\} && \text{(def. 3.4.5 inverse images)}\\
&= \{x \in X : f(x) \in U \text{ and } f(x) \notin V\} && \text{(def. 3.1.26 difference sets)}\\
&= \{x \in X : f(x) \in U\} \setminus \{x \in X : f(x) \in V\} && \text{(How to justify?)}\\
&= f^{-1}(U) \setminus f^{-1}(V)
\end{aligned}$$

Exercise 3.4.5 Let $f : X \to Y$ be a function from one set X to another set Y. Show that $f(f^{-1}(S)) = S$ for every $S \subseteq Y$ if and only if f is surjective. Show that $f^{-1}(f(S)) = S$ for every $S \subseteq X$ if and only if f is injective.

Attempt. To show that $f(f^{-1}(S)) = S$ for every $S \subseteq Y$ if and only if f is surjective, we want to show

1. ($\Rightarrow$) $f(f^{-1}(S)) = S$ for every $S \subseteq Y \implies f$ is surjective. We prove by contrapositive. Suppose f is not surjective. Then there exists $y \in Y$ such that $y \neq f(x)$ for all $x \in X$. Let $S = \{y\}$, so $f^{-1}(S) = \emptyset$. Therefore $f(f^{-1}(S)) = \emptyset \neq S$. Hence the statement $f(f^{-1}(S)) = S$ for every $S \subseteq Y$ is false, as desired.

2. ($\Leftarrow$) f is surjective $\implies f(f^{-1}(S)) = S$ for every $S \subseteq Y$. Suppose f is surjective, for every $S \subseteq Y$, we want to show that

   (a) ($\subseteq$) $f(f^{-1}(S)) \subseteq S$. Let $y \in f(f^{-1}(S))$, and let $x \in f^{-1}(S)$ such that $y = f(x)$. By definition 3.4.5 of inverse images, $f(x) \in S$, so $y \in S$.

   (b) ($\supseteq$) $S \subseteq f(f^{-1}(S))$. Let $y \in S$. Since f is surjective, there exists $x \in X$ such that $y = f(x)$. So $f(x) \in S$. By definition 3.4.5 of inverse images, $x \in f^{-1}(S)$, which implies $f(x) \in f(f^{-1}(S))$ by definition 3.4.1 of image of sets.

To show that $f^{-1}(f(S)) = S$ for every $S \subseteq X$ if and only if f is injective, we want to show

1. ($\Rightarrow$) $f^{-1}(f(S)) = S$ for every $S \subseteq X \implies f$ is injective. We prove by contrapositive. Suppose f is not injective. Let $x, x' \in X, x \neq x'$, $f(x) = f(x') = y$, and let $S = \{x\}$. So $f(S) = \{y\}, f^{-1}(f(S)) = \{x, x'\} \neq S$. Therefore, the statement $f^{-1}(f(S)) = S$ for every $S \subseteq X$ is false, as desired.

2. ($\Leftarrow$) f is injective $\implies f^{-1}(f(S)) = S$ for every $S \subseteq X$. Suppose f is injective. For every $S \subseteq X$, we want to show that

   (a) ($\subseteq$) $f^{-1}(f(S)) \subseteq S$. Let $x \in f^{-1}(f(S))$. By definition 3.4.5 of inverse images, $f(x) \in f(S)$. So, by definition 3.4.1 of images of sets, $f(x) = f(s)$ for some $s \in S$. Since f is injective, $x = s$. Therefore, $x \in S$, as desired.

   (b) ($\supseteq$) $S \subseteq f^{-1}(f(S))$. Let $x \in S$. By definition 3.4.1 of images of sets, $f(x) \in f(S)$. By definition 3.4.5 of inverse images, $x \in f^{-1}(f(S))$, as desired.

□

Remarks.

1. In general, it may appear that $f(x) \in U$ is a stronger statement than $f(x) \in f(S)$. The reason is that $f(x) \in U \iff x \in f^{-1}(U)$, whereas $f(x) \in f(S) \not\Rightarrow x \in S$, but rather $f(x) \in f(S) \iff f(x) = f(s)$ for some $s \in S$. But then of course $f(x) \in f(S) \iff x \in f^{-1}(f(S))$. This is a good reminder that $f^{-1} \circ f$ is not in general an identity function.

2. In general, by definition 3.4.1 of images of sets,

$$y \in f(S) \iff y = f(x) \text{ for some } x \in S.$$

   Suppose, however, $f(x) \in f(S)$. Then

$$f(x) \in f(S) \iff f(x) = f(s) \text{ for some } s \in S$$

   which can be quite useful (e.g. if f was injective).

3. During a proof via contrapositive, a clever trick is to narrow the proof to finding a counter example to the hypothesis that is supposed to hold in general.

Exercise 3.4.6

(i) Prove Lemma 3.4.10. (*Hint*: start with the set $\{0,1\}^X$ and apply the replacement axiom, replacing each function f with the object $f^{-1}(\{1\})$.)

(ii) Conversely, show that Axiom 3.11 can be deduced the preceding axioms of set theory if one accepts Lemma 3.4.10 as an axiom. (This may help explain why we refer to Axiom 3.11 as the "power set axiom".)

Attempt.

(i) We want to show that there exists a set Z such that $Y \in Z \iff Y \subseteq X$ for all objects Y. By axiom 3.11 of power set, there exists a set $\{0,1\}^X = \{f : X \to \{0,1\}\}$ which consists of all the functions from X to $\{0,1\}$. Note that there is at most one $f^{-1}(\{1\})$ for a given $f \in \{0,1\}^X$. By axiom 3.7 of replacement, there exists a set Z $= \{f^{-1}(\{1\}) : f \in \{0,1\}^X\}$. We aim to show

   (a) $(\Rightarrow) Y \in Z \implies Y \subseteq X$. Suppose $Y \in Z$. Then $Y = f^{-1}(\{1\})$ for some $f \in \{0,1\}^X$. By axiom 3.11 of power set, the domain of f is X, so Y being a preimage must be a subset of X. Hence $Y \in Z \implies Y \subseteq X$.

   (b) $(\Leftarrow) Y \subseteq X \implies Y \in Z$. Suppose $Y \subseteq X$. Let $f : X \to \{0,1\}$ be a function such that $f(x) = 1$ for every $x \in Y$ and $f(x) = 0$ for every $x \notin Y$. Note that $f \in \{0,1\}^X$, since f is defined for every elements in X to the codomain $\{0,1\}$. So $Y = f^{-1}(\{1\})$. Hence $Y \in Z$. We conclude $Y \subseteq X \implies Y \in Z$.

(ii) Let X and Y be sets, so the set $X \times Y = \{(x,y) : x \in X \text{ and } y \in Y\}$ contains all ordered pairs of elements from X and Y. By Lemma 3.4.10 as an axiom, the set $\Omega = \{S : S \subseteq X \times Y\}$ exists. We want to show that there exists a set, denoted Y^X, which consists of all the functions from domain X to codomain Y.

   For each $S \in \Omega$, let

$$P(S) \iff \forall x \in X, \exists! y \in Y, \text{ such that } (x,y) \in S.$$

   By axiom 3.6 of specification, the set $\{S \in \Omega : P(S) \text{ is true}\}$ exists. Since Ω contains all the possible subsets of $X \times Y$, the set $\{S \in \Omega : P(S) \text{ is true}\}$ is the set of all functions from domain X to codomain Y. Therefore Y^X exists.

□

Remarks.

1. I found the second part much more challenging than the first part. In particular, trying to characterize $Y^X = \{f \mid f : X \to Y\}$ didn't help for this is insufficiently clear.

2. Let X and Y be sets. A specific function $f : X \to Y$ can be defined as a set of ordered pairs from every $x \in X$ to exactly one $y \in Y$. If both X and Y are finite, then the total number of possible functions from X to Y, or sets of ordered pairs, is finite, and specifically is equal to $|Y|^{|X|}$.

3. Simple as (2) may seem, trying to express this in a single set definition, however, seems impossible. The reason is that any condition that can be specified inside a set definition must refer only to each individual element of the set, but not to the entire set itself which is still being defined. This runs into problem when we need to specify relationship among elements.

4. Instead, a function $f : X \to Y$ can be defined in multiple stages: first as a set, and then the additional constraints on the set can be specified outside the set definition. For example,

$$f = \{(x, y) : x \in X, y \in Y\}$$

   such that $\forall x \in X, \exists! y \in Y$ with $(x, y) \in f$.

5. The key insight to the second part is that a function is concretely defined as a set of ordered pairs. Furthermore, such set is a subset of the cartesian product of the domain and codomain of the function.

6. However, defining functions as sets of ordered pairs loses information (specifically about the codomain). For example, let f and g be two functions. Both have the same domain, say $\mathbb{Z}$ for integers, but f has codomain $\mathbb{N}$ (natural number), whereas g has codomain $\mathbb{R}$ (real number). Now, let $f(z) = g(z)$ for all $z \in Z$. The two *function graphs* are equal, but the two functions are not.

Exercise 3.4.7 Let X, Y be sets. Define a *partial function* from X to Y to be any function $f : X' \to Y'$ whose domain X' is a subset of X, and whose codomain Y' is a subset of Y. Show that the collection of all partial functions from X to Y is itself a set. (Hint: use Exercise 3.4.6, the power set axiom, the replacement axiom, and the union axiom.)

Attempt. Let X, Y be sets. By Lemma 3.4.10, the set $\Omega_X = \{S : S \subseteq X\}$ exists, and so does the set $\Omega_Y = \{S : S \subseteq Y\}$. Let $X' \in \Omega_X$ and $Y' \in \Omega_Y$. By axiom 3.11 of power set, there exists $Y'^{X'}$, a set of all functions from domain X' to codomain Y'. For any object $S \in \Omega_Y$, there is exactly one set, $S^{X'}$, that contains all functions from X' to S. By axiom 3.7 of replacement, we have $A_{X'} = \{S^{X'} : S \in \Omega_Y\}$. By axiom 3.12 of union, we have $B_{X'} = \cup A_{X'}$, which is the set of all partial functions from X' to Y. For any object $S \in \Omega_X$, there is exactly one set, B_S, that contains all partial functions from S to Y. By axiom 3.7 of replacement, we have $C = \{B_S : S \in \Omega_X\}$. Hence, by axiom 3.12 of union, there exists $\cup C$, a set that contains all partial functions from X to Y. □

Remarks. We avoid the use of the Cartesian product $X \times Y$ for this exercise, since it has not been defined at this stage. Instead, we applied axiom 3.7 of replacement twice in a nested fashion. It's important to specify the condition (either explicitly or implicitly) before axiom 3.7 of replacement is applied, namely, that "there is at most one y for which $P(x, y)$ is true".

Exercise 3.4.8 Show that Axiom 3.5 can be deduced from Axiom 3.1, Axiom 3.4, and Axiom 3.12.

Attempt. Given two sets A, B, we want to show there exists a set $A \cup B$, which consists of all the elements which belong to A or B. By axiom 3.1, sets are objects so it makes sense to have A, B as elements of a set. By axiom 3.4, we have the set $\{A, B\}$. By axiom 3.12, $\bigcup\{A, B\}$ is a set whose elements are precisely those objects which are elements of either A or B. Hence $\bigcup\{A, B\} = A \cup B$. We conclude the set $A \cup B$ exists. □

Exercise 3.4.9 Show that if β and β' are two elements of a set I, and to each $\alpha \in I$ we assign a set A_α, then

$$\{x \in A_\beta : x \in A_\alpha \text{ for all } \alpha \in I\} = \{x \in A_{\beta'} : x \in A_\alpha \text{ for all } \alpha \in I\},$$

and so the definition of $\bigcap_{\alpha \in I} A_\alpha$ defined in (3.3) does not depend on β. Also explain why (3.4) is true.

Attempt. Let $S_\beta = \{x \in A_\beta : x \in A_\alpha \text{ for all } \alpha \in I\}$, and $S_{\beta'} = \{x \in A_{\beta'} : x \in A_\alpha \text{ for all } \alpha \in I\}$. We want to show $S_\beta \subseteq S_{\beta'}$ and $S_{\beta'} \subseteq S_\beta$. Suppose $y \in S_\beta$. By definition, $y \in A_\beta$, and $y \in A_\alpha$ for every $\alpha \in I$. In particular, $y \in A_{\beta'}$ since $\beta' \in I$. Therefore $y \in S_{\beta'}$. We conclude $S_\beta \subseteq S_{\beta'}$. Conversely, $S_{\beta'} \subseteq S_\beta$ by applying similar argument. Hence $S_\beta = S_{\beta'}$.

To explain why (3.4) is true, we want to show that the implications hold in both directions.

1. ($\Rightarrow$) $y \in \bigcap_{\alpha \in I} A_\alpha \implies (y \in A_\alpha \text{ for all } \alpha \in I)$. Let $y \in \bigcap_{\alpha \in I} A_\alpha$. By definition 3.3, the statement ($y \in A_\beta$ for some $\beta \in I$ such that $y \in A_\alpha$ for every $\alpha \in I$) holds. Since there is no dependency on β as shown above, we conclude that $y \in A_\alpha$ for every $\alpha \in I$.

2. ($\Leftarrow$) $(y \in A_\alpha \text{ for all } \alpha \in I) \implies y \in \bigcap_{\alpha \in I} A_\alpha$. Conversely, given $y \in A_\alpha$ for all $\alpha \in I$, I is non-empty, and it must be the case that $y \in A_\beta$ for some $\beta \in I$. Therefore, the statement ($y \in A_\beta$ for some $\beta \in I$ such that $y \in A_\alpha$ for every $\alpha \in I$) holds.

□

Exercise 3.4.10 Suppose that I and J are two sets, and for all $\alpha \in I \cup J$ let A_α be a set. Show that $\left(\bigcup_{\alpha \in I} A_\alpha\right) \cup \left(\bigcup_{\alpha \in J} A_\alpha\right) = \bigcup_{\alpha \in I \cup J} A_\alpha$. If I and J are non-empty, show that $\left(\bigcap_{\alpha \in I} A_\alpha\right) \cap \left(\bigcap_{\alpha \in J} A_\alpha\right) = \bigcap_{\alpha \in I \cup J} A_\alpha$.

Attempt. Let $B = \left(\bigcup_{\alpha \in I} A_\alpha\right) \cup \left(\bigcup_{\alpha \in J} A_\alpha\right)$, and let $C = \bigcup_{\alpha \in I \cup J} A_\alpha$. To show $B = C$, we want to show that $B \subseteq C$ and $C \subseteq B$.

1. ($\Rightarrow$) Let $y \in B$. By (3.2), $y \in A_\alpha$ for some $\alpha \in I$ or $y \in A_\alpha$ for some $\alpha \in J$. Hence. $y \in A_\alpha$ for some $\alpha \in I$ or $\alpha \in J$. We conclude $y \in C$.

2. ($\Leftarrow$) Let $y \in C$. By (3.2), $y \in A_\alpha$ for some $\alpha \in I$ or $\alpha \in J$. Hence, $y \in A_\alpha$ for some $\alpha \in I$ or $y \in A_\alpha$ for some $\alpha \in J$. We conclude $y \in B$.

Now let $B = \left(\bigcap_{\alpha \in I} A_\alpha\right) \cap \left(\bigcap_{\alpha \in J} A_\alpha\right)$, and let $C = \bigcap_{\alpha \in I \cup J} A_\alpha$. To show $B = C$, we want to show that $B \subseteq C$ and $C \subseteq B$.

1. ($\Rightarrow$) Let $y \in B$. By (3.3), $y \in A_\alpha$ for every $\alpha \in I$ and $y \in A_\alpha$ for every $\alpha \in J$. Hence, $y \in A_\alpha$ for every $\alpha \in I$ or $\alpha \in J$. We conclude $y \in C$.

2. ($\Leftarrow$) Let $y \in C$. By (3.3), $y \in A_\alpha$ for every $\alpha \in I$ or $\alpha \in J$. Hence, $y \in A_\alpha$ for every $\alpha \in I$ and $y \in A_\alpha$ for every $\alpha \in J$. We conclude $y \in B$.

□

Exercise 3.4.11 Let X be a set, let I be a non-empty set, and for all $\alpha \in I$ let A_α be a subset of X. Show that

$$X \setminus \bigcup_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I} (X \setminus A_\alpha)$$

and

$$X \setminus \bigcap_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} (X \setminus A_\alpha).$$

This should be compared with De Morgan's laws in Proposition 3.1.27 (although one cannot derive the above identities directly from De Morgan's laws, as I could be infinite).

Attempt. We aim to show $y \in X \setminus \bigcup_{\alpha \in I} A_\alpha \iff y \in \bigcap_{\alpha \in I} (X \setminus A_\alpha)$.

$$\begin{aligned}
y \in X \setminus \bigcup_{\alpha \in I} A_\alpha &\iff y \in X \text{ and } y \notin \bigcup_{\alpha \in I} A_\alpha && \text{(def. 3.1.26 difference sets)}\\
&\iff y \in X \text{ and } \neg(y \in \bigcup_{\alpha \in I} A_\alpha)\\
&\iff y \in X \text{ and } \neg(\exists \alpha \in I, y \in A_\alpha) && \text{(equation 3.2)}\\
&\iff y \in X \text{ and } (\forall \alpha \in I, y \notin A_\alpha) && \text{(De Morgan's law)}\\
&\iff \forall \alpha \in I, y \in X \text{ and } y \notin A_\alpha && \text{(logical-and is associative)}\\
&\iff \forall \alpha \in I, y \in X \setminus A_\alpha && \text{(def. 3.1.26 difference sets)}\\
&\iff y \in \bigcap_{\alpha \in I} (X \setminus A_\alpha) && \text{(equation 3.4)}
\end{aligned}$$

□

Now we aim to show $y \in X \setminus \bigcap_{\alpha \in I} A_\alpha \iff y \in \bigcup_{\alpha \in I} (X \setminus A_\alpha)$.

$$\begin{aligned}
y \in X \setminus \bigcap_{\alpha \in I} A_\alpha &\iff y \in X \text{ and } y \notin \bigcap_{\alpha \in I} A_\alpha && \text{(def. 3.1.26 difference sets)}\\
&\iff y \in X \text{ and } \neg(y \in \bigcap_{\alpha \in I} A_\alpha)\\
&\iff y \in X \text{ and } \neg(\forall \alpha \in I, y \in A_\alpha) && \text{(equation 3.4)}\\
&\iff y \in X \text{ and } (\exists \alpha \in I, y \notin A_\alpha) && \text{(De Morgan's law)}\\
&\iff \exists \alpha \in I, y \in X \text{ and } y \notin A_\alpha\\
&\iff \exists \alpha \in I, y \in X \setminus A_\alpha && \text{(def. 3.1.26 difference sets)}\\
&\iff y \in \bigcup_{\alpha \in I} (X \setminus A_\alpha) && \text{(equation 3.2)}
\end{aligned}$$

□

Remark. We cannot use (standard) induction in the proof because the set involved can be uncountably infinite, and, more crucially, may not be well-ordered, which is a necessary condition for the application of (transfinite) induction. Yet, demonstrably logic and a few set operations can still apply and save the day!

3.5 Cartesian Products

Definition 3.5.1 (Ordered pair) If x and y are any objects (possibly equal), we define the *ordered pair* (x, y) to be a new object, consisting of x as its first component and y as its second component. Two ordered pairs (x, y) and (x', y') are considered equal if and only if both their components match, i.e.,

$$(x, y) = (x', y') \iff (x = x' \text{ and } y = y'). \tag{3.5}$$

Definition 3.5.4 (Cartesian product) If X and Y are sets, then we define the Cartesian product $X \times Y$ to be the collection of ordered pairs, whose first component lies in X and second component lies in Y, thus

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

or equivalently

$$a \in (X \times Y) \iff (a = (x, y) \text{ for some } x \in X \text{ and } y \in Y).$$

One can show that the Cartesian product $X \times Y$ is in fact a set.

Definition 3.5.6 (Ordered n-tuple and n-fold Cartesian product) Let n be a natural number. An *ordered n-tuple* $(x_i)_{1 \leq i \leq n}$ (also denoted $(x_1, \dots, x_n)$) is a collection of objects x_i, one for every natural number i between 1 and n; we refer to x_i as the i^{th} *component* of the ordered n-tuple. Two ordered n-tuples $(x_i)_{1 \leq i \leq n}$ and $(y_i)_{1 \leq i \leq n}$ are said to be equal iff $x_i = y_i$ for all $1 \leq i \leq n$. If $(X_i)_{1 \leq i \leq n}$ is an ordered n-tuple of sets, we define their *Cartesian product* $\prod_{1 \leq i \leq n} X_i$ (also denoted $\prod_{i=1}^n X_i$ or $X_1 \times \ldots \times X_n$) by

$$\prod_{1 \leq i \leq n} X_i := \{(x_i)_{1 \leq i \leq n} : x_i \in X_i \text{ for all } 1 \leq i \leq n\}.$$

If x is an object, then (x) is a 1-tuple, which we shall identify with x itself (even though the two are, strictly speaking, not the same object).

The *empty Cartesian product* $\prod_{1 \leq i \leq 0} X_i$ gives, not the empty set $\{\}$, but rather the singleon set $\{()\}$ whose only element is the *0-tuple* $()$, also known as the *empty tuple.*

If n is a natural number, we often write X^n as shorthand for the n-fold Cartesian product $X^n := \prod_{1 \leq i \leq n} X$. Thus X^1 is essentially the same set as X (if we ignore the distinction between an object x and the 1-tuple (x)), while X^2 is essentially the Cartesian product $X \times X$. The set X^0 is a singleton set $()$.

Lemma 3.5.11 (Finite choice) *Let $n \geq 1$ be a natural number, and for each natural number $1 \leq i \leq n$, let X_i be a non-empty set. Then there exists an n-tuple $(x_i)_{1 \leq i \leq n}$ such that $x_i \in X_i$ for all $1 \leq i \leq n$. In other words, if each X_i is non-empty, then the set $\prod_{1 \leq i \leq n} X_i$ is also non-empty.*

— Exercises —

Exercise 3.5.1

(i) Suppose we *define* the ordered pair (x, y) for any objects x and y by the formula $(x, y) := \{\{x\}, \{x, y\}\}$ (thus using several applications of Axiom 3.4). Thus for instance $(1, 2)$ is the set $\{\{1\}, \{1, 2\}\}$, $(2, 1)$ is the set $\{\{2\}, \{2, 1\}\}$, and $(1, 1)$ is the set $\{\{1\}\}$. Show that such a definition (known as the *Kuratowski definition* of an ordered pair) indeed obeys the property (3.5).

(ii) Suppose we instead define an ordered pair using the alternate definition $(x, y) := \{x, \{x, y\}\}$. Show that this definition (known as the *short definition* of an ordered pair) also verifies (3.5) and is thus also an acceptable definition of ordered pair. (Warning: this is tricky; one needs the axiom 3.10 of regularity, and in particular Exercise 3.2.2.)

(iii) Show that regardless of the definition of ordered pair, the Cartesian product $X \times Y$ of any two sets X, Y is again a set. (Hint: first use the axiom of replacement to show that for any $x \in X$, that $\{(x, y) : y \in Y\}$ is a set, and then apply the axiom of union.)

Attempt.

(i) We want to show that $((x, y) = (x', y')) \implies (x = x' \text{ and } y = y')$, and conversely $(x = x' \text{ and } y = y') \implies ((x, y) = (x', y'))$.

(a) ($\Rightarrow$) By the Kuratowski definition, $(x, y) = (x', y')$ iff $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$. The two sets are equal if either (1) $\{x\} = \{x'\}$ and $\{x, y\} = \{x', y'\}$, or (2) $\{x\} = \{x', y'\}$ and $\{x, y\} = \{x'\}$. (2) is possible only if $x = y = x' = y'$. In that case, we have ($x = x'$ and $y = y'$) vacuously. For (1), $\{x\} = \{x'\}$ implies $x = x'$. Then $\{x, y\} = \{x', y'\}$ iff $\{x, y\} = \{x, y'\}$. This implies either $y = y'$, or ($x = y'$ and $y = x$). Either way, we have ($x = x'$ and $y = y'$), as desired.

(b) ($\Leftarrow$) If ($x = x'$ and $y = y'$), then clearly, by the Kuratowski definition, the two corresponding sets of (x, y) and (x', y'), are equal. Thus the reverse implication holds.

□

(ii) We want to show that $((x, y) = (x', y')) \implies (x = x'$ and $y = y')$, and conversely ($x = x'$ and $y = y'$) $\implies ((x, y) = (x', y'))$.

(a) ($\Rightarrow$) By the short definition of an ordered pair, $((x, y) = (x', y'))$ iff $(\{x, \{x, y\}\} = \{x', \{x', y'\}\})$. The two sets are equal if either (1) $x = x'$ and $\{x, y\} = \{x', y'\}$, or (2) $x = \{x', y'\}$ and $\{x, y\} = x'$. For (2), $x' \in x$ and $x \in x'$, but this violates axiom 3.10 of regularity (per Exercise 3.2.2). Therefore, case (2) is impossible. The only remaining possibility is case (1), which implies either $y = y'$, or ($x = y'$ and $x = y$). Either way, we have ($x = x'$ and $y = y'$), as desired.

(b) ($\Leftarrow$) If $x = x'$ and $y = y'$, then $\{x, \{x, y\}\} = \{x', \{x', y'\}\}$. By the short definition of an ordered pair, we have $(x, y) = (x', y')$.

□

(iii) We want to show that the Cartesian product $X \times Y$ of any two sets X, Y is a set. Let $x \in X$, we have exactly one (x, y) for every $y \in Y$. Therefore, by axiom 3.7 of replacement, the set $S_x = \{(x, y) : y \in Y\}$ exists. Also we have exactly one S_x for every $x \in X$. Thus the set $\{S_x : x \in X\}$ exists, and is equal to $A = \{\{(x, y) : y \in Y\} : x \in X\}$. By axiom 3.12 of union, we have $\bigcup A = \{(x, y) : x \in X, y \in Y\}$. By definition 3.5.6, $X \times Y = \{(x, y) : x \in X, y \in Y\}$. Thus, we conclude the Cartesian product of any two sets X, Y is a set. □

Exercise 3.5.2 Suppose we define an ordered n-tuple to be a surjective function

$$x : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to X$$

whose codomain is some arbitrary set X (so different ordered n-tuples are allowed to have different ranges); we then write x_i for $x(i)$ and also write x as $(x_i)_{1 \leq i \leq n}$. Using this definition, verify that we have $(x_i)_{1 \leq i \leq n} = (y_i)_{1 \leq i \leq n}$ if and only if $x_i = y_i$ for all $1 \leq i \leq n$. Also, show that if $(X_i)_{1 \leq i \leq n}$ are an ordered n-tuple of sets, then the Cartesian product, as defined in Definition 3.5.6, is indeed a set. (Hint: use Exercise 3.4.7 and the axiom of specification.)

Attempt. By definition $(x_i)_{1 \leq i \leq n}$ is a surjective function $x : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to X$. Similarly, $(y_i)_{1 \leq i \leq n}$ is a surjective function $y : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to X$. We aim to verify that $(x_i)_{1 \leq i \leq n} = (y_i)_{1 \leq i \leq n}$ implies ($x_i = y_i$ for all $1 \leq i \leq n$), and, conversely, ($x_i = y_i$ for all $1 \leq i \leq n$) implies $(x_i)_{1 \leq i \leq n} = (y_i)_{1 \leq i \leq n}$.

1. ($\Rightarrow$) Assume $(x_i)_{1 \leq i \leq n} = (y_i)_{1 \leq i \leq n}$. By definition, the two functions x and y are equal. By definition 3.3.8 of equality of functions, their domain and codomain must agree. Furthermore, $x(i) = y(i)$ for all $i \in \{i \in \boldsymbol{N} : 1 \leq i \leq n\}$. Therefore, $x_i = y_i$ for all $1 \leq i \leq n$.

2. ($\Leftarrow$) Assume $x_i = y_i$ for all $1 \leq i \leq n$. So $x(i) = y(i)$ for all $i \in \{i \in \boldsymbol{N} : 1 \leq i \leq n\}$, which means the images of both functions are equal. Since both functions are surjective with equal images, their codomains are equal. Also, their domains are clearly identical. We conclude the two functions satisfy the definition 3.3.8 of equality of functions, and are therefore equal. It follows $(x_i)_{1 \leq i \leq n} = (y_i)_{1 \leq i \leq n}$.

□

Also, we aim to show that if $(X_i)_{1\leq i\leq n}$ are an ordered n-tuple of sets, then the Cartesian product, as defined in Definition 3.5.6, is a set. If $(X_i)_{1\leq i\leq n}$ are an ordered n-tuple of sets, then by the above definition each such tuple is a surjective function

$$x : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to Y$$

whose codomain Y is some arbitrary set of sets, i.e., $Y = \{X_i : 1 \leq i \leq n\}$. (Note that two set elements $X_i, X_j \in Y$ with $i \neq j$ may not be distinct unless the function is injective.) The Cartesian product, as defined in Definition 3.5.6, is

$$\prod_{1\leq i\leq n} X_i := \{(x_i)_{1\leq i\leq n} : x_i \in X_i \text{ for all } 1 \leq i \leq n\}.$$

We thus interpret the Cartesian product (of sets) as a set of all possible functions from the domain $\{i \in \boldsymbol{N} : 1 \leq i \leq n\}$ to the elements of the respective set elements of $Y = \{X_i : 1 \leq i \leq n\}$. The aim is to show that $\prod_{1\leq i\leq n} X_i$ exists.

Let $I = \{i \in \boldsymbol{N} : 1 \leq i \leq n\}$. By axiom 3.12 of union, there exists a set $A = \bigcup Y$, which contains the union of all the sets of Y. By axiom 3.11 of power set, there exists a set $\Omega = A^I$ that contains all the functions from I to A, which is a union of all the sets of Y, namely,

$$\begin{aligned}\Omega &= \{x \mid x : I \to A\}\\ &= \{x \mid x : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to \bigcup\{X_i : 1 \leq i \leq n\}\}\end{aligned}$$

By axiom 3.6 of specification, there exists a set $Q \subseteq \Omega$, namely

$$\begin{aligned}Q &= \{x \mid x : I \to \bigcup\{X_i : 1 \leq i \leq n\} \text{ such that } x(i) \in X_i \text{ for all } 1 \leq i \leq n\}\\ &= \{x \mid (x_i)_{1\leq i\leq n} : x_i \in X_i \text{ for all } 1 \leq i \leq n\}\\ &= \prod_{1\leq i\leq n} X_i.\end{aligned}$$

We conclude that if $(X_i)_{1\leq i\leq n}$ are an ordered n-tuple of sets, then the Cartesian product, as defined in Definition 3.5.6, is a set. □

Remarks. One of the crucial steps in this exercise is how an ordered n-tuple of sets is defined or properly interpreted from the perspective of defining an ordered n-tuple as a surjective function. Obvious in hindsight, but gave me a headache at first! The other crucial step, of course, is a union of all the sets, and then formulate a set of all functions via power set. So crude, yet so ingenious and simple! A form of bruce-forcing taken to the extreme.

Exercise 3.5.3 Show that the definitions of equality for ordered pair and ordered n-tuple are consistent with the reflexivity, symmetry, and transitivity axioms, in the sense that if these axioms are assumed to hold for the individual components x, y of an ordered pair (x, y), then they hold for the ordered pair itself.

Attempt. Suppose we have three n-ordered tuples of any objects for $n \in \boldsymbol{N}$ and $n > 0$, namely, $(x_i)_{1\leq i\leq n}$, $(y_i)_{1\leq i\leq n}$ and $(z_i)_{1\leq i\leq n}$.

1. (reflexivity) Since $x_i = x_i$ for all $1 \leq i \leq n$, we have $(x_i)_{1\leq i\leq n} = (x_i)_{1\leq i\leq n}$.
2. (symmetry) Since $(x_i = y_i \implies y_i = x_i)$ for all $1 \leq i \leq n$, we have $(x_i)_{1\leq i\leq n} = (y_i)_{1\leq i\leq n} \implies (y_i)_{1\leq i\leq n} = (x_i)_{1\leq i\leq n}$.
3. (transitivity) Since $(x_i = y_i \text{ and } y_i = z_i) \implies x_i = z_i$ for all $1 \leq i \leq n$, we have $((x_i)_{1\leq i\leq n} = (y_i)_{1\leq i\leq n} \text{ and } (y_i)_{1\leq i\leq n} = (z_i)_{1\leq i\leq n}) \implies (x_i)_{1\leq i\leq n} = (z_i)_{1\leq i\leq n}$.

Exercise 3.5.4 Let A, B, C be sets. Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$, that $A \times (B \cap C) = (A \times B) \cap (A \times C)$, and that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$. (One can of course prove similar identities in which the roles of the left and right factors of the Cartesian product are reversed.)

Attempt.

1. We aim to show $A \times (B \cup C) = (A \times B) \cup (A \times C)$. By definition 3.5.1, for every ordered pair (x_1, x_2),

$$\begin{aligned}
& (x_1, x_2) \in A \times (B \cup C) && \\
\iff & x_1 \in A \wedge (x_2 \in B \cup C) && \text{(def. 3.5.4 of Cartesian product)} \\
\iff & x_1 \in A \wedge (x_2 \in B \vee x_2 \in C) && \text{(axiom 3.5 pairwise union)} \\
\iff & (x_1 \in A \wedge x_2 \in B) \vee (x_1 \in A \wedge x_2 \in C) && \text{(distribute logical-and over logical-or)} \\
\iff & (x_1, x_2) \in (A \times B) \cup (A \times C) && \text{(def. 3.5.4 of Cartesian product)}
\end{aligned}$$

Therefore, $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

2. We aim to show $A \times (B \cap C) = (A \times B) \cap (A \times C)$. By definition 3.5.1, for every ordered pair (x_1, x_2),

$$\begin{aligned}
& (x_1, x_2) \in A \times (B \cap C) && \\
\iff & x_1 \in A \wedge x_2 \in B \cap C && \text{(def. 3.5.4 of Cartesian product)} \\
\iff & x_1 \in A \wedge (x_2 \in B \wedge x_2 \in C) && \text{(def. 3.1.22 intersections)} \\
\iff & (x_1 \in A \wedge x_2 \in B) \wedge (x_1 \in A \wedge x_2 \in C) && \\
\iff & (x_1, x_2) \in (A \times B) \cap (A \times C) && \text{(def. 3.5.4 of Cartesian product)}
\end{aligned}$$

Therefore, $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

3. We aim to show $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$. We start from the right-hand side. By definition 3.5.1, for every ordered pair (x_1, x_2),

$$\begin{aligned}
& (x_1, x_2) \in (A \times B) \setminus (A \times C) && \\
\iff & x_1 \in A \wedge x_2 \in B \wedge \neg(x_1 \in A \wedge x_2 \in C) && \\
\iff & x_1 \in A \wedge x_2 \in B \wedge (x_1 \notin A \vee x_2 \notin C) && \text{(De Morgan's law)} \\
\iff & (x_1 \in A \wedge x_2 \in B \wedge x_1 \notin A) \vee (x_1 \in A \wedge x_2 \in B \wedge x_2 \notin C) && \text{(distribute } \wedge \text{ over } \vee\text{)} \\
\iff & x_1 \in A \wedge x_2 \in B \wedge x_2 \notin C && \text{(contradiction)} \\
\iff & (x_1, x_2) \in A \times (B \setminus C) &&
\end{aligned}$$

Therefore, $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

□

Exercise 3.5.5 Let A, B, C, D be sets. Show that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$. Is it true that $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$? Is it true that $(A \times B) \setminus (C \times D) = (A \setminus C) \times (B \setminus D)$?

Attempt.

1. We aim to show that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$. By definition 3.5.1, for every ordered pair (x_1, x_2),

$$\begin{aligned}
& (x_1, x_2) \in (A \times B) \cap (C \times D) && \\
\iff & (x_1, x_2) \in (A \times B) \wedge (x_1, x_2) \in (C \times D) && \text{(def. 3.1.22 intersections)} \\
\iff & (x_1 \in A \wedge x_2 \in B) \wedge (x_1 \in C \wedge x_2 \in D) && \text{(def. 3.5.4 of Cartesian product)} \\
\iff & (x_1 \in A \wedge x_1 \in C) \wedge (x_2 \in B \wedge x_2 \in D) && \text{(commutativity of logical-and)} \\
\iff & (x_1 \in A \cap C) \wedge (x_2 \in B \cap D) && \text{(def. 3.1.22 intersections)} \\
\iff & (x_1, x_2) \in (A \cap C) \times (B \cap D) && \text{(def. 3.5.4 of Cartesian product)}
\end{aligned}$$

Therefore, we conclude that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$. □

2. We aim to show $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$ is false by counter-example. Let $A = \{a\}, B = \emptyset, C = \emptyset, D = \{d\}$. So $(A \times B) \cup (C \times D) = \emptyset$, but $(A \cup C) \times (B \cup D) = \{(a, d)\}$. Hence $(A \times B) \cup (C \times D) \neq (A \cup C) \times (B \cup D)$. □

3. We aim to show $(A \times B) \setminus (C \times D) = (A \setminus C) \times (B \setminus D)$ is false by counter-example. Let $A = \{a\}, B = \{b\}, C = A, D = \emptyset$. So $(A \times B) \setminus (C \times D) = \{(a, b)\}$, but $(A \setminus C) \times (B \setminus D) = \emptyset$. Hence $(A \times B) \setminus (C \times D) \neq (A \setminus C) \times (B \setminus D)$. □

Exercise 3.5.6 Let A, B, C, D be non-empty sets. Show that $A \times B \subseteq C \times D$ if and only if $A \subseteq C$ and $B \subseteq D$, and that $A \times B = C \times D$ if and only if $A = C$ and $B = D$. What happens if some or all of the hypothesis that the sets A, B, C, D are non-empty are removed?

Attempt. We aim to show $A \times B \subseteq C \times D$ if and only if $A \subseteq C$ and $B \subseteq D$. (3.5.6a)

1. ($\Rightarrow$) Suppose $A \times B \subseteq C \times D$. Since B is non-empty, let $b \in B$ be arbitrary. For every $x_1 \in A$, $(x_1, b) \in A \times B$ implies $(x_1, b) \in C \times D$, which in turn implies $x_1 \in C$. Therefore $A \subseteq C$. Similarly, since A is non-empty, let $a \in A$ be arbitrary, and argue likewise to show $B \subseteq D$. We conclude that $A \times B \subseteq C \times D$ implies ($A \subseteq C$ and $B \subseteq D$).

   Let P be the statement $A \times B \subseteq C \times D \implies (A \subseteq C$ and $B \subseteq D)$. We now consider what happens to P if some or all of the sets A, B, C, D are empty.

   (a) If both A and B are empty, P is true vacuously.

   (b) If, however, A is empty but not B, then even though both $A \times B \subseteq C \times D$ and $A \subseteq C$ hold vacuously, $B \subseteq D$ is false. Thus P is false. Similarly, if B is empty but not A, then P is false.

   (c) If C or D is empty (or both), then either A or B must be empty.

      i. If A is empty (but not B), then $B \subseteq D$ is false, so P is false.

      ii. If B is empty (but not A), then $A \subseteq C$ is false, so P is false.

   In summary, if some or all of the sets A, B, C, D are empty, P is vacuously true if and only if both A and B are empty.

2. ($\Leftarrow$) Suppose $A \subseteq C$ and $B \subseteq D$. It follows that every $x_1 \in A$ implies $x_1 \in C$, and every $x_2 \in B$ implies $x_2 \in D$. Hence, $(x_1, x_2) \in A \times B \implies (x_1, x_2) \in C \times D$. We conclude that ($A \subseteq C$ and $B \subseteq D$) implies $A \times B \subseteq C \times D$.

   Let Q be the statement ($A \subseteq C$ and $B \subseteq D$) $\implies A \times B \subseteq C \times D$. We now consider what happens to Q if some or all of the sets A, B, C, D are empty.

   (a) If A or B is empty, then $A \times B = \emptyset$, so Q is vacuously true.

   (b) If C is empty, then A must be empty. Likewise, if D is empty, then B must be empty. In both cases, Q is vacuously true for the same reasons as in (a).

   In summary, Q always holds vacuously if some or all of the sets A, B, C, D are empty.

We conclude that if some or all of the sets A, B, C, D are empty, the statement ($A \times B \subseteq C \times D$ if and only if $A \subseteq C$ and $B \subseteq D$) holds vacuously if and only if both A and B are empty. (3.5.6b)
□

Moving on, we now proceed to show $A \times B = C \times D$ if and only if $A = C$ and $B = D$. Given A, B, C, D are non-empty sets, this pretty much follows from the previous proposition:

$$\begin{aligned}
& A \times B = C \times D \\
\iff & (A \times B \subseteq C \times D) \wedge (C \times D \subseteq A \times B) && \text{(axiom 3.2)} \\
\iff & (A \subseteq C \wedge B \subseteq D) \wedge (C \subseteq A \wedge D \subseteq B) && \text{(3.5.6a)} \\
\iff & (A \subseteq C \wedge C \subseteq A) \wedge (B \subseteq D \wedge D \subseteq B) && (\wedge \text{ is commutative}) \\
\iff & A = C \wedge B = D && \text{(axiom 3.2)}
\end{aligned}$$

Observe that the statement ($A \times B = C \times D$ if and only if $A = C$ and $B = D$) is equivalent to the conjunction of the following two statements:

1. ($A \times B \subseteq C \times D$ if and only if $A \subseteq C$ and $B \subseteq D$)

2. ($A \times B \supseteq C \times D$ if and only if $A \supseteq C$ and $B \supseteq D$)

Therefore, by applying the analysis of 3.5.6b to both statements, we conclude that if some or all of the sets A, B, C, D are empty, the statement ($A \times B = C \times D$ if and only if $A = C$ and $B = D$) holds vacuously if and only if all A, B, C, D are all empty. □

Remarks.

1. One trick that I learned from this exercise is how to leverage on the given fact that the sets are non-empty. Namely, fix an arbitrary object from one set, and then reason about the associated cartesian product in a much simpler fashion.

2. Initially I tried converting subset statements into implications, and then into combinations of negation, conjunction, and disjunction. While this approach worked to some extent, it quickly became complicated without much benefit. Reasoning directly with the implications turned out to be cleaner for this exercise.

Exercise 3.5.7 Let X, Y be sets, and let $\pi_{X\times Y\to X} : X \times Y \to X$ and $\pi_{X\times Y\to Y} : X \times Y \to Y$ be the maps $\pi_{X\times Y\to X}(x, y) := x$ and $\pi_{X\times Y\to Y}(x, y) := y$; these maps are known as the *co-ordinate functions* on $X \times Y$. Show that for any functions $f : Z \to X$ and $g : Z \to Y$, there exists a unique function $h : Z \to X \times Y$ such that $\pi_{X\times Y\to X} \circ h = f$ and $\pi_{X\times Y\to Y} \circ h = g$. (Compare this to the last part of Exercise 3.3.8, and to Exercise 3.1.7.) This function h is known as the *pairing* of f and g and is denoted $h = (f, g)$.

Attempt. We aim to show that the function h exists and is unique. Given sets X, Y, as shown in 3.5.1(iii), the Cartesian product X×Y is also a set. Let $f : Z \to X$ and $g : Z \to Y$ be any two functions. By definition 3.3.1 of functions, we can define a function $i : Z \to X \times Y$ such that, for every $z \in Z$,

$$i(z) = (f(z), g(z)).$$

Since $\pi_{X\times Y\to X} \circ i(z) = f(z)$ for every $z \in Z$, and their domain and codomain agree, by definition 3.3.8 equality of functions, $\pi_{X\times Y\to X} \circ i$ is equal to f. Similarly, since $\pi_{X\times Y\to Y} \circ i(z) = g(z)$ for every $z \in Z$, and their domain and codomain agree, $\pi_{X\times Y\to Y} \circ i$ is equal to g. Since function i satisfies the definition of h, we conclude that the function h exists.

Assume, for contradiction, that $i \neq h$. Then there exists $z \in Z$ such that $i(z) \neq h(z)$. Let $i(z) = (f(z), g(z))$, and let $h(z) = (x, y)$. So either $f(z) \neq x$ or $g(z) \neq y$. But this is impossible. So the assumption is false, and the two functions i and h must be equal. We conclude that there exists a unique function $h : Z \to X \times Y$ such that $\pi_{X\times Y\to X} \circ h = f$ and $\pi_{X\times Y\to Y} \circ h = g$. □

Exercise 3.5.8 Let $X_1, \ldots, X_n$ be sets. Show that the Cartesian product $\prod_{i=1}^n X_i$ is empty if and only if at least one of the X_i is empty.

Attempt.

1. ($\Rightarrow$) We aim to show $\prod_{i=1}^n X_i = \emptyset$ implies at least one of the X_i is empty by contrapositive. Suppose none of the X_i is empty. Then there exists at least one element in their Cartesian product, so $\prod_{i=1}^n X_i$ is non-empty. Hence the forward implication holds.

2. ($\Leftarrow$) We aim to show if at least one of the X_i is empty, then $\prod_{i=1}^n X_i$ is empty by contrapositive. Suppose $\prod_{i=1}^n X_i$ is non-empty. Then there exists $(x_1, \ldots, x_n) \in \prod_{i=1}^n X_i$ with $x_1 \in X_1, \ldots, x_n \in X_n$, so none of the X_i is empty. Hence the reverse implication holds.

□

Exercise 3.5.9 Suppose that I and J are two sets, and for all $\alpha \in I$ let A_α be a set, and for all $\beta \in J$ let B_β be a set. Show that $(\bigcup_{\alpha\in I} A_\alpha) \cap (\bigcup_{\beta\in J} B_\beta) = \bigcup_{(\alpha,\beta)\in I\times J}(A_\alpha \cap B_\beta)$. What happens if one interchanges all the union and intersection symbols here?

Attempt. By definition 3.2 of union, for any object y, let P be the statement $(y \in (\bigcup_{\alpha\in I} A_\alpha) \cap (\bigcup_{\beta\in J} B_\beta))$, which holds iff $y \in A_\alpha$ for some $\alpha \in I$, and $y \in B_\beta$ for some $\beta \in J$. By definition 3.5.4 of Cartesian product, $((\alpha, \beta)$ for some $\alpha \in I$ and $\beta \in J)$ iff $(\alpha, \beta) \in I \times J$. Therefore, P holds iff $y \in A_\alpha$ and $y \in B_\beta$ for some $(\alpha, \beta) \in I \times J$. It follows that $P \iff y \in \bigcup_{(\alpha,\beta)\in I\times J}(A_\alpha \cap B_\beta)$. We conclude $(\bigcup_{\alpha\in I} A_\alpha) \cap (\bigcup_{\beta\in J} B_\beta) = \bigcup_{(\alpha,\beta)\in I\times J}(A_\alpha \cap B_\beta)$. □

Interchanging all the union and intersection symbols, we aim to check if

$$(\bigcap_{\alpha\in I} A_\alpha) \cup (\bigcap_{\beta\in J} B_\beta) = \bigcap_{(\alpha,\beta)\in I\times J} (A_\alpha \cup B_\beta).$$

Note that by definition 3.3 of intersection, both the index sets I, J must be non-empty; otherwise, the expressions become nonsensical. (See remarks below for more details.)

Let y be any object. Let

$$P := y \in (\bigcap_{\alpha\in I} A_\alpha) \cup (\bigcap_{\beta\in J} B_\beta)$$

which holds iff ($y \in A_\alpha$ for all $\alpha \in I$, or $y \in B_\beta$ for all $\beta \in J$). Let

$$Q := y \in \bigcap_{(\alpha,\beta)\in I\times J} (A_\alpha \cup B_\beta)$$

which holds iff ($y \in A_\alpha$ or $y \in B_\beta$ for all $(\alpha, \beta) \in I \times J$).

1. ($\Rightarrow$) Since $J \neq \emptyset$, ($y \in A_\alpha$ for all $\alpha \in I$) implies ($y \in A_\alpha \cup B_\beta$ for all $(\alpha, \beta) \in I \times J$). Similarly, since $I \neq \emptyset$, ($y \in B_\beta$ for all $\beta \in J$) implies ($y \in B_\beta \cup A_\alpha$ for all $(\alpha, \beta) \in I \times J$). Therefore, $P \implies Q$.
2. ($\Leftarrow$) We aim to show that $Q \implies P$ by contrapositive. Suppose P is false. Let $y \notin A_i$ for a specific $i \in I$, and $y \notin B_j$ for a specific $j \in J$. So $y \notin A_i \cup B_j$. Since $(i, j) \in I \times J$, it follows that Q is false, i.e., $y \notin \bigcap_{(\alpha,\beta)\in I\times J}(A_\alpha \cup B_\beta)$. Therefore, $Q \implies P$.

We conclude that $(\bigcap_{\alpha\in I} A_\alpha) \cup (\bigcap_{\beta\in J} B_\beta) = \bigcap_{(\alpha,\beta)\in I\times J}(A_\alpha \cup B_\beta)$. □

Remarks.

1. This exercise uncovers a subtle difference between the definition of

   (a) $\bigcup_{\alpha\in I} A_\alpha := \bigcup\{A_\alpha : \alpha \in I\}$, a union of families of sets, and

   (b) $\bigcap_{\alpha\in I} A_\alpha := \{x \in A_\beta : x \in A_\alpha \text{ for all } \alpha \in I\}$, an intersection of families of sets

   when the index set I is empty.

   For (1), the property $\alpha \in \emptyset \iff$ (for some $\alpha \in \emptyset$) is always false, and therefore $\{A_\alpha : \alpha \in \emptyset\} = \emptyset$, and hence $\bigcup_{\alpha\in\emptyset} A_\alpha = \emptyset$.

   For (2), the property ($x \in A_\alpha$ for all $\alpha \in \emptyset$) is vacuously true, but $x \in A_\beta$ is undefined since β is also undefined. Another way to see this is that $\{x \in A_\beta : x \in A_\alpha \text{ for all } \alpha \in \emptyset\} = \{x \in A_\beta : \text{ true}\} = \{x \in A_\beta\}$, where β is clearly undefined. So the expression becomes nonsensical. In other words, inherently the definition requires $I \neq \emptyset$.

2. The second part is more challenging, after interchanging all the union and intersection symbols. In particular, the reverse implication was not immediate obvious. After failing to find a counter example, the crucial step turned out to be proving the contrapositive while focusing on a specific (negative) case.

Exercise 3.5.10 If $f : X \to Y$ is a function, define the *graph* of f to be the subset of $X \times Y$ defined by $\{(x, f(x)) : x \in X\}$.

(i) Show that two functions $f : X \to Y, \tilde{f} : X \to Y$ are equal if and only if they have the same graph.

(ii) Conversely, if G is any subset of $X \times Y$ with the property that for each $x \in X$, the set $\{y \in Y : (x, y) \in G\}$ has exactly one element (or in other words, G obeys the *vertical line test*), show that there is exactly one function $f : X \to Y$ whose graph is equal to G.

(iii) Suppose we define a function f to be an ordered triple $f = (X, Y, G)$, where X, Y are sets, and G is a subset of $X \times Y$ that obeys the vertical line test. We then *define* the domain of such a triple to be X, the codomain to be Y and for every $x \in X$, we define $f(x)$ to be the unique $y \in Y$ such that $(x, y) \in G$. Show that this definition is compatible with Definition 3.3.1 in the sense that every choice of domain X, codomain Y, and property $P(x, y)$ obeying the vertical line test produces a function as defined here that obeys all the properties required of it in that definition, and is also similarly compatible with Definition 3.3.8.

Attempt.

(i) If $f = \tilde{f}$, then $f(x) = \tilde{f}(x)$ for all $x \in X$. By axiom 3.2 of equality of sets, their graphs are equal. Conversely, suppose there exists $a \in X$ and $f(a) \neq \tilde{f}(a)$. Then their graphs differ, namely $(a, f(a)) \in \{(x, f(x) : x \in X)\}$, but $(a, f(a)) \notin \{(x, \tilde{f}(x) : x \in X)\}$. Hence by contrapositive the reverse implication holds. □

(ii) Let $f : X \to Y$ be a function from domain X to codomain Y, such that $f(x) = y$ and $(x, y) \in G$. The assumption of G guarantees that such a y exists and is unique for every $x \in X$. By construction, the graph of f is equal to G. Therefore f exists.

Suppose we have another function $g : X \to Y$ whose graph is equal to G. For every $x \in X$, we have $(x, f(x)) \in G$, and $(x, g(x)) \in G$. Since G obeys the vertical line test, $(x, f(x)) = (x, g(x))$ for every $x \in X$, so $f = g$. Therefore, f is unique. □

(iii) We aim to show the ordered triple $f = (X, Y, G)$ is compatible with Definition 3.3.1 of a function.

Let X, Y be any sets, and let G be any subset of $X \times Y$ such that G obeys the vertical line test. Then let (X, Y, G) be an ordered triple.

By definition, the set X and Y of the ordered triple is, respectively, the domain and codomain of a function as defined in 3.3.1.

Let $P(x, y)$ be a property that is true iff $(x, y) \in G$ for some $x \in X$ and some $y \in Y$. Given G objeys the vertical line test, by (ii), there is exactly one function with domain X and codomain Y whose graph is equal to G. Namely, $f : X \to Y$ is the function defined by P on the domain X and domain Y to be an object which, given any input $x \in X$, assigns an output $f(x) \in Y$ for which $P(x, f(x))$ is true. Therefore the ordered triple (X, Y, G) is compatible with Definition 3.3.1.

Furthermore, let X', Y' be any sets, and let G' be any subset of $X' \times Y'$ such that G' obeys the vertical line test. Let g be the unique function with domain X' and codomain Y' whose graph is equal to G'.

By definition 3.5.6, two ordered triples (X, Y, G) and (X', Y', G') are equal if and only if $X = X'$, $Y = Y'$ and $G = G'$. By definition 3.3.8, the two functions $f : X \to Y, g : X' \to Y'$ are said to be equal if (and only if) their domains and codomains agree (i.e., $X = X'$ and $Y = Y'$), and furthermore that $f(x) = g(x)$ for all $x \in X$. But $f(x) = g(x)$ for all $x \in X$ is equivalent to $(x, f(x)) = (x, g(x))$ for all $x \in X$ (i.e., $G = G'$). Therefore the ordered triple is also compatible with Definition 3.3.8. □

Remarks. It seems definition 3.3.8 has a typo in that "if" should be "if and only if". Namely,

> Two functions $f : X \to Y, g : X' \to Y'$ are said to be equal **if and only if** their domains and codomains agree (i.e., $X = X'$ and $Y = Y'$), and furthermore that $f(x) = g(x)$ for all $x \in X$.

(Reported to Tao on May 13, 2025.)

Exercise 3.5.11 Show that Axiom 3.11 can in fact be deduced from Lemma 3.4.10 and the other axioms of set theory, and thus Lemma 3.4.10 can be used as an alternate formulation of the power set axiom. (*Hint*: for any two sets X and Y, use Lemma 3.4.10 and the axiom of specification to construct the set of all subsets of $X \times Y$ which obey the vertical line test. Then use Exercise 3.5.10 and the axiom of replacement.)

Attempt. Let X, Y be any two sets. By definition 3.5.4 of Cartesian product, there exists a set $X \times Y = \{(x, y) : x \in X, y \in Y\}$. By Lemma 3.4.10, there exists a set

$$\Omega_{X\times Y} = \{G : G \text{ is a subset of } X \times Y\}$$

that contains all the subsets of $X \times Y$. For each $G \in \Omega_{X\times Y}$, let $P(G)$ be the property:

$$\text{for each } x \in X, \text{ the set } \{y \in Y : (x, y) \in G\} \text{ has exactly one element.}$$

(i.e, G obeys the vertical line test). By axiom 3.6 of specification, there exists a set

$$\Omega_P = \{G \in \Omega_{X\times Y} : P(G)\}$$

whose elements are precisely those subsets of $X \times Y$ that obey the vertical line test. Let $f : X \to Y$ be any function with domain X and codomain Y. For each $G \in \Omega_P$, let $Q(G, f)$ be the statement:

$$f \text{ is a function with domain } X, \text{ codomain } Y, \text{ and graph equal to } G.$$

By exercise 3.5.10(ii), for each $G \in \Omega_P$, there exists exactly one function $f : X \to Y$ satisfying $Q(G, f)$. So by axiom 3.7 of replacement, there exists a set

$$Y^X = \{f : X \to Y \mid Q(G, f) \text{ is true for some } G \in \Omega_P\}.$$

Hence Y^X is a set of functions, each of which corresponds to a unique subset of $X \times Y$ that obey the vertical line test, and vice-versa. We conclude Y^X is the set of all the functions from domain X to codomain Y. Therefore Axiom 3.11 can be deduced from Lemma 3.4.10 and the other axioms of set theory, as required. □

Exercise 3.5.12 This exercise will establish a rigorous version of Proposition 2.1.16 that avoids circularity (in particular, avoiding the use of any object that required Proposition 2.1.16 to construct).

(i) Let X be a set, let $f : \boldsymbol{N} \times X \to X$ be a function, and let c be an element of X. Show that there exists a function $a : \boldsymbol{N} \to X$ such that

$$a(0) = c$$

and

$$a(n\text{++}) = f(n, a(n)) \text{ for all } n \in \boldsymbol{N},$$

and furthermore that this function is unique. (*Hint*: first show inductively, by a modification of the proof of Lemma 3.5.11, that for every natural number $N \in \boldsymbol{N}$, there exists a unique function $a_N : \{n \in \boldsymbol{N} : n \leq N\} \to X$ such that $a_N(0) = c$ and $a_N(n\text{++}) = f(n, a_N(n))$ for all $n \in \boldsymbol{N}$ such that $n < N$.)

(ii) (Warning: this is challenging.) Prove (i) without using any properties of the natural numbers other than the Peano axioms directly (in particular, without using the ordering of the natural numbers, and without appealing to Proposition 2.1.16). (*Hint*: first show inductively, using only the Peano axioms and basic set theory, that for every natural number $N \in \boldsymbol{N}$, there exists a unique pair A_N, B_N of subsets of $\boldsymbol{N}$ which obeys the following properties: (a) $A_N \cap B_N = \emptyset$, (b) $A_N \cup B_N = \boldsymbol{N}$, (c) $0 \in A_N$, (d) $N{+}{+} \in B_N$, (e) Whenever $n \in B_N$, we have $n{+}{+} \in B_N$. (f) Whenever $n \in A_N$ and $n \neq N$, we have $n{+}{+} \in A_N$. Once one obtains these sets, use A_N as a substitute for $\{n \in \boldsymbol{N} : n \leq N\}$ in the previous argument.)

Attempt. Let X be a set, let $f : \boldsymbol{N} \times X \to X$ be a function, and let c be an element of X. Let Q be the statement: there exists a unique function $a : \boldsymbol{N} \to X$ such that

$$a(0) = c$$

and

$$a(n{+}{+}) = f(n, a(n)) \text{ for all } n \in \boldsymbol{N}.$$

(i) We aim to prove Q by first proving another statement $P(N)$, which is defined as follows: for every natural number $N \in \boldsymbol{N}$, there exists a unique function $a_N : \{n \in \boldsymbol{N} : n \leq N\} \to X$ such that

$$a_N(0) = c$$

and

$$a_N(n{+}{+}) = f(n, a_N(n)) \text{ for all } n \in \boldsymbol{N} \text{ such that } n < N.$$

We induct on N, starting with the base case $P(0)$. Since zero is the only element in the domain of a_0, and by definition $a_0(0) = c$, a_0 is well defined. Let $b_0 : \{0\} \to X$ be another function satisfying the same conditions. Then $b_0(0) = c = a_0(0)$, so $b_0 = a_0$. Hence a_0 is unique, closing the base case.

Assume inductively that $P(N)$ is true. Let $a_{N{+}{+}} : \{n \in \boldsymbol{N} : n \leq N{+}{+}\} \to X$ be a function such that

$$a_{N{+}{+}}(n) = \begin{cases} a_N(n) & \text{if } n \leq N \\ f(N, a_N(N)) & \text{if } n = N{+}{+} \end{cases} \tag{1}$$

Since a_N is well defined and unique by the inductive hypothesis, $a_{N{+}{+}}$ is also well defined and unique.

For $n = 0$,

$$\begin{aligned} a_{N{+}{+}}(0) &= a_N(0) && \text{(definition (1))} \\ &= c && \text{(inductive hypothesis)} \end{aligned}$$

For $n < N$,

$$\begin{aligned} a_{N{+}{+}}(n{+}{+}) &= a_N(n{+}{+}) && \text{(definition (1))} \\ &= f(n, a_N(n)) && \text{(inductive hypothesis)} \\ &= f(n, a_{N{+}{+}}(n)) && \text{(definition (1) first equation)} \end{aligned}$$

For $n = N$,

$$\begin{aligned} a_{N{+}{+}}(n{+}{+}) &= f(n, a_N(n)) && \text{(definition (1) second equation)} \\ &= f(n, a_{N{+}{+}}(n)) && \text{(definition (1) first equation)} \end{aligned}$$

Therefore, $a_{N{+}{+}}(n{+}{+}) = f(n, a_{N{+}{+}}(n))$ for all $n < N{+}{+}$, and $P(N{+}{+})$ is true, closing the induction.

Now, we proceed to prove Q. Let $a : \boldsymbol{N} \to X$ be a function such that $a(n) = a_n(n)$ for every $n \in \boldsymbol{N}$. Since a_n exists and is unique for every $n \in \boldsymbol{N}$, it follows that function a exists and is unique. In particular,

$$\begin{aligned} a(0) &= a_0(0) && \text{(definition)} \\ &= c && (P(0)) \end{aligned}$$

and for every $n \in \boldsymbol{N}$,

$$\begin{aligned} a(n\text{++}) &= a_{n\text{++}}(n\text{++}) && \text{(definition)} \\ &= f(n, a_n(n)) && \text{(definition (1) second equation)} \\ &= f(n, a(n)) && \text{(definition)} \end{aligned}$$

Therefore Q is true, as desired. □

(ii) We aim to prove Q, but without using any properties of the natural numbers other than the Peano axioms directly, by first proving Lemma 3.5.12a defined as follows:

Lemma 3.5.12a For every natural number $N \in \boldsymbol{N}$, there exists a unique pair A_N, B_N of subsets of $\boldsymbol{N}$ which obeys the following properties:

(a) $A_N \cap B_N = \emptyset$,

(b) $A_N \cup B_N = \boldsymbol{N}$,

(c) $0 \in A_N$,

(d) $N\text{++} \in B_N$,

(e) Whenever $n \in B_N$, we have $n\text{++} \in B_N$;

(f) Whenever $n \in A_N$ and $n \neq N$, we have $n\text{++} \in A_N$.

First, however, we will show that

$$\text{For all } n \in \boldsymbol{N}, n \neq n\text{++}. \tag{3.5.12b}$$

We induct on n, starting with the base case $n = 0$. By axiom 2.3, $0 \neq 0\text{++}$ so the base case holds. Assume inductively that $n \neq n\text{++}$. By axiom 2.4, $n\text{++} \neq (n\text{++})\text{++}$. So the induction is closed.

Now we are ready to prove lemma 3.5.12a by inducting on N, starting with $N = 0$.

Base case: Let $A_0 = \{0\}$, let $B_0 = \boldsymbol{N} \setminus A_0$.

1. By proposition 3.1.27(g), $A_0 \cap B_0 = A_0 \cap (\boldsymbol{N} \setminus A_0) = \emptyset$ so (a) is true.
2. Also, $A_0 \cup B_0 = A_0 \cup (\boldsymbol{N} \setminus A_0) = \boldsymbol{N}$ so (b) is true.
3. Since $0 \in A_0$, (c) is true by construction.
4. Note, by construction, A_0, B_0 are two disjoint subsets that fully partition $\boldsymbol{N}$. Since A_0 is a singleton subset of 0, the successor 0++ is a natural number by axiom 2.2, but is distinct from 0 by axiom 2.3. So $(0\text{++} \notin A_0$ and $A_0 \cup B_0 = \boldsymbol{N}) \implies 0\text{++} \in B_0$. Hence (d) is true.
5. (e) is vacuously true since $0 \notin B_0$.
6. (f) is vacuously true since $0 \in A_0$ but $0 \neq 0$ is false.

By construction the pair A_0, B_0 of subsets of $\boldsymbol{N}$ is unique. This closes the base case.

Inductive hypothesis: Assume inductively that lemma 3.5.12a is true for some $N \in \boldsymbol{N}$.

We claim that

$$\text{For all } n \in \boldsymbol{N}, n\text{++} \in A_N \implies n \in A_N. \tag{3.5.12c}$$

Suppose, for contrapositive, that $n \notin A_N$. By (a) and (b) of the inductive hypothesis, $n \in B_N$, which implies $n\text{++} \in B_N$ by (e). Therefore $n\text{++} \notin A_N$ by (a) and (b). We conclude proposition 3.5.12c is true.

Induction: Let $A_{N\text{++}} = A_N \cup \{N\text{++}\}$, let $B_{N\text{++}} = \boldsymbol{N} \setminus A_{N\text{++}}$.

1. By proposition 3.1.27(g), $A_{N\text{++}} \cap B_{N\text{++}} = A_{N\text{++}} \cap (\boldsymbol{N} \setminus A_{N\text{++}}) = \emptyset$ so (a) is true.
2. Also, $A_{N\text{++}} \cup B_{N\text{++}} = A_{N\text{++}} \cup (\boldsymbol{N} \setminus A_{N\text{++}}) = \boldsymbol{N}$ so (b) is true.
3. (c) is true since $0 \in A_N$ by the inductive hypothesis, and by construction $A_N \subseteq A_{N\text{++}}$. So $0 \in A_{N\text{++}}$.

4. We aim to show $(N{+}{+}){+}{+} \in B_{N{+}{+}}$. By the inductive hypothesis, $N{+}{+} \in B_N$ which implies $N{+}{+} \neq n$ for all $n \in A_N$. Then by axiom 2.4, $(N{+}{+}){+}{+} \neq n{+}{+}$ for all $n \in A_N$. Also, $(N{+}{+}){+}{+} \neq N{+}{+}$ by 3.5.12b. Therefore $(N{+}{+}){+}{+} \neq n{+}{+}$ for all $n \in A_N \cup \{N{+}{+}\}$, i.e., $(N{+}{+}){+}{+} \neq n{+}{+}$ for all $n \in A_{N{+}{+}}$. Since $A_{N{+}{+}} \cup B_{N{+}{+}} = \boldsymbol{N}$ by (b), $N{+}{+} \in B_{N{+}{+}}$ as desired. So (d) is true.

5. We aim to show that whenever $n \in B_{N{+}{+}}$, we have $n{+}{+} \in B_{N{+}{+}}$. Suppose, for contradiction, that there exists $n \in B_{N{+}{+}}$ and $n{+}{+} \notin B_{N{+}{+}}$. By (a) and (b), this implies $n{+}{+} \in A_{N{+}{+}}$. Since $A_{N{+}{+}} = A_N \cup \{N{+}{+}\}$, either (i) $n{+}{+} \in A_N$ or (ii) $n{+}{+} = N{+}{+}$.

   (i) By proposition 3.5.12c, $n{+}{+} \in A_N \implies n \in A_N$ which in turn implies $n \in A_{N{+}{+}}$ since $A_N \subseteq A_{N{+}{+}}$ by construction.

   (ii) $n{+}{+} = N{+}{+}$ implies $n{+}{+} \in A_{N{+}{+}}$ by construction. By proposition 3.5.12c, $n \in A_{N{+}{+}}$.

   In both cases, $n \in A_{N{+}{+}}$ contradicts the assumption that $n \in B_{N{+}{+}}$ since $A_{N{+}{+}}$ and $B_{N{+}{+}}$ are disjoint by (a). So the assumption is false, and (e) is true.

6. We aim to show that whenever $n \in A_{N{+}{+}}$ and $n \neq N{+}{+}$, we have $n{+}{+} \in A_{N{+}{+}}$. Since $A_{N{+}{+}} = A_N \cup \{N{+}{+}\}$, there are three possible cases:

   (i) $n \in A_N$ and $n \neq N$. By the inductive hypothesis, $n{+}{+} \in A_N$. Since $A_N \subseteq A_{N{+}{+}}$ by construction, we have $n{+}{+} \in A_{N{+}{+}}$. Note that $n \in A_N \implies n \neq N{+}{+}$ as a consequence of axiom 2.3 and 2.4.

   (ii) $n = N$. By inductive hypothesis, $n \in A_N$. By construction, since $A_N \subseteq A_{N{+}{+}}$, we have $n \in A_{N{+}{+}}$. By axiom 2.4, $n = N \implies n{+}{+} = N{+}{+}$, so $n{+}{+} \in A_{N{+}{+}}$ by construction. Note that $n = N \implies n \neq N{+}{+}$ as a consequence of axiom 2.3 and 2.4.

   (iii) $n = N{+}{+}$. Since $n \neq N{+}{+}$ is false, the statement "whenever $n \in A_{N{+}{+}}$ and $n \neq N{+}{+}$, we have $n{+}{+} \in A_{N{+}{+}}$" is vacuously true.

   In all cases, whenever $n \in A_{N{+}{+}}$ and $n \neq N{+}{+}$, we have $n{+}{+} \in A_{N{+}{+}}$. So (f) is true.

Let $A'_{N{+}{+}}, B'_{N{+}{+}}$ be another pair of subsets of $\boldsymbol{N}$ such that they satisfy conditions (a) to (f). By condition (c), $0 \in A'_{N{+}{+}}$. By condition (f), whenever $n \in A'_{N{+}{+}}$ and $n \neq N{+}{+}$, we have $n{+}{+} \in A'_{N{+}{+}}$. Since both $A'_{N{+}{+}}$ and $A_{N{+}{+}}$ contain exactly the same elements, $A'_{N{+}{+}} = A_{N{+}{+}}$. By condition (a) and (b), $A'_{N{+}{+}}$ and $B'_{N{+}{+}}$ are disjoint subsets that fully partiion $\boldsymbol{N}$. So $B'_{N{+}{+}} = B_{N{+}{+}}$. We conclude the pair $A_{N{+}{+}}, B_{N{+}{+}}$ are unique. This closes the induction of Lemma 3.5.12a.

Let A_N, B_N be a unique pair of subsets of $\boldsymbol{N}$ that satisfied the properties of lemma 3.5.12a. We aim to prove Q by first proving another statement $S(N)$, which is defined as follows: for every natural number $N \in \boldsymbol{N}$, there exists a unique function $a_N : A_N \to X$ such that

$$a_N(0) = c$$

and

$$a_N(n{+}{+}) = f(n, a_N(n)) \text{ for all } n \in \boldsymbol{N} \text{ such that } n \in A_N \setminus \{N\}.$$

We induct on N, starting with the base case $S(0)$. The same argument for the base case of $P(0)$ in (i) applies, so the base case holds.

Assume inductively that $S(N)$ is true. Let $a_{N{+}{+}} : A_{N{+}{+}} \to X$ be a function such that

$$a_{N{+}{+}}(n) = \begin{cases} a_N(n) & \text{if } n \in A_N \\ f(N, a_N(N)) & \text{if } n = N{+}{+} \end{cases} \tag{2}$$

Since a_N is well defined and unique by the inductive hypothesis, $a_{N{+}{+}}$ is also well defined and unique.

For $n = 0$,

$$\begin{aligned} a_{N{+}{+}}(0) &= a_N(0) && \text{(definition (2))} \\ &= c && \text{(inductive hypothesis)} \end{aligned}$$

For $n \in A_N \setminus \{N\}$,

$$\begin{aligned} a_{N{+}{+}}(n{+}{+}) &= a_N(n{+}{+}) && \text{(definition (2))} \\ &= f(n, a_N(n)) && \text{(inductive hypothesis)} \\ &= f(n, a_{N{+}{+}}(n)) && \text{(definition (2) first equation)} \end{aligned}$$

For $n = N$,

$$\begin{aligned} a_{N{+}{+}}(n{+}{+}) &= f(n, a_N(n)) && \text{(definition (2) second equation)} \\ &= f(n, a_{N{+}{+}}(n)) && \text{(definition (2) first equation)} \end{aligned}$$

Therefore, $a_{N{+}{+}}(n{+}{+}) = f(n, a_{N{+}{+}}(n))$ for all $n \in A_N$, and $S(N{+}{+})$ is true, closing the induction.

Now, we proceed to prove Q. Let $a : \boldsymbol{N} \to X$ be a function such that $a(n) = a_n(n)$ for every $n \in \boldsymbol{N}$. Since a_n exists and is unique for every $n \in \boldsymbol{N}$, it follows that function a exists and is unique. In particular,

$$\begin{aligned} a(0) &= a_0(0) && \text{(definition)} \\ &= c && (S(0)) \end{aligned}$$

and for every $n \in \boldsymbol{N}$,

$$\begin{aligned} a(n{+}{+}) &= a_{n{+}{+}}(n{+}{+}) && \text{(definition)} \\ &= f(n, a_n(n)) && \text{(definition (2) second equation)} \\ &= f(n, a(n)) && \text{(definition)} \end{aligned}$$

Therefore Q is true, as desired. □

Remarks.

1. (d)-(f) in the induction step of proving Lemma 3.5.12a are the most challenging.

2. The induction step of proving Lemma 3.5.12a can potentially be simplified if we let $B_{N{+}{+}} = B_N \setminus \{N{+}{+}\}$ instead of $B_{N{+}{+}} = B_N \setminus A_{N{+}{+}}$. The reason is that we can directly leverage on the induction hypothesis that we have on B_N, instead of indirectly via $B_{N{+}{+}}$. Obvious in hindsight.

Exercise 3.5.13 The purpose of this exercise is to show that there is essentially only one version of the natural number system in set theory (cf. the discussion in Remark 2.1.12). Suppose we have a set $\boldsymbol{N}'$ of "alternative natural numbers", an "alternative zero" $0'$, and an "alternative increment operation" which takes any alternative natural number $n' \in \boldsymbol{N}'$ and returns another alternative natural number $n'{+}{+}' \in \boldsymbol{N}'$, such that the Peano axioms (Axioms 2.1-2.5) all hold with the natural numbers, zero, and increment replaced by their alternative counterparts. Show that there exists a bijection $f : N \to \boldsymbol{N}'$ from the natural numbers to the alternative natural numbers such that $f(0) = 0'$, and such that for any $n \in N$ and $n' \in \boldsymbol{N}'$, we have $f(n) = n'$ if and only if $f(n{+}{+}) = n'{+}{+}'$. (Hint: use Exercise 3.5.12.)

Attempt. Let $\boldsymbol{N}'$ be a set of "alternative natural numbers", an "alternative zero" $0'$, and an "alternative increment operation" which takes any alternative natural number $n' \in \boldsymbol{N}'$ and returns another alternative natural number $n'{+}{+}' \in \boldsymbol{N}'$, such that the Peano axioms (Axioms 2.1-2.5) all hold with the natural numbers, zero, and increment replaced by their alternative counterparts.

We aim to show that there exists a bijection $f : N \to \boldsymbol{N}'$ from the natural numbers to the alternative natural numbers such that $f(0) = 0'$, and such that for any $n \in N$ and $n' \in \boldsymbol{N}'$, we have $f(n) = n'$ if and only if $f(n{+}{+}) = n'{+}{+}'$.

Let $g : \boldsymbol{N} \times \boldsymbol{N}' \to \boldsymbol{N}'$ be a function such that

$$g(n, x) = x{+}{+}' \text{ for all } n \in \boldsymbol{N}, x \in \boldsymbol{N}'.$$

In essense, g ignores the first component of the pair tuple, and applies the "alternative increment operation" to the second component.

Let $0'$ be an element of $\boldsymbol{N}'$, and let $f : \boldsymbol{N} \to \boldsymbol{N}'$ be a function such that

$$f(0) = 0'$$

and

$$f(n\text{++}) = g(n, f(n)) \text{ for all } n \in \boldsymbol{N}.$$

By Exercise 3.5.12, function f exists and is unique. We aim to show $f(n) = n'$ if and only if $f(n\text{++}) = n'\text{++}'$.

1. ($\Rightarrow$) Suppose $f(n) = n'$. Then

$$\begin{aligned} f(n\text{++}) &= g(n, f(n)) && \text{(definition of } f) \\ &= g(n, n') \\ &= n'\text{++} && \text{(definition of } g) \end{aligned}$$

   Therefore $f(n) = n' \implies f(n\text{++}) = n'\text{++}'$.

2. ($\Leftarrow$) Suppose $f(n\text{++}) = n'\text{++}'$. Then

$$\begin{aligned} g(n, f(n)) &= f(n\text{++}) && \text{(definition of } f) \\ &= n'\text{++}' \end{aligned}$$

   By the definition of g, we have $f(n) = n'$. Therefore $f(n\text{++}) = n'\text{++}' \implies f(n) = n'$.

Conversely, let $h : \boldsymbol{N}' \times \boldsymbol{N} \to \boldsymbol{N}$ be a function such that

$$h(n', x) = x\text{++} \text{ for all } n' \in \boldsymbol{N}', x \in \boldsymbol{N}.$$

We can construct an inverse function $f^{-1} : \boldsymbol{N}' \to \boldsymbol{N}$ such that

$$f^{-1}(0') = 0$$

and

$$f^{-1}(n'\text{++}') = h(n', f^{-1}(n')) \text{ for all } n' \in \boldsymbol{N}'.$$

We can then apply similar arguments to show that f^{-1} is unique, and $f^{-1}(n') = n$ if and only if $f^{-1}(n'\text{++}') = n\text{++}$. Since f is invertible, f is a bijection, as desired. □

Attempt variant. Instead of constructing an inverse function to prove the bijectivitiy of f, we aim to prove injectivity and surjectivity directly.

Injectivity. Let $m, n \in \boldsymbol{N}$. We aim to show that $m \neq n \implies f(m) \neq f(n)$. We induct on n, starting with $n = 0$. Since $m \neq 0$, it must be a successor by axiom 2.3. Let $x\text{++} = m$ for some $x \in \boldsymbol{N}$. Assume, for contradiction, that $f(x\text{++}) = f(0) = 0'$. So we have

$$\begin{aligned} f(x\text{++}) &= g(x, f(x)) && \text{(definition of } f) \\ &= f(x)\text{++}' && \text{(definition of } g) \\ &= 0' && \text{(assumption)} \end{aligned}$$

which is a contradiction by axiom 2.3, since $0'$ cannot be a successor. Hence the base case holds. Assume inductively that $m \neq n \implies f(m) \neq f(n)$. We aim to show $m \neq n\text{++} \implies f(m) \neq f(n\text{++})$. There are two cases: $m = 0$ and $m \neq 0$.

If $m = 0$, then $f(m) = f(0) = 0'$, whereas $f(n\text{++}) = g(n, f(n)) = f(n)\text{++}'$. By axiom 2.3, $0' \neq f(n)\text{++}'$. Therefore, $m \neq n\text{++} \implies f(m) \neq f(n\text{++})$ when $m = 0$.

If $m \neq 0$, then it must be a successor by axiom 2.3. Let $x{+}{+} = m$ for some $x \in \boldsymbol{N}$. We aim to show $x{+}{+} \neq n{+}{+} \implies f(x{+}{+}) \neq f(n{+}{+})$. By axiom 2.4 $x{+}{+} \neq n{+}{+} \implies x \neq n$, which implies, by the inductive hypothesis, $f(x) \neq f(n)$. Assume, for contradiction, that $f(x{+}{+}) = f(n{+}{+})$. We have

$$\begin{aligned} f(x{+}{+}) &= f(n{+}{+}) \\ g(x, f(x)) &= g(n, f(n)) && \text{(defintion of } f) \\ f(x){+}{+}' &= f(n){+}{+}' && \text{(defintion of } g) \end{aligned}$$

which, by axiom 2.4, implies $f(x) = f(n)$, a contradiction. Hence the assumption is false, and we have $m \neq n{+}{+} \implies f(m) \neq f(n{+}{+})$ when $m \neq 0$. This closes the inductive proof for the injectivity of f.

Surjectivity. We aim to show that for all $n' \in \boldsymbol{N}'$ there exists $n \in N$ such that $f(n) = n'$. We induct on n'. For the base case, by the definition of f, we have $f(0) = n'$ when $n' = 0'$. Assume inductively that $n \in N$ exists such that $f(n) = n'$ for a specific $n' \in \boldsymbol{N}'$. We want to check if there exists $x \in N$ such that $f(x) = n{+}{+}'$. But $n{+}{+}' = g(n, f(n)) = f(n{+}{+})$, so $x \in N$ exists, namely, $x = n{+}{+}$. This closes the induction.

Since f is both injective and surjective, f is bijective. □

Remarks.

1. Once the inverse function is constructed, we need to futher verify that both $f \circ f^{-1}$ and $f^{-1} \circ f$ are the identitiy functions.

2. Instead of constructing an inverse function to prove bijectivitiy, a more direct approch is to prove injectivity and surjectivity. However, it seems perhaps a little surprising, but inevitable, that induction is involved in the process. Obvious in hindsight, the inductive hypothesis for the surjectivity proof was not immediately obvious.

3.6 Cardinality of Sets

Definition 3.6.1 (Equal cardinality) We say that two sets X and Y have *equal cardinality* iff there exists a bijection $f : X \to Y$ from X to Y.

Proposition 3.6.4 (Equal cardinality is an equivalence relation) *Let X, Y, Z be sets. Then X has equal cardinality with X. If X has equal cardinality with Y, then Y has equal cardinality with X. If X has equal cardinality with Y and Y has equal cardinality with Z, then X has equal cardinality with Z.* (Proof at Exercise 3.6.1.)

Definition 3.6.5 (Cardinality n) Let n be a natural number. A set X is said to have *cardinality* n, iff it has equal cardinality with $\{i \in \boldsymbol{N} : 1 \leq i \leq n\}$. We also say that X *has n elements* iff it has cardinality n.

Proposition 3.6.8 (Uniqueness of cardinality) *Let X be a set with some cardinality n. Then X cannot have any other cardinality, i.e., X cannot have cardinality m for any $m \neq n$.*

Lemma 3.6.9 (Cardinality reduction) *Suppose that $n \geq 1$, and X has cardinality n. Then X is non-empty, and if x is any element of X, then the set $X - \{x\}$ (i.e., X with the element x removed) has cardinality $n - 1$.*

Strictly speaking, $n - 1$ has not yet been defined in this text. For the purposes of this lemma, we define $n - 1$ to be the unique natural number m such that $m{+}{+} = n$; this m is given by Lemma 2.2.10 of unique predecessor.

Definition 3.6.10 (Finite sets) A set is *finite* iff it has cardinality n for some natural number n; otherwise, the set is called *infinite*. If X is a finite set, we use $\#(X)$to denote the cardinality of X.

Theorem 3.6.12 ($\boldsymbol{N}$ is infinite) *The set of natural numbers $\boldsymbol{N}$ is infinite.*

Proposition 3.6.14 (Cardinal arithmetic)

(a) *Let X be a finite set, and let x be an object which is not an element of X. Then $X \cup \{x\}$ is finite and $\#(X \cup \{x\}) = \#(X) + 1$.*

(b) *Let X and Y be finite sets. Then $X \cup Y$ is finite and $\#(X \cup Y) \leq \#(X) + \#(Y)$. If in addition X and Y are disjoint (i.e., $X \cap Y = \emptyset$), then $\#(X \cup Y) = \#(X) + \#(Y)$.*

(c) *Let X be a finite set, and let Y be a subset of X. Then Y is finite, and $\#(Y) \leq \#(X)$. If in addition $Y \neq X$ (i.e., Y is a proper subset of X), then we have $\#(Y) < \#(X)$.*

(d) *If X is a finite set, and $f : X \to Y$ is a function, then $f(X)$ is a finite set with $\#(f(X)) \leq \#(X)$. One has equality $\#(f(X)) = \#(X)$ if and only if f is one-to-one.*

(e) *Let X and Y be finite sets. Then Cartesian product $X \times Y$ is finite and $\#(X \times Y) = \#(X) \times \#(Y)$.*

(f) *Let X and Y be finite sets. Then the set Y^X (defined in Axiom 3.11) is finite and $\#(Y^X) = \#(Y)^{\#(X)}$.*

(Proof at Exercise 3.6.4.)

Remark 3.6.15 Proposition 3.6.14 suggests that there is another way to define the arithmetic operations of natural numbers; not defined recursively as in Definitions 2.2.1, 2.3.1, 2.3.11, but instead using the notions of union, Cartesian product, and power set. This is the basis of *cardinal arithmetic*, which is an alternative foundation to arithmetic than the Peano arithmetic we have developed here. (See Exercises 3.6.5, 3.6.6.)

— Exercises —

Exercise 3.6.1 Prove Proposition 3.6.4.

Attempt. Let X, Y, Z be sets. We want to show

1. X has equal cardinality with X. By definition 3.6.1, we aim to show there exists a bijection from X to X. Let $f : X \to X$ be a function such that $f(x) = x$ for every $x \in X$. Let $x, y \in X$ and $x \neq y$. Since $f(x) = x$ and $f(y) = y$, $f(x) \neq f(y)$. Hence f is injective. For every $x \in X$, we have $f(x) = x$. So f is surjective. Hence f is bijective, as desired.

2. if X has equal cardinality with Y, then Y has equal cardinality with X. Equivalently, we aim to show if there is a bijection from X to Y, then there is a bijection from Y to X.

   Suppose $f : X \to Y$ is a bijection from X to Y. Since f is injective, every $x \in X$ maps to a unique $f(x) \in Y$. Since f is surjective, we can define a function $f^{-1} : Y \to X$ such that for every $y \in Y$, $f^{-1}(y) = x$ such that $f(x) = y$ for some $x \in X$. Since there exists $x \in X$ for every $y \in Y$ such that $f(x) = y$, f^{-1} is well defined.

   Let $y, y' \in Y$ and $y \neq y'$. Since f is surjective, there must exist $x, x' \in X$ such that $f(x) = y$ and $f(x') = y'$. Since f is injective, $y \neq y' \implies f(x) \neq f(x') \implies x \neq x'$. Then $f^{-1}(f(x)) = x$ and $f^{-1}(f(x')) = x'$ implies $f^{-1}(f(x)) \neq f^{-1}(f(x')) \iff f^{-1}(y) \neq f^{-1}(y')$. Since $y \neq y \implies f^{-1}(y) \neq f^{-1}(y')$, f^{-1} is injective. For every $x \in X$ we have $f^{-1}(f(x)) = x$, so f^{-1} is surjective. Hence f^{-1} is bijective, as desired.

3. if X has equal cardinality with Y and Y and equal cardinality with Z, then X has equal cardinality with Z. Equivalently, we aim to show if there is a bijection from X to Y and a bijection from Y to Z, then there is a bijection from X to Z.

   Suppose $f : X \to Y$ is a bijection from X to Y, and suppose $g : Y \to Z$ is a bijection from Y to Z. Let $h = g \circ f$ be a function from X to Z. h is well defined since f and g are both well defined by assumption.

Let $x, x' \in X$ and $x \neq x'$. Then let $y, y' \in Y$ such that $y = f(x), y' = f(x')$. Since f is injective, $y \neq y'$, and since g is injective, $g(y) \neq g(y')$. Since $x \neq x' \implies (g \circ f)(x) \neq (g \circ f)(x')$, h is injective.

Since f is surjective, X is mapped onto the entire Y. Similarly, since g is surjective, Y is in turn mapped onto the entire Z. It follows $g \circ f$ maps X onto the entire Z, so h is surjective.

Since h is both injective and surjective, h is bijective, as desired.

□

Exercise 3.6.2 Show that a set X has cardinality 0 if and only if X is the empty set.

Attempt. By definition 3.6.5, a set X has cardinality 0 iff it has equal cardinality with $\{i \in \boldsymbol{N} : 1 \leq i \leq 0\}$, which is the empty set. Let $f : X \to \emptyset$ be a function. We aim to show that $X = \emptyset$ iff f is bijective.

1. $(\Rightarrow)$ Suppose $X = \emptyset$. Since both the domain and codomain are empty, f is both injective and surjective vacuously.
2. $(\Leftarrow)$ Suppose $f : X \to \emptyset$ is bijective. For every $x \in X$, there must exists some $f(x) \in \emptyset$, which is impossible. So X must be empty.

This concludes the proof. □

Exercise 3.6.3 Let n be a natural number, and let $f : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to \boldsymbol{N}$ be a function. Show that there exists a natural number M such that $f(i) \leq M$ for all $1 \leq i \leq n$. (Hint: induct on n. You may also want to peek at Lemma 5.1.14.) Thus finite subsets of the natural numbers are bounded. Use this to give an alternate proof of Theorem 3.6.12 that does not use Lemma 3.6.9.

Attempt. Let n be a natural number, and let $f : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to \boldsymbol{N}$ be a function. Let $P(n)$ be the property that there exists a natural number M such that $f(i) \leq M$ for all $1 \leq i \leq n$. First, we will show $P(n)$ holds, and then use $P(n)$ to give an alternate proof of Theorem 3.6.12 that does not use Lemma 3.6.9.

Proof of $P(n)$. We induct on n. For $n = 0$, the domain of the function is empty, so the base case $P(0)$ holds vacuously. Assume inductively that $P(n)$ is true for a specific n. We aim to show $P(n{+}{+})$ is true.

Let $f' : \{i \in \boldsymbol{N} : 1 \leq i \leq n{+}{+}\} \to \boldsymbol{N}$ be a function. We can define $f : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to \boldsymbol{N}$ as a function that retricts f' to a subset of the domain such that $f(i) = f'(i)$ for $1 \leq i \leq n$. By the inductive hypothesis, there exists $M \in \boldsymbol{N}$ such that $f(i) \leq M$ for all $1 \leq i \leq n$. Let $j = f'(n{+}{+})$. If $j \leq M$, then $f'(i) = f(i) \leq M$ for all $1 \leq i \leq n$, and $f'(n{+}{+}) \leq M$, so we are done. If $j > M$, then there exists $M' = j$, and $f'(i) \leq M'$ for all $1 \leq i \leq n{+}{+}$. This closes the induction.

Proof of theorem 3.6.12 using $P(n)$. We aim to show that the set of natural numbers $\boldsymbol{N}$ is infinite. Suppose for contradiction that the set of natural numbers $\boldsymbol{N}$ is finite. By definition 3.6.10 of finite sets, $\boldsymbol{N}$ has cardinality $\#(\boldsymbol{N}) = n \in \boldsymbol{N}$. Let $f : \{i \in \boldsymbol{N} : 1 \leq i \leq n\} \to \boldsymbol{N}$ to be a function such that $f(i) = i$ for every $i \in \boldsymbol{N}$. By $P(n)$, there exists some $M \in \boldsymbol{N}$ such that $f(i) \leq M$ for all $1 \leq i \leq n$. By axiom 2.2 of successor, $M{+}{+}$ is a natural number, so $M{+}{+}$ must be an element of the finite set $\{i \in \boldsymbol{N} : 1 \leq i \leq n\} = \boldsymbol{N}$. This implies $M{+}{+} \leq n \leq M$, a contradiction. Hence the assumption is false, and $\boldsymbol{N}$ is infinite. □

Appendix A The Basics of Mathematical Logic

A.1 Mathematical statements

— Exercises —

Exercise A.1.1. What is the negation of the statement "either X is true, or Y is true, but not both"?

Attempt: Either both X and Y are true, or both are false.

$$\begin{aligned} S &= (X \vee Y) \wedge \neg(X \wedge Y) \\ \neg S &= \neg(X \vee Y) \vee (X \wedge Y) \\ &= (\neg X \wedge \neg Y) \vee (X \wedge Y) \end{aligned}$$ □

Exercise A.1.2. What is the negation of the statement "X is true if and only if Y is true"? (There may be multiple ways to phrase this negation).

Attempt: (i) X is opposite of Y. (ii) Either X is true and Y is false, or Y is true and X is false.

$$\begin{aligned} S &= X \text{ iff } Y \\ &= (\neg Y \vee X) \wedge (\neg X \vee Y) \\ \neg S &= \neg(\neg Y \vee X) \vee \neg(\neg X \vee Y) \\ &= (Y \wedge \neg X) \vee (X \wedge \neg Y) \end{aligned}$$ □

Exercise A.1.3. Suppose that you have shown that whenever X is true, then Y is true, and whenever X is false, then Y is false. Have you now demonstrated that X and Y are logically equivalent? Explain.

Attempt: Yes. It can be easily shown that if Y is true then X must be true or else it would lead to contradiction. Similarly, when Y is false X must be false. Thus the logical equivalence: $X \wedge Y \vee \neg X \wedge \neg Y$, or X iff Y. □

Exercise A.1.4. Suppose that you have shown that whenever X is true, then Y is true, and whenever Y is false, then X is false. Have you now demonstrated that X is true if and only if Y is true? Explain.

Attempt: No. Whenever Y is true, X can be false and there is no contradiction. □

Exercise A.1.5. Suppose you know that X is true if and only if Y is true, and you know that Y is true if and only if Z is true. Is this enough to show that X, Y, Z are all logically equivalent? Explain.

Attempt: Yes. Given X is logically equivalent to Y, which is logically equivalent to Z, X is logically equivalent to Z. □

Exercise A.1.6. Suppose you know that whenever X is true, then Y is true; that whenever Y is true, then Z is true; and whenever Z is true, then X is true. Is this enough to show that X, Y, Z are all logically equivalent? Explain.

Attempt: Yes. If any one of X, Y, Z is false, the others must also be false for the circular implications to hold. For the same reason, if any of them is true, then all of them must be true. □

A.5 Nested Quantifiers

— Exercises —

Exercise A.5.1. What does each of the following statements mean, and which of them are true? Can you find gaming metaphors for each of these statements?

(a) For every positive number x, and every positive number y, we have $y^2 = x$.

(b) There exists a positive number x such that for every positive number y, we have $y^2 = x$.

(c) There exists a positive number x, and there exists a positive number y, such that $y^2 = x$.

(d) For every positive number y, there exists a positive number x such that $y^2 = x$.

(e) There exists a positive number y such that for every positive number x, we have $y^2 = x$.

Attempt:

(a) The square of every positive number is equal to each other – false. There are two ways to play the game: you can choose either a positive number x or y (but not both) first. Then your opponent can always pick the other positive number to show that y^2 is not equal to x to defeat that.

(b) The square of every positive number is the same positive number – false. You choose a positive number x first. Then your opponent can pick a positive number y to show that y^2 is not equal to x to defeat that.

(c) There is at least one positive number y with a positive square – true. There are two ways to play the game: your opponent hands you either a positive number x or y (but not both), and you can always find the other positive number so that the square of y is equal to x.

(d) The square of every positive number is a positive number – true. You opponent hands you a positive number y, and you can always find a positive number x that is equal to y^2.

(e) The square of any positive number is equal to the same positive number – false. You choose a positive numbrer y first. Then your opponent can find a positive number x that is not equal to y^2 to defeat that.

A.6 Some examples of proofs and quantifiers

— Exercises —

Exercise It is impossible to prove the statement "There exists a $\delta > 0$ such that for every $\epsilon > 0, 2\delta < \epsilon$.". Why?

Attempt: Suppose δ is a positive number such that the statement is true. We want to show this would lead to a contradiction. Since $2\delta < \epsilon$ for every $\epsilon > 0$, we can choose $\epsilon := \delta$. Thus $2\delta < \delta$, which is absurd as desired. Therefore, the statement is false. □

A.7 Equality

Four required *axioms of equality* for the purpose of logic:

- (Reflexive axiom). Given any object x, we have $x = x$.
- (Symmetry axiom). Given any two objects x and y of the same type, if $x = y$, then $y = x$.
- (Transitive axiom). Given any three objects x, y, z of the same type, if $x = y$ and $y = z$, then $x = z$.
- (Substitution axiom). Given any two objects x and y of the same type, if $x = y$, then $f(x) = f(y)$ for all functions or operations f.

— Exercises —

Exercise A.7.1. Suppose you have four real numbers a, b, c, d and you know that $a = b$ and $c = d$. Use the above four axioms to deduce that $a + d = b + c$.

Attempt: Since $a = b$, substitution of a by b in $a + d$ gives $a + d = b + d$. Since $c = d$, by symmetry we have $d = c$, and substitution of d by c in $b + d$ gives $b + d = b + c$. Therefore, $a + d = b + d = b + c$. By transitivity, we have $a + d = b + c$ as desired. □