MATH 161, Autumn 2024
SCRIPT 1: Sets, Functions and Cardinality

Sets and functions are among the most fundamental objects in mathematics. A formal treatment of set theory was first undertaken at the end of the 19th Century and was finally codified in the form of the Zermelo-Fraenkel axioms. While fascinating in its own right, pursuit of these formalisms at this point would distract us from our main purpose of studying Calculus. Thus, we present a simplified version that will suffice for our immediate purposes.

Sets

Definition 1.1. (Working Definition) A *set* is an object S with the property that, given any x, we have the dichotomy that precisely one of the two conditions $x \in S$ or $x \notin S$ is true. In the former case, we say that x is an *element* of S, and in the latter, we say that x is not an element of S.

A set is often presented in one of the following forms:

- A complete listing of its elements.

  Example: the set $S = \{1, 2, 3, 4, 5\}$ contains precisely the five smallest positive integers.

- A listing of some of its elements with ellipses to indicate unnamed elements.

  Example 1: the set $S = \{3, 4, 5, \ldots, 100\}$ contains the positive integers from 3 to 100, including 6 through 99, even though these latter are not explicitly named.

  Example 2: the set $S = \{2, 4, 6, \ldots, 2n, \ldots\}$ is the set of all positive even integers.

- A two-part indication of the elements of the set by first identifying the source of all elements and then giving additional conditions for membership in the set.

  Example 1: $S = \{x \in \mathbb{N} \mid x \text{ is prime}\}$ is the set of primes.

  Example 2: $S = \{x \in \mathbb{Z} \mid x^2 < 3\}$ is the set of integers whose squares are less than 3.

Definition 1.2. Two sets A and B are *equal* if they contain precisely the same elements, that is, $x \in A$ if and only if $x \in B$. When A and B are equal, we denote this by $A = B$.

Definition 1.3. A set A is a *subset* of a set B if every element of A is also an element of B, that is, if $x \in A$, then $x \in B$. When A is a subset of B, we denote this by $A \subset B$. If $A \subset B$ but $A \neq B$ we say that A is a *proper* subset of B.

Exercise 1.4. Let $A = \{1, \{2\}\}$.
Is $1 \in A$? Yes.
Is $2 \in A$? No.
Is $\{1\} \subset A$? Yes.
Is $\{2\} \subset A$? No.
Is $1 \subset A$? No.
Is $\{1\} \in A$? No.
Is $\{2\} \in A$? Yes.
Is $\{\{2\}\} \subset A$? Yes.
Explain.

Definition 1.5. Let A and B be two sets. The *union* of A and B is the set

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

Definition 1.6. Let A and B be two sets. The *intersection* of A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

Theorem 1.7. *Let A and B be two sets. Then:*

a) $A = B$ *if and only if* $A \subset B$ *and* $B \subset A$.

Proof. Let $P(n)$ be the contrapositive of Theorem 1.7 (a), where we want to prove $P(n)$. Then, $P(n)$ is the statement that if $A \not\subset B$ or $B \not\subset A$, then $A \neq B$ (the or here is inclusive).

By Definition 1.3, if $A \not\subset B$, then there exists some $x \in A$ such that $x \notin B$. Therefore, by Definition 1.2, $A \neq B$.

Similarly, by Definition 1.3, if $B \not\subset A$, then there exists some $y \in B$ such that $y \notin A$. Therefore, by Definition 1.2, $A \neq B$.

This completes the proof.

QED

b) $A \subset A \cup B$.

Proof. We prove this by contradiction. Assume $A \not\subset A \cup B$. Then, by Definition 1.3, there must exist some $x \in A$ such that $x \notin A \cup B$. This violates Definition 1.5. This completes the proof.

QED

c) $A \cap B \subset A$.

Proof. We prove this by contradiction. Assume $A \cap B \not\subset A$. Then, by Definition 1.3, there must exist some $x \in A \cap B$ such that $x \notin A$. This violates Definition 1.6. This completes the proof.

QED

A special example of the intersection of two sets is when the two sets have no elements in common. This motivates the following definition.

Definition 1.8. The *empty set* is the set with no elements, and it is denoted $\emptyset$. That is, no matter what x is, we have $x \notin \emptyset$.

Definition 1.9. Two sets A and B are *disjoint* if $A \cap B = \emptyset$.

Exercise 1.10. Show that if A is any set, then $\emptyset \subset A$.

Proof. We prove this by contradiction. Assume $\emptyset \not\subset A$. Then, by Definition 1.3, there must exist some $x \in \emptyset$ such that $x \notin A$. This requires that $x \in \emptyset$, which violates Definition 1.8. This completes the proof.

QED

Definition 1.11. Let A and B be two sets. The *difference* of B from A is the set

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

The set $A \setminus B$ is also called the *complement* of B relative to A. When the set A is clear from the context, this set is sometimes denoted B^c, but we will try to avoid this imprecise formulation and use it only with warning.

Exercise 1.12. Let $A = \{x \in \mathbb{N} \mid x \text{ is even}\}; B = \{x \in \mathbb{N} \mid x \text{ is odd}\}; C = \{x \in \mathbb{N} \mid x \text{ is prime}\}; D = \{x \in \mathbb{N} \mid x \text{ is a perfect square}\}$. Find all possible set differences.
$A \setminus B = A$.
$B \setminus A = B$.
$A \setminus C = \{x \in \mathbb{N} \mid x \text{ is even} \mid x \geq 4\}$.
$C \setminus A = \{x \in \mathbb{N} \mid x \text{ is prime} \mid x \neq 2\}$.
$A \setminus D = \{x \in \mathbb{N} \mid x \text{ is even} \mid \text{for all y} \in A,\ x \neq y^2\}$.
$D \setminus A = \{x \in \mathbb{N} \mid x \text{ is a perfect square} \mid \sqrt{x} \notin A\}$.
$B \setminus C = \{x \in B \mid x \text{ is not prime}\}$.
$C \setminus B = \{2\}$.
$B \setminus D = \{x \in B \mid x \text{ is not a perfect square}\}$.
$D \setminus B = \{x \in D \mid x \text{ is even}\}$.
$C \setminus D = C$.
$D \setminus C = D$.
$A \setminus A = B \setminus B = C \setminus C = D \setminus D = \emptyset$.

Theorem 1.13. *Let A, B and X be sets. Then:*

a) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$

Proof. We proceed by direct proof. By Definition 1.5 and Definition 1.11, the LHS is the set of all elements in X that are in neither A nor B. In formal notation, $X \setminus (A \cup B) = \{x \in X \mid x \notin A, x \notin B\}$.

By Definition 1.6 and Definition 1.11, the RHS is the set of all elements that are in both, $(X \setminus A)$ and $(X \setminus B)$. In turn, $(X \setminus A)$ is $\{x \in X \mid x \notin A\}$ and $(X \setminus B)$ is $\{x \in X \mid x \notin B\}$. Therefore, $X \setminus (A \cup B) = \{x \in X \mid x \notin A, x \notin B\}$.

Hence, the expression for LHS matches the expression for RHS. This completes the proof.

QED

b) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Proof. We proceed by direct proof. By Definition 1.6 and Definition 1.11, the LHS is the set of all elements in X that are in not in the intersection of A and B, i.e., elements that are in X, and also are in either A or B or neither, but not both. In formal notation, this is $\{x \in X \mid x \notin A \cap B\}$.

By Definition 1.5 and Definition 1.11, the RHS is the set of all elements that are in $(X \setminus A)$ or $(X \setminus B)$ or both. This, in turn, is the set of all elements $(x \in X \mid x \notin A)$ or $(x \in X \mid x \notin B)$ or $(x \in X \mid x \notin A, x \notin B)$. If an element is not in A, or it is not in B, or it is in neither A nor B, then it is not in $A \cap B$. Therefore, the RHS is $\{x \in X \mid x \notin A \cap B\}$.

Hence, the expression for LHS matches the expression for RHS. This completes the proof.

QED

Sometimes we will encounter families of sets. The definitions of intersection/union can be extended to infinitely many sets.

Definition 1.14. Let $\mathcal{A} = \{A_\lambda \mid \lambda \in I\}$ be a collection of sets indexed by a nonempty set I. Then the intersection and union of $\mathcal{A}$ are the sets

$$\bigcap_{\lambda \in I} A_\lambda = \{x \mid x \in A_\lambda,\ \text{for all } \lambda \in I\},$$

and

$$\bigcup_{\lambda \in I} A_\lambda = \{x \mid x \in A_\lambda,\ \text{for some } \lambda \in I\}.$$

Theorem 1.15. *Let X be a set, and let $\mathcal{A} = \{A_\lambda \mid \lambda \in I\}$ be a nonempty collection of sets. Then:*

1. $X \setminus \left(\bigcup_{\lambda \in I} A_\lambda\right) = \bigcap_{\lambda \in I}(X \setminus A_\lambda)$.

   Proof. We proceed by direct proof. By Definition 1.11 and Definition 1.14, the LHS is the set $\{x \in X \mid x \notin \bigcup_{\lambda \in I} A_\lambda\}$. Since $x \notin \bigcup_{\lambda \in I} A_\lambda$, this implies that for all $\lambda \in I$, $x \notin A_\lambda$.

   By Definition 1.11 and Definition 1.14, the RHS is the intersection of sets $\{x \in X \mid x \notin A_\lambda\}$ for all $\lambda \in I$.

   Hence, the expression for LHS matches the expression for RHS. This completes the proof.

   QED

2. $X \setminus \left(\bigcap_{\lambda \in I} A_\lambda\right) = \bigcup_{\lambda \in I}(X \setminus A_\lambda)$.

   Proof. We proceed by direct proof. By Definition 1.11 and Definition 1.14, the LHS is the set $\{x \in X \mid x \notin \bigcap_{\lambda \in I} A_\lambda\}$. Since $x \notin \bigcap_{\lambda \in I} A_\lambda$, this implies that $\neg\forall\lambda \in I : x \in A_\lambda$. This is equivalent to $\exists\lambda \in I : x \in X, x \notin A_\lambda$.

   By Definition 1.11 and Definition 1.14, the RHS is the set $\{x \mid x \in X \setminus A_\lambda, \text{for some } \lambda \in I\}$. This is equivalent to $\exists\lambda \in I : x \in X, x \notin A_\lambda$.

   Hence, the expression for LHS matches the expression for RHS. This completes the proof.

   QED

Definition 1.16. Let A and B be two nonempty sets. The *Cartesian product* of A and B is the set of ordered pairs

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

If (a, b) and $(a', b') \in A \times B$, we say that (a, b) and (a', b') are *equal* if and only if $a = a'$ and $b = b'$. In this case, we write $(a, b) = (a', b')$.

Functions

Definition 1.17. Let A and B be two nonempty sets. A *function* f from A to B is a subset $f \subset A \times B$ such that for all $a \in A$ there exists a unique $b \in B$ satisfying $(a, b) \in f$. To express the idea that $(a, b) \in f$, we most often write $f(a) = b$. To express that f is a function from A to B in symbols we write $f\colon A \to B$.

Exercise 1.18. Let the function $f\colon \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = 2n$. Write f as a subset of $\mathbb{Z} \times \mathbb{Z}$.

$f \subset \mathbb{Z} \times \mathbb{Z}$ is the set $f = \{(n, 2n) \mid n \in \mathbb{Z}\} = \{\dots, (-2, -4), (-1, -2), (0, 0), (1, 2), (2, 4), \dots\}$.

Definition 1.19. Let $f\colon A \to B$ be a function. The *domain* of f is A and the *codomain* of f is B. If $X \subset A$, then the *image of X under f* is the set

$$f(X) = \{f(x) \in B \mid x \in X\}.$$

If $Y \subset B$, then the *preimage of Y under f* is the set

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Exercise 1.20. Must $f(f^{-1}(Y)) = Y$ and $f^{-1}(f(X)) = X$? For each, either prove that it always holds or give a counterexample.

Let A and B be non-empty sets such that $A = \{1, 2\}, B = \{1, 2, 3\}$. Let $f\colon A \to B$ be defined by $f(1) = 1, f(2) = 2$. Let $Y \subset B = \{2, 3\}$. Then $f^{-1}(Y) = \{2\}$ and $f(f^{-1}(Y)) = \{2\} \neq Y$. Thus, we have a counterexample where $f(f^{-1}(Y)) \neq Y$.

Let A and B be non-empty sets such that $A = \{1, 2, 3\}, B = \{1, 2\}$. Let $f\colon A \to B$ be defined by $f(1) = 1, f(2) = 2, f(3) = 2$. Let $X \subset A = \{2\}$. Then $f(X) = \{2\}$ and $f^{-1}(f(X)) = \{2, 3\} \neq X$. Thus, we have a counterexample where $f^{-1}(f(X)) \neq X$.

Definition 1.21. A function $f\colon A \to B$ is *surjective* (also known as 'onto') if, for every $b \in B$, there is some $a \in A$ such that $f(a) = b$. The function f is *injective* (also known as 'one-to-one') if for all $a, a' \in A$, if $f(a) = f(a')$, then $a = a'$. The function f is *bijective*, (also known as a bijection or a 'one-to-one' correspondence) if it is surjective and injective.

Exercise 1.22. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n + 2$. Is f injective? Yes, since $a + 2 = a' + 2$ implies $a = a'$. Is f surjective? No, since 1 and 2 are not in the image of f.

Exercise 1.23. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x + 2$. Is f injective? Yes (same proof as above, for Exercise 1.22). Is f surjective? Yes, since for all $y \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that $y = x + 2$.

Exercise 1.24. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective? Yes, since $a^2 = (a')^2$ implies $a = a'$. Is f surjective? No, since 2 is not in the image of f.

Exercise 1.25. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$. Is f injective? No, since $a^2 = (a')^2$ does not imply $a = a'$. This is because $a = -a'$ also leads to $a^2 = (a')^2$. Is f surjective? No, since 2 is not in the image of f.

Definition 1.26. Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$. Then the *composition* $g \circ f : A \longrightarrow C$ is defined by $(g \circ f)(x) = g(f(x))$, for all $x \in A$.

Proposition 1.27. *Let A, B, and C be sets and suppose that $f : A \longrightarrow B$ and $g : B \longrightarrow C$. Then $g \circ f : A \longrightarrow C$ and*

a) if f and g are both injections, so is $g \circ f$.

Proof. We prove this by contradiction. Assume that $g \circ f$ is not an injection, i.e., $(g \circ f)(a) = (g \circ f)(a')$ but $a \neq a'$.

Since g is an injection, we know that $b = b'$, i.e., $f(a) = f(a')$. Since f is an injection, this implies that $a = a'$. We have reached a contradiction and this completes the proof.

QED

b) if f and g are both surjections, so is $g \circ f$.

Proof. We prove this by contradiction. Assume that $g \circ f$ is not a surjection, i.e., $\exists c \in C$ such that $\forall a \in A : (g \circ f)(a) \neq c$. In other words, we assume that there exists some $c \in C$ such that there is no $a \in A$ for which $(g \circ f)(a) = c$. Let this value of c be denoted by c_0.

Since g is surjective, $\forall c \in C : \exists b \in B$ such that $g(b) = c$. Hence, let b_0 be defined by $g(b_0) = c_0$. Since f is surjective, $\forall b \in B : \exists a \in A$ such that $f(a) = b$. Hence, let a_0 be defined by $f(a_0) = b_0$.

Then, $(g \circ f)(a_0) = g((f(a_0'))) = g(b_0) = c_0$, and we have reached a contradiction. This completes the proof.

QED

c) if f and g are both bijections, so is $g \circ f$.

Proof. We have shown above that if f and g are both injections, so is $g \circ f$, and if f and g are both surjections, so is $g \circ f$.

Since f and g are both bijections, i.e., f and g are both injections as well as surjections, we know that $g \circ f$ is both an injection and a surjection. Therefore, $g \circ f$ is a bijection.

QED

Proposition 1.28. *Suppose that $f\colon A \to B$ is bijective. Then there exists a bijection $g\colon B \to A$ that satisfies $(g \circ f)(a) = a, \forall a \in A$, and $(f \circ g)(b) = b$, for all $b \in B$. The function g is often called the* inverse *of f and denoted f^{-1}. It should not be confused with the preimage.*

Proof. We know that f is surjective, i.e., for all $b \in B$, there exists some $a_b \in A$ such that $f(a_b) = b$.

We use this formulation to define $g(b) = a_b$. Then $(f \circ g)(b) = f(g(b)) = f(a_b) = b$ for all $b \in B$.

Let $a \in A$ and let $b = f(a)$. We know that $b = f(a_b)$, hence $f(a) = f(a_b)$ which implies $a = a_b$, since f is injective.

Therefore, $(g \circ f)(a) = g(b) = a_b = a$, hence $(g \circ f)(a) = a$ for all $a \in A$.

For all $a \in A$, there exists $b \in B$ such that $g(b) = a$, namely $g(b) = a_b$. This follows from our earlier formulation of a_b. Hence, g is surjective.

Suppose $g(b) = g(b')$. Then, it follows that $a_b = a_{b'}$. We know that $a_b = a_{b'}$ implies $f(a_b) = f(a_{b'})$, i.e., $b = b'$. Hence, $b = b'$ follows from $g(b) = g(b')$, and g is injective.

Since g is both surjective and injective, we know that it is bijective. This completes the proof. QED

Definition 1.29. We say that two sets A and B are in *bijective correspondence* when there exists a bijection from A to B or, equivalently, from B to A.

Cardinality

Definition 1.30. Let $n \in \mathbb{N}$ be a natural number. We define $[n]$ to be the set $\{1, 2, \ldots, n\}$. Additionally, we define $[0] = \emptyset$.

Definition 1.31. A set A is *finite* if $A = \emptyset$ or if there exists a natural number n and a bijective correspondence between A and the set $[n]$. If A is not finite, we say that A is *infinite*.

Theorem 1.32. *Let $n, m \in \mathbb{N}$ with $n < m$.*
Then there does not exist an injective function $f : [m] \to [n]$.

Hint: Fix $k \in \mathbb{N}$. Prove, by induction on n, that for all $n \in \mathbb{N}$, there is no injective function $f : [n + k] \to [n]$.

Proof by Contradiction. Since $n, m \in \mathbb{N}$ and $m > n$, let $m = n + k$ for some $k \in \mathbb{N}$. We want to prove, by induction on n, that for all $n \in \mathbb{N}$, there is no injective function $f : [n + k] \to [n]$.

Consider the base case for $n = 1$. We want to show that there is no injective function $f : [1 + k] \to [1]$. We know that $[1 + k] = \{1, 2, \ldots, 1 + k\}$ and $[1] = \{1\}$. Since $k \in \mathbb{N}$, we have that $k > 0$, i.e., $k \geq 1$. Since there is only one element in the set $[1]$, any function $f\colon [1 + k] \to [1]$ must be defined by $f(x) = 1$ for all $x \in [1 + k]$.

Hence, by this definition, for all $x \in [1+k]$, $f(x) = f(x') = 1$ even if $x \neq x'$. We have an explicit counterexample, since $1, 2 \in [1 + k]$ and $f(1) = 1 = f(2)$. Therefore, there is no injective function $f : [1 + k] \to [1]$. This completes the base case.

Our inductive step is that we assume there is no injective function $g' : [n + k] \to [n]$, then we use this to show that there is no injective function $g : [n + k + 1] \to [n + 1]$. By contraposition, this is equivalent to saying that if there exists an injective function $g : [n + k + 1] \to [n + 1]$, then there exists an injective function $g' : [n + k] \to [n]$.

Hence, we begin by assuming that there exists an injective function $g : [n + k + 1] \to [n + 1]$.

Case 1: $\nexists a \in [n + k + 1]$ such that $g(a) = n + 1$. Then, define $g'\colon [n + k] \to [n]$ by $g'(x) = g(x)$. Then, if g is injective, so is g'.

Case 2: $\exists! a \in [n+k+1]$ such that $g(a) = n+1$. (Note: we know that any such a must be unique from our assumption that g is injective). Then, for all $x \in [n+k]$, define

$$g'(x) = \begin{cases} g(x), \text{if } x < a \\ g(x+1), \text{if } x \geq a \end{cases}$$

We first show that for all $x \in [n+k], g'(x) \in [n]$.

Case un: If $x < a$, i.e., $x \neq a$, then since g is injective, $g(x) \neq g(a) = n+1$, hence $g'(x) = g(x) \in [n]$.

Case deux: If $x \geq a$, i.e, $x+1 > a$ and $x+1 \neq a$, then since g is injective, $g(x+1) \neq g(a) = n+1$, hence $g'(x) = g(x+1) \in [n]$.

We now show that $g'(x)$ is injective. To do this, we take two elements $p, q \in [n+k]$ such that $p \neq q$, and we show that $g'(p) \neq g'(q)$.

Case one: $p, q < a$. In this case, $g'(p) = g(p)$ and $g'(q) = g(q)$. Since g is injective, if $p \neq q$, then $g(p) \neq g(q)$, hence $g'(p) \neq g'(q)$. Therefore, g' is injective.

Case two: $p < a$ and $q \geq a$. From these conditions, it follows that $q+1 > a > p$, hence $p \neq q+1$. In this case, $g'(p) = g(p)$ and $g'(q) = g(q+1)$. Since g is injective, if $p \neq q+1$, then $g(p) \neq g(q+1)$, hence $g'(p) \neq g'(q)$. Therefore, g' is injective.

Case three: $q < a$ and $p \geq a$. From these conditions, it follows that $p+1 > a > q$, hence $p+1 \neq q$. In this case, $g'(p) = g(p+1)$ and $g'(q) = g(q)$. Since g is injective, if $p+1 \neq q$, then $g(p+1) \neq g(q)$, hence $g'(p) \neq g'(q)$. Therefore, g' is injective.

Case four: $p, q \geq a$. In this case, $g'(p) = g(p+1)$ and $g'(q) = g(q+1)$. Since g is injective, if $p \neq q$, i.e., $p+1 \neq q+1$, then $g(p+1) \neq g(q+1)$, hence $g'(p) \neq g'(q)$. Therefore, g' is injective.

This completes the proof.

QED

The above proof is the one we did in class. I have also attempted another proof below, which I am not entirely sure is valid.

Direct Proof by Induction. Since $n, m \in \mathbb{N}$ and $m > n$, let $m = n+k$ for some $k \in \mathbb{N}$. We want to prove, by induction on n, that for all $n \in \mathbb{N}$, there is no injective function $f : [n+k] \to [n]$.

Consider the base case for $n = 1$. We want to show that there is no injective function $f : [1+k] \to [1]$. We know that $[1+k] = \{1, 2, \ldots, 1+k\}$ and $[1] = \{1\}$. Since $k \in \mathbb{N}$, we have that $k > 0$, i.e., $k \geq 1$. Since there is only one element in the set $[1]$, any function $f \colon [1+k] \to [1]$ must be defined by $f(x) = 1$ for all $x \in [1+k]$.

Hence, by this definition, for all $x \in [1+k], f(x) = f(x') = 1$ even if $x \neq x'$. We have an explicit counterexample, since $1, 2 \in [1+k]$ and $f(1) = 1 = f(2)$. Therefore, there is no injective function $f : [1+k] \to [1]$. This completes the base case.

Next, we want to show that if there is no injective function $f : [n+k] \to [n]$, then there is no injective function $f : [n+k+1] \to [n+1]$.

Since there is no injective function $f : \{1, 2, \ldots, n+k\} \to \{1, 2, \ldots, n\}$, this implies that for any function $f : \{1, 2, \ldots, n+k\} \to \{1, 2, \ldots, n\}$, there exist some $a, a' \in [n+k]$ such that $f(a) = f(a')$ but $a \neq a'$.

$[n+k] \subset [n+k+1]$ and $[n] \subset [n+1]$, hence for all $y \in [n+k], y \in [n+k+1]$ and for all $z \in [n], z \in [n+1]$.

Therefore, for any function $f : \{1, 2, \ldots, n+k+1\} \to \{1, 2, \ldots, n+1\}$, we know that there exist $a, a' \in [n+k+1]$ such that $f(a) = f(a')$ but $a \neq a'$, and this completes the inductive step.

This completes the proof.

QED

Theorem 1.33. *Let A be a finite set. Suppose that A is in bijective correspondence both with $[m]$ and with $[n]$. Then $m = n$.*

Proof. We prove this by contradiction. Assume $m \neq n$, and without loss of generality let $m = n+k$, where $k \in \mathbb{N}$.

Since A is in bijective correspondence with $[m]$, there exists a bijective function $f\colon A \to [m]$. Hence, there exists an inverse bijective function $f^{-1}\colon [m] \to A$.

Since A is in bijective correspondence with $[n]$, there exists a bijective function $g\colon A \to [n]$.

Then, $g \circ f^{-1}\colon [m] \to [n]$ must be a bijection. We know that $m = n + k$, hence this implies that there exists a bijection from $[n+k]$ to $[n]$.

We know that any function from $[n+k]$ to $[n]$ cannot be injective, hence there cannot be such a bijection. We have reached a contradiction, and this completes the proof.

QED

The preceding result allows us to make the following important definition.

Definition 1.34 (Cardinality of a finite set)**.** If A is a finite set that is in bijective correspondence with $[n]$, then we say that the *cardinality* of A is n, and we write $|A| = n$. (By Theorem 1.33, there is exactly one such natural number n.) We define the cardinality of the empty set to be 0.

Exercise 1.35. Let A and B be finite sets.

a) If $A \subset B$, then $|A| \leq |B|$.

   Proof. Suppose A is in bijective correspondence with $[p]$ and B is in bijective correspondence with $[q]$.

   Let $f\colon [p] \to A$ be an injection, and let $g\colon B \to [q]$ be an injection. Let $h\colon A \to B$ be defined by $h(x) = x$ for all $x \in A$. Hence, if $h(x) = h(x')$, then $x = x'$, so h is an injection.

   Theorem 1.32 says that if $m > n$, then there does not exist an injection from $[m]$ to $[n]$. The contrapositive is that if there exists an injection from $[m]$ to $[n]$, then $m \leq n$.

   Since h is an injection from A to B, we know that $|A| \leq |B|$. This completes the proof.

   QED

b) Let $A \cap B = \emptyset$. Then $|A \cup B| = |A| + |B|$.

   Proof. We want to show that if A is in bijective correspondence with $[p]$ and B is in bijective correspondence with $[q]$, then $A \cup B$ is in bijective correspondence with $[p+q]$.

   If $A \cap B = \emptyset$, then for all $a \in A$, $a \notin B$. Hence $A \cup B = \{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$.

   We know that $[q] = \{1, 2, \ldots, q\}$ is in bijective correspondence with $\{p+1, p+2, \ldots, p+q\}$.

   We know that the elements $\{a_1, a_2, \ldots, a_n\}$ are in bijective correspondence with $[p]$. The elements $\{b_1, b_2, \ldots, b_n\}$ are in bijective correspondence with $[q]$, and hence also with $\{p+1, p+2, \ldots, p+q\}$.

Hence, $A \cup B$ is in bijective correspondence with $\{1, 2, \ldots, p, p+1, p+2, \ldots, p+q\} = [p+q]$.

QED

c) $|A \cup B| + |A \cap B| = |A| + |B|$.

Proof. We rewrite the expression in terms of unions of disjoint sets, so that we can use the result from part b. Thus, $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$.

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

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

Then, the LHS is $|A \cup B| + |A \cap B| = |A \setminus B| + |B \setminus A| + 2 \cdot |A \cap B|$.

The RHS is $|A| + |B| = |A \setminus B| + |B \setminus A| + 2 \cdot |A \cap B|$. This completes the proof.

QED

d) $|A \times B| = |A| \cdot |B|$.

Proof. Let $n = |A|$. We prove this by induction on n. For the base case, let $n = 0$, i.e., $A = \emptyset$. Then, since there are no elements in A, we know that $A \times B = \emptyset$. Hence, $|A \times B| = 0 = 0 \cdot |B| = |A| \cdot |B| = n \cdot |B|$.

For the inductive step, we want to show that if $|A| = n+1$, then $|A \times B| = (n+1) \cdot |B|$.

Let $A' = A \setminus \{x\}$ for some $x \in A$. Then, $A \times B = (A' \times B) \cup (\{x\} \times B)$.

We know that $|A'| = n$, hence by the inductive hypothesis, $|A' \times B| = |A'| \cdot |B| = n \cdot |B|$.

Next, $|\{x\} \times B| = |\{x\}| \cdot |B| = 1 \cdot |B|$. Since $A' \cap \{x\} = \emptyset$, we know that $|A \times B| = |A' \times B| + |\{x\} \times B| = n \cdot |B| + 1 \cdot |B| = (n+1) \cdot |B|$. This completes the proof.

QED

Important Note: In future scripts you may assume basic properties of finite sets and methods of counting elements without having to refer back to the notions presented in this script.When $|A| = n$, we say that A contains n elements.

Definition 1.36. An set A is said to be *countable* either if it is finite if or if it is in bijective correspondence with $\mathbb{N}$. An infinite set that is not countable is called *uncountable*.

Exercise 1.37. Prove that $\mathbb{Z}$ is a countable set.

Proof. To prove that $\mathbb{Z}$ is a countable set, we must show that there exists a bijection between $\mathbb{Z}$ and $\mathbb{N}$. To do this, we construct a function $f : \mathbb{Z} \to \mathbb{N}$ and then show that it is bijective.

Let this function f be defined by

$$f(x) = \begin{cases} 1 & \text{if } x = 0, \\ 2x & \text{if } x > 0, \\ -2x + 1 & \text{if } x < 0. \end{cases}$$

First, we show that f is surjective. We know that $f(0) = 1$, so we need to show that $f(x)$ reaches every $n \in \mathbb{N}, n > 1$. All natural numbers greater than 1 are either even or odd. For all even natural numbers, we have that $n = f(\frac{n}{2})$. For all odd natural numbers, we have that $n = f(\frac{1-n}{2})$.

Next, we show that f is injective. By contraposition, we want to show that if $x \neq x'$, then $f(x) \neq f(x')$. We know that 0 is the only element in $\mathbb{Z}$ such that $f(x) = 1$. We also know that if $x > 0$ and $x' < 0$ or vice versa, then $f(x) \neq f(x')$. Finally, if $x, x' > 0$ and $x \neq x'$, then $2x \neq 2x'$. Similarly, if $x, x' < 0$ and $x \neq x'$, then $-2x + 1 \neq -2x' + 1$.

This completes the proof.

QED

Theorem 1.38. *Every subset of* $\mathbb{N}$ *is countable.*

Hint: when A *is an infinite subset of* $\mathbb{N}$*, construct a bijection* $f\colon \mathbb{N} \to A$ *inductively/recursively. This looks similar to a proof by induction: define an initial term (or terms) explicitly and then present a rule that defines* $f(n+1)$ *assuming that* $f(1), \ldots, f(n)$ *have already been defined. For example, the factorial of* n *is defined inductively by letting* $0! = 1$ *and*

$$(n+1)! = (n+1) \cdot n!$$

for $n \geq 0$*. After constructing your function you must verify that it is indeed a bijection.*

Proof. We prove this by contradiction. Assume there is some set $M \subset \mathbb{N}$ that is not countable.

Case 1: M is finite. In this case, let $q = |M|$. Then, we know that there is a bijective correspondence between M and $[q]$. Hence, M is countable and we have reached a contradiction.

Case 2: M is infinite, hence $M \neq \emptyset$. By the well-ordering principle, we know that every non-empty subset of $\mathbb{N}$ has a least element. Therefore, for any $K \subset \mathbb{N}$, let $j(K)$ denote the least element of K.

Then, let $f\colon \mathbb{N} \to M$ be defined by $f(1) = j(M)$ and for all $n \in \mathbb{N}, n \geq 1$,

$$f(n+1) = j(M \setminus \{f(1), f(2), \ldots, f(n)\}).$$

We want to show that f is bijective. We know that for all $m \in M$, there exists some subset $M_m \subset M$ such that $m = j(M_m)$. Then, we want to show that for all $m \in M$, there exists a unique $n \in \mathbb{N}$ such that $f(n) = m$. We demonstrate this by construction: for all $m \in M, n = 1 + |M \setminus M_m|$ is the unique element in $\mathbb{N}$ such that $f(n) = m$.

First, we show that $f(1 + |M \setminus M_m|) = m$. By the recursive definition of f, we know that $f(1 + |M \setminus M_m|) = j(M \setminus \{f(1), f(2), \ldots, f(|M \setminus M_m|)\} = m$.

Next, we show that this n is unique. Suppose there is some $n' \neq n$. Then, $f(n') = j(M \setminus \{f(1), f(2), \ldots, f(n'-1)\}$. Since $n' \neq n, \{f(1), f(2), \ldots, f(n'-1)\} \neq \{f(1), f(2), \ldots, f(n-1)\}$, hence $M \setminus \{f(1), f(2), \ldots, f(n'-1)\} \neq M \setminus \{f(1), f(2), \ldots, f(n-1)\}$, hence $j(M \setminus \{f(1), f(2), \ldots, f(n'-1)\}) \neq j(M \setminus \{f(1), f(2), \ldots, f(n-1)\})$. Therefore, $f(n') \neq f(n)$.

This completes the proof.

QED

Theorem 1.39. *If there exists an injection* $f : A \longrightarrow B$ *where* B *is countable, then* A *is countable. Hint: Use Theorem 1.38.*

Proof. Case 1: f is bijective. In this case, $|A| = |B|$, so if B is countable, then A is countable.

Case 2: f is not bijective, i.e., f is injective but not surjective. Then, there exists some element $b_0 \in B$ such that for all $a \in A, f(a) \neq b_0$. Hence, $|A| < |B|$.

Subcase one: If B is finite, and B is countable, then there exists a bijective correspondence from B to $[k]$ for some $k \in \mathbb{N}$. Then, we know that there exists a bijective correspondence from A to $[j]$ for some $j \in \mathbb{N}, j < k$. Hence, A is countable.

Subcase two: If B is infinite, and B is countable, then there exists a bijective correspondence $g\colon B \to \mathbb{N}$. Since $f\colon A \to B$ is an injection, we have that $g \circ f\colon A \to X$ is a bijection, where $X \subset \mathbb{N}$.

By Theorem 1.38, every subset of $\mathbb{N}$ is countable, hence X is countable. A is in bijective correspondence with X, therefore A is countable. This completes the proof.

QED

Corollary 1.40. *Every subset of a countable set is also countable.*

Proof. Let B be a countable set, and let $A \subset B$. Then, for all $a \in A, a \in B$.

Let $f\colon A \to B$ be defined by $f(n) = n$. If $f(n) = f(n')$, then $n = n'$, hence f is injective.

Since there exists an injection $f\colon A \to B$ and B is countable, A is also countable.

QED

Corollary 1.41. *If there exists a surjection $g\colon B \to A$ where B is countable, then A is countable. Hint: Use Theorem 1.39.*

Proof. Since B is countable, either there exists a bijective correspondence $f\colon B \to [n]$ or there exists a bijective correspondence $f\colon B \to \mathbb{N}$.

Since $g\colon B \to A$ is surjective, we know that for all $a \in A$, there exists $b_i \in B$ such that $g(b_i) = a$.

If A is finite, then we define $h\colon A \to [n]$. If A is infinite, then we define $h\colon A \to \mathbb{N}$. In both cases, for all $a \in A, h(a) = \min\{i \in \mathbb{N} \mid g(b_i) = a\}$.

We want to show that h is injective. Suppose $a, a' \in A$ are such that $h(a) = h(a')$. Then, $g(b_i) = a$ and $g(b_i) = a'$, so $a = a'$. Hence, h is injective and since both $[n]$ and $\mathbb{N}$ are countable, therefore A is countable.

QED

Exercise 1.42. Prove that $\mathbb{N} \times \mathbb{N}$ is countable by considering the function $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ given by $f(n, m) = (10^n - 1)10^m$.

(Alternatively you could use either one of the functions $g(n, m) = 2^n \cdot 3^m$ and $h(n, m) = \binom{n+m}{2} + n$.)

Proof. Let $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $g(n, m) = 2^n \cdot 3^m$.

Assume $n \neq n_0$, and without loss of generality suppose $n_0 < n$. We want to show that $g(n_0, m) \neq g(n, m)$.

Suppose $g(n_0, m) = g(n, m)$, i.e., $2^{n_0} \cdot 3^m = 2^n \cdot 3^m$. Then, dividing both sides by 2^{n_0}, we get $3^m = 2^{n-n_0} \cdot 3^m$. Since $n \neq n_0, n - n_0 \neq 0$, hence the LHS is odd while the RHS is even. Thus, we have reached a contradiction.

Similarly, assume $m \neq m_0$, and without loss of generality suppose $m_0 < m$. We want to show that $g(n, m_0) \neq g(n, m)$.

Suppose $g(n, m_0) = g(n, m)$, i.e., $2^n \cdot 3^{m_0} = 2^n \cdot 3^m$. Then, dividing both sides by 3^{m_0}, we get $2^n = 2^n \cdot 3^{m-m_0}$. Then, the RHS is divisible by 3 but the LHS is not. Thus, we have reached a contradiction.

Therefore, g is injective. By Theorem 1.39, there exists an injection $g\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ and $\mathbb{N}$ is countable. Therefore, $\mathbb{N}\times\mathbb{N}$ is countable.

QED

Additional Exercises

In all exercises you are expected to prove your answer, unless explicitly stated otherwise.

1. In each of the following, write out the elements of the sets.

   a) $(\{n\in\mathbb{Z}\mid \text{n is divisible by } 2\}\cap\mathbb{N})\cup\{-5\}$
   b) $\{F,G,H\}\times\{5,8,9\}$
   c) $\{[n]\mid n\in\mathbb{N}, 1\le n\le 3\}$
   d) $\{(x,y)\in\mathbb{N}\times\mathbb{N}\mid y=2x,\ x=2y\}$
   e) $(\{1,2\}\times\{1,2\})\times\{1,2\}$
   f) $(\{1,2\}\cup\{1,2\})\cup\{1,2\}$
   g) $\{1,2\}\cup\emptyset$
   h) $\{1,2\}\cap\emptyset$
   i) $\{1,2\}\cup\{\emptyset\}$
   j) $\{1,2\}\cap\{\emptyset\}$
   k) $\{\{a\}\cup\{b\}\mid a\in\mathbb{N}, b\in\mathbb{N}, 1\le a\le 4, 3\le b\le 5\}$
   l) $\{\{12\}\}\cup\{12\}$

2. Let A and B be subsets of the set X. The symmetric sum $A\oplus B$ (sometimes also called symmetric difference) of sets A and B is defined by

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

   Prove that

$$A\oplus B=(A\cup B)\cap[X\setminus(A\cap B)].$$

   Proof. We proceed by direct proof. By Theorem 1.7, $A\oplus B=(A\cup B)\cap[X\setminus(A\cap B)]$ if and only if $A\oplus B\subset(A\cup B)\cap[X\setminus(A\cap B)]$ and $(A\cup B)\cap[X\setminus(A\cap B)]\subset A\oplus B$.

   First, we want to show that $A\oplus B\subset(A\cup B)\cap[X\setminus(A\cap B)]$. Consider an element $y\in A\oplus B$. By the definition of the symmetric sum, $y\in\{x\in A\mid x\notin B\}\cup\{x\in B\mid x\notin A\}$, therefore either $y\in\{x\in A\mid x\notin B\}$ or $y\in\{x\in B\mid x\notin A\}$.

   In both cases, $y\in A\cup B$ and $y\in[X\setminus(A\cap B)]$. Since for all $y\in A\oplus B, y\in(A\cup B)\cap[X\setminus(A\cap B)]$, this shows that $A\oplus B\subset(A\cup B)\cap[X\setminus(A\cap B)]$.

   Next, we want to show that $(A\cup B)\cap[X\setminus(A\cap B)]\subset A\oplus B$. Consider an element $z\in(A\cup B)\cap[X\setminus(A\cap B)]$. Then, $z\in(A\cup B)$ and $z\in[X\setminus(A\cap B)]$.

$z \in (A \cup B)$ implies $z \in A$ or $z \in B$. $z \in [X \setminus (A \cap B)]$ implies $z \notin A \cap B$. Therefore, either $z \in A$ and $z \notin B$ in which case $z \in A \setminus B \subset A \oplus B$, or $z \in B$ and $z \notin A$ in which case $z \in B \setminus A \subset A \oplus B$.

Thus, for all $z \in (A \cup B) \cap [X \setminus (A \cap B)]$, $z \in A \oplus B$. Hence, $(A \cup B) \cap [X \setminus (A \cap B)] \subset A \oplus B$.

This completes the proof.

QED

3.

Definition 1.43. Let A be a set. The "power set" of A, denoted $\wp(A)$, is the set of all subsets of A; that is, $\wp(A) = \{B \mid B \subset A\}$.

(a) If A is a set, show that $\wp(A) \neq \emptyset$.

Proof. If A is any set, we know that $\emptyset \subset A$. Hence, $\emptyset \in \wp(A)$, therefore $\wp(A) \neq \emptyset$. QED

(b) Let $\emptyset$ be the empty set. Write down the elements of $\wp(\wp(\emptyset))$.
$\wp(\wp(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

4. Let A, B, C be subsets of $\mathbb{N}$. Extend Theorem 1.7 by showing that, for any $k \in \mathbb{N}$

$$A \subset A \cup B \cup C,$$
$$A \cap B \cap C \subset A.$$

Can this be extended to four sets A, B, C, D? What about five? Is there any limit?

5. (a) Set $A = \{1, 2\}$, $B = \{3, 4\}$, and $f = \{(a, b) \mid a \in A, b \in B\}$.
Write out the elements of f. Is f a function $A \to B$?

(b) Let $C = \{(1, 2), (2, 2), (3, 2)\}$.
Can C be a function? (For starters, what would A and B be?)

(c) Write out the elements of the set $D = \{(b, a) \mid (a, b) \in C\}$, where C is as given in b).
Can D be a function?

6. Take the sets $A = \{1, 2, 3\}$ and $B = \{1, 4, 9\}$. Consider the following four statements:

(a) For all $a \in A$, there is some $b \in B$ such that $a^2 = b$.

(b) There is some $b \in B$ such that, for all $a \in A$, $a^2 = b$.

(c) There is some $b \in B$ such that $a^2 = b$ for all $a \in A$.

(d) For all $a \in A$, $a^2 = b$ for some $b \in B$.

Each statement is equivalent to exactly one other in the list. Which statements are true? Which pairs are equivalent to each other?

7. Let $f : \mathbb{N} \to \mathbb{N}$ be given by $f(n) = n^3$.

(a) Is f surjective? Is f injective?

(b) Let $A \subset \mathbb{N}$ be the set $\{1, 2, \ldots, 30\}$. What is $f^{-1}(f(A))$? What is $f(f^{-1}(A))$?

8. Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $f(m, n) = mn$. Is f injective? Surjective? If $A \subset \mathbb{Z}$ is the set of even integers, what is $f^{-1}(A)$?

9. Let $f : A \to B$ and $g : B \to C$ be functions.

   (a) Suppose that f and $g \circ f$ are injective. Is g necessarily injective?

   Proof. No. For a counterexample, consider $A = \{1\}, B = \{p, q\}, C = \{x\}$. Let $f\colon A \to B$ be defined by $f(1) = p$ and let $g\colon B \to C$ be defined by $g(p) = g(q) = x$. Then both f and $g \circ f$ are injective, but g is not injective.

   More generally, let $B_0 \subset B$ be the image of f. Then, for every $b_0 \in B_0$, i.e., for every element of B that is reached by f, there exists a unique $a \in A$ such that $f(a) = b_0$.

   Similarly, let $C_0 \subset C$ be the image of $g \circ f$. Then, for every $c_0 \in C_0$, i.e., for every element of C that is reached by $g \circ f$, there exists a unique $a \in A$ such that $(g \circ f)(a) = c_0$.

   However, there could exist some $b' \in B, b' \notin B_0$ such that $g(b') = c_0$. Then $g(b_0) = g(b') = c_0$ and $b_0 \neq b'$. Hence, g is not necessarily injective.

   QED

   (b) Suppose that g and $g \circ f$ are injective. Is f necessarily injective?

   Proof. Let $x \neq y$. Then, since $g \circ f$ is injective, we know that $(g \circ f)(x) \neq (g \circ f)(y)$. Further, since g is injective, we know that $f(x) \neq f(y)$.

   Thus, $f(x) \neq f(y)$ follows from $x \neq y$, hence we know that f is necessarily injective.

   QED

   (c) Suppose that f and $g \circ f$ are surjective. Is g necessarily surjective?

   Proof. Yes. Since f is surjective, $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

   Since $g \circ f$ is surjective, $\forall c \in C, \exists a \in A$ such that $(g \circ f)(a) = g(f(a)) = c$.

   Assume g is not surjective. Then, there exists some $c_0 \in C$ such that for all $b \in B$, $g(b) \neq c_0$.

   We know that there exists some $a_0 \in A$ such that $(g \circ f)(a_0) = c_0$, and $f(a_0) = b_0$. Hence, $g(b_0) = c_0$ and we have reached a contradiction.

   QED

   (d) Suppose that g and $g \circ f$ are surjective. Is f necessarily surjective?

   Proof. No. For a counterexample, consider $A = \{1\}, B = \{p, q\}, C = \{x\}$. Let $f\colon A \to B$ be defined by $f(1) = p$ and let $g\colon B \to C$ be defined by $g(p) = g(q) = x$. Then both g and $g \circ f$ are surjective, but f is not surjective.

   QED

10. Let $f : A \longrightarrow B$ be a function. Let $X \subset A$ and $Y \subset B$.

    (a) Prove that if f is surjective then $f(f^{-1}(Y)) = Y$.

Proof. If f is surjective, we know that for all $b \in B$, there exists some $a \in A$ such that $f(a) = b$. To denote this, for all $i \in \mathbb{N}, i \leq |B|$, let a_i correspond to b_i by the relation $f(a_i) = b_i$.

Let $Y \subset B = \{b_1, b_2, \ldots, b_n\}$, then we have that $f^{-1}(Y) = \{a_1, a_2, \ldots, a_n\}$. Hence, $f(f^{-1}(Y)) = \{b_1, b_2, \ldots, b_n\} = Y$.

QED

(b) Prove that if f is injective then $f^{-1}(f(X)) = X$.

Proof. If f is injective, we know that $f(a) = f(a')$ implies $a = a'$.

Let $X \subset A = \{a_1, a_2, \ldots, a_n\}$. Since f is one-to-one, we know that the number of elements in $f(X)$ must be the same as the number of elements in X, i.e., $|f(X)| = |X|$. Hence, let $f(X) = \{b_1, b_2, \ldots, b_n\}$.

Assume $b_i, b_k \in f(X)$ and $b_i = b_k$, i.e., $f(a_i) = f(a_k)$. Then, since f is injective, $a_i = a_k$. Since f is a function, any particular $a_i \in X$ cannot map to two or more different $b_i \in f(X)$. Since f is injective, for every $b_i \in f(X), \exists! a_i \in X$ such that $f(a_i) = b_i$. Hence, we know that $f^{-1}(f(X)) = \{a_1, a_2, \ldots, a_n\} = X$.

QED

(c) Are the converse statements also true? i.e. If $f(f^{-1}(Y))) = Y$ for all subsets $Y \subset B$, must f be surjective? If $f^{-1}(f(X)) = X$ for all subsets $X \subset A$, must f be injective?

Proof. Yes. Both the converse statements are true. We prove them by contraposition.

In the first case, we assume that f is not surjective, and then show that there exists some $Y \subset B$ such that $f(f^{-1}(Y))) \neq Y$. We present a demonstration by counterexample.

Let $A = \{1\}, B = \{p, q\}, Y = \{p, q\}$, and let $f \colon A \to B$ be defined by $f(1) = p$. Since $\neg\exists a \in A$ such that $f(a) = q$, f is not surjective. Then, $f^{-1}(Y) = \{1\}$ and $f(f^{-1}(Y)) = f(1) = p \neq Y$.

In the second case, we assume that f is not injective, and then show that there exists some $X \subset A$ such that $f^{-1}(f(X)) \neq X$. We present a demonstration by counterexample.

Let $A = \{1, 2\}, B = \{p\}, X = \{1\}$, and let $f \colon A \to B$ be defined by $f(1) = p, f(2) = p$. Then $f(X) = f(1) = p$ and $f^{-1}(f(X)) = f^{-1}(p) = \{1, 2\} \neq X$.

QED

11. Let $f : A \longrightarrow B$ be a bijection. Let g be the inverse function to f, given by Proposition 1.27. Let $Y \subset B$. Show that $g(Y) = f^{-1}(Y)$.

Note: $g(Y)$ denotes the image of Y under the map g and $f^{-1}(Y)$ denotes the preimage of Y under f. Thus when $g = f^{-1}$ exists as a function, the two possible interpretations of $f^{-1}(Y)$ coincide.

Proof. Define $g \colon B \to A$ as $g(b) = a_b$ for all $b \in B$, where a_b is the unique element of A such that $f(a_b) = b$.

Let $Y \subset B = \{b_1, b_2, \ldots, b_n\}$, then we have that the preimage $f^{-1}(Y) = \{a_{b1}, a_{b2}, \ldots, a_{bn}\}$.

By the definition of g, the image of Y under the map g is $g(Y) = a_b$ for all $b \in Y$. Hence, $g(Y) = \{a_{b1}, a_{b2}, \ldots, a_{bn}\}$.

This completes the proof.

QED

12. Recall the definition of power set, Definition 1.43.

(a) Let A be any set. Show that there is no bijection between A and its power set $\wp(A)$. (Hint: If $f : A \to \wp(A)$ is any function, think about the set $B = \{a \in A \mid a \notin f(a)\} \subset A$.)

Proof. We prove this by contradiction. Assume that there exists a bijection $f : A \to \wp(A)$. We show that f cannot be surjective.

Let $B \subset A$ be defined by $B = \{a \in A \mid a \notin f(a)\}$. Then, $B \in \wp(A)$.

If f is surjective, then for all $Y \in \wp(A)$, there exists some $a \in A$ such that $f(a) = Y$. We want to show that there exists some $Y_0 \in \wp(A)$ such that for all $a \in A, f(a) \neq Y_0$.

Let $Y_0 = B$. Assume that there exists some $a_0 \in A$ such that $f(a_0) = B$.

If $a_0 \in B$, then by definition $a_0 \notin f(a_0)$, hence $f(a_0) \neq B$. If $a_0 \notin B$, then by definition $a_0 \in f(a_0)$, hence $f(a_0) \neq B$.

Therefore, f is not surjective, hence it is not bijective. This completes the proof.

QED

The above is my official submission for the homework assignment. Out of curiosity, I have attempted another proof, which I am not sure is fully valid/rigorous.

Second Proof Attempt. Assume that there exists a bijection $f \colon A \to \wp(A)$. Then, there must exist a bijection $g \colon \wp(A) \to A$, i.e., g must be both injective and surjective. We show that g cannot be injective using the fact that for all $j, k \in \mathbb{N}$, there does not exist an injection from $[j + k]$ to $[j]$.

Let $|A| = k$, then we know that there exists a bijection $h \colon A \to [k]$.

By definition, $\wp(A)$ is the set of all subsets of A. Hence, for all $a \in A$, and for all $A' \in \wp(A)$, either $a \in A'$ or $a \notin A'$. Therefore, $|\wp(A)| = 2^{|A|}$.

In Script 0, we showed that $(1 + x)^n \geq 1 + nx$ for all $x > -1, n \in \mathbb{N}$. Substituting $x = 1$, we get that $2^n \geq 1 + n$ for all $n \in \mathbb{N}$. Hence, $2^{|A|} \geq 1 + |A|$. Therefore, $|\wp(A)| \geq 1 + |A|$, i.e, there exists some bijection $q \colon \wp(A) \to [1 + k]$. Hence, there also exists some bijection $q' \colon [1 + k] \to \wp(A)$.

Therefore, if $g \colon \wp(A) \to A$ is bijective, then $h \circ g \colon \wp(A) \to [k]$ must be bijective.

Hence, $h \circ g \circ q' \colon [1 + k] \to [k]$ must be bijective. We know that $h \circ g \circ q'$ cannot be injective, hence it cannot be bijective.

We have reached a contradiction, and this completes the proof.

QED

(b) Show that there is no injective map from $\wp(\mathbb{N})$ to $\mathbb{N}$.

Proof. Let $g\colon \wp(A) \to A$ be a function. We show that g cannot be injective using the fact that for all $j, k \in \mathbb{N}$, there does not exist an injection from $[j+k]$ to $[j]$.

Let $|A| = k$, then we know that there exists a bijection $h\colon A \to [k]$.

By definition, $\wp(A)$ is the set of all subsets of A. Hence, for all $a \in A$, and for all $A' \in \wp(A)$, either $a \in A'$ or $a \notin A'$. Therefore, $|\wp(A)| = 2^{|A|}$.

In Script 0, we showed that $(1+x)^n \geq 1 + nx$ for all $x > -1, n \in \mathbb{N}$. Substituting $x = 1$, we get that $2^n \geq 1 + n$ for all $n \in \mathbb{N}$. Hence, $2^{|A|} \geq 1 + |A|$. Therefore, $|\wp(A)| \geq 1 + |A|$, i.e, there exists some bijection $q\colon \wp(A) \to [1+k]$. Hence, there also exists some bijection $q'\colon [1+k] \to \wp(A)$.

Therefore, if $g\colon \wp(A) \to A$ is injective, then $h \circ g\colon \wp(A) \to [k]$ must be injective (since h is bijective).

Hence, $h \circ g \circ q'\colon [1+k] \to [k]$ must be injective (since q' is bijective). We have reached a contradiction, and this completes the proof.

QED

13. Let A be a set with cardinality n. Let $f\colon [n] \longrightarrow A$ be a bijection. Show that $A = \{f(1), f(2), \cdots, f(n)\}$ and deduce that we can write $A = \{a_1, a_2, \cdots, a_n\}$.

14. Let $f : A \to B$ be a function.

    (a) Let X and Y be subsets of A. Is it true that $f(X \cup Y) = f(X) \cup f(Y)$? Is it true that $f(X \cap Y) = f(X) \cap f(Y)$? Either prove or give a counterexample in each case.

    Proof for Unions. Suppose $m \in f(X \cup Y)$. Then, $m = f(k)$ for some $k \in X \cup Y$. If $k \in X$, then $m \in f(X)$. If $k \in Y$, then $m \in f(Y)$. Therefore, $m \in f(X) \cup f(Y)$. Hence, $f(X \cup Y) \subset [f(X) \cup f(Y)]$.

    Suppose $m \in f(X) \cup f(Y)$. If $m \in f(X)$, then $m = f(k)$ for some $k \in X$, i.e., $m = f(k)$ for some $k \in X \cup Y$, hence $m \in f(X \cup Y)$. If $m \in f(Y)$, then $m = f(k)$ for some $k \in Y$, i.e., $m = f(k)$ for some $k \in X \cup Y$, hence $m \in f(X \cup Y)$. Hence, $[f(X) \cup f(Y)] \subset f(X \cup Y)$. Therefore, $f(X \cup Y) = f(X) \cup f(Y)$.

    QED

    Proof for Intersections. We present a counterexample. Let $A = \{1, 2\}, B = \{p\}$. Let $X \subset A, Y \subset A$ be defined by $X = \{1\}, Y = \{2\}$.

    Then, $X \cap Y = \emptyset$, therefore $f(X \cap Y) = \emptyset$.

    $f(X) = f(Y) = \{p\}$, hence $f(X) \cap f(Y) = \{p\}$.

    $\{p\} \neq \emptyset$. This completes the proof by counterexample.

    QED

    (b) Now let X and Y be subsets of B. Is it true that $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$? Is it true that $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$? Either prove or give a counterexample in each case.

    Proof for Unions. Suppose $m \in f^{-1}(X \cup Y)$. Then, $f(m) \in X \cup Y$. If $f(m) \in X$, then $m \in f^{-1}(X)$, hence $m \in f^{-1}(X) \cup f^{-1}(Y)$. If $f(m) \in Y$, then $m \in f^{-1}(Y)$, hence $m \in f^{-1}(X) \cup f^{-1}(Y)$. Hence, $f^{-1}(X \cup Y) \subset [f^{-1}(X) \cup f^{-1}(Y)]$.

Suppose $m \in f^{-1}(X) \cup f^{-1}(Y)$. If $m \in f^{-1}(X)$, then $f(m) \in X$, hence $f(m) \in X \cup Y$, therefore $m \in f^{-1}(X \cup Y)$. If $m \in f^{-1}(Y)$, then $f(m) \in Y$, hence $f(m) \in X \cup Y$, therefore $m \in f^{-1}(X \cup Y)$. Hence, $[f^{-1}(X) \cup f^{-1}(Y)] \subset f^{-1}(X \cup Y)$.
Therefore, $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

QED

Proof for Intersections. Suppose $m \in f^{-1}(X \cap Y)$. Then, $f(m) \in X \cap Y$, i.e., $f(m) \in X$ and $f(m) \in Y$. Hence, $m \in f^{-1}(X)$ and $m \in f^{-1}(Y)$, therefore $m \in f^{-1}(X) \cap f^{-1}(Y)$. Hence, $f^{-1}(X \cap Y) \subset [f^{-1}(X) \cap f^{-1}(Y)]$.
Suppose $m \in f^{-1}(X) \cap f^{-1}(Y)$. Then, $m \in f^{-1}(X)$ and $m \in f^{-1}(Y)$. Hence, $f(m) \in X$ and $f(m) \in Y$, so $f(m) \in X \cap Y$. Therefore, $m \in f^{-1}(X \cap Y)$. Hence, $[f^{-1}(X) \cap f^{-1}(Y)] \subset f^{-1}(X \cap Y)$.
Therefore, $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.

QED

15. Suppose that $A, B \subset \mathbb{N}$. Prove that if A and B are finite and there is a bijection $f : A \to B$, then $|A| = |B|$.

16. Prove that there is no set A with maximal cardinality. In other words, show that there does not exist a set A with the property that if B is a set, then B has smaller cardinality than A.

17. a) Let X be a countable set and Y a finite set such that $X \cap Y = \emptyset$. Show that $X \cup Y$ is countable.

Proof. Case 1: X is finite. Then, let $a = |X|$ and $b = |Y|$, then we know that $|X \cup Y| = a + b$. Let $c \in \mathbb{N}, c = a + b$, then we know that $X \cup Y$ is countable since there exists a bijection from $X \cup Y$ to $[c]$.
Case 2: X is infinite. We know that there exists a bijection $f\colon X \to \mathbb{N}$ and there exists a bijection from Y to $[b]$, where $b = |Y|$. Then, define $g\colon X \cup Y \to \mathbb{N}$ by

$$g(x) = \begin{cases} i, \text{for } x_i \in Y \\ f(x_j) + b, \text{for } x_j \notin Y. \end{cases}$$

for all $x \in X \cup Y$. (Note: we know that $X \cap Y = \emptyset$, hence $\forall i, \forall j, x_i \neq x_j$.)
We first show that g is surjective. For all $n \in \mathbb{N}$, there exists an $x_n \in X \cup Y$ such that $g(x_n) = n$. This is given by

$$x_n = \begin{cases} x_{i=n} \text{ if } n \leq b \\ f^{-1}(n-b), \text{if } n > b. \end{cases}$$

Next, we show that g is injective.
Case 1: $x_i, x_{i'} \in Y, x_i \neq x_{i'}$. Then, $g(x_i) = i \neq i' = g(x_{i'})$.
Case 2: $x_j, x_{j'} \notin Y, x_j \neq x_{j'}$. Then, since f is injective, $f(x_j) \neq f(x_{j'})$, hence $f(x_j) + b \neq f(x_{j'}) + b$, therefore $g(x_j) \neq g(x_{j'})$.
Case 3: $x_i \in Y, x_j \notin Y$ (it follows that $x_i \neq x_j$). Then, $g(x_i) = i \leq b$ while $g(x_j) = f(x_j) + b > b$, therefore $g(x_i) \neq g(x_j)$.
This completes the proof.

QED

b) Prove that a union of 2 disjoint countable sets is countable.

Proof. Let $X \cap Y = \emptyset$ where X and Y are countable. Then, we want to show that $X \cup Y$ is countable.
Case 1: if X, Y are finite, then $|X \cup Y| = |X| + |Y|$, hence $X \cup Y$ is countable.
Case 2: if X is finite and Y is countable or vice versa, then by part a), $X \cup Y$ is countable.
Case 3: if X, Y are infinite and countable, then we know that there exists a bijection $f\colon X \to \mathbb{N}$ and there exists a bijection $g\colon Y \to \mathbb{N}$.
Then, we define $h\colon X \cup Y \to \mathbb{N}$ as

$$h(m) = \begin{cases} (2 \cdot f(m)) - 1 \text{ if } m \in X \\ 2 \cdot g(m), \text{if } m \in Y. \end{cases}$$

First, we show that h is surjective. For all $n \in \mathbb{N}$,

$$n = \begin{cases} h(m_i) \text{ such that } m \in Y, i = \frac{n}{2} \text{ if } n \text{ is even} \\ h(m_j) \text{ such that } m \in X, j = \frac{n+1}{2} \text{ if } n \text{ is odd.} \end{cases}$$

Next, we show that h is injective.
Case 1: $m \in Y, m' \in X$, then $h(m)$ is even and $h(m')$ is odd, hence $h(m) \neq h(m')$.
Case 2: $m \in Y, m' \in Y, m \neq m'$. Then, $h(m) = 2 \cdot g(m) \neq 2 \cdot g(m') = h(m')$ since g is injective.
Case 3: $m \in X, m' \in X, m \neq m'$. Then, $h(m) = (2 \cdot f(m)) - 1 \neq (2 \cdot f(m')) - 1 = h(m')$ since f is injective.
This completes the proof.

QED

c) Use a) and b) to prove that $\mathbb{Z}$ is countable.

Proof. Let $\mathbb{N}_0 = \{-1, -2, -3, \dots\}$ be the set of negative integers. Then, we know that $\mathbb{N}_0$ is countable, since there exists a bijection $f\colon \mathbb{N}_0 \to \mathbb{N}$ defined as $f(n) = -n$ for all $n \in \mathbb{N}_0$.
We also know that $\mathbb{Z} = \mathbb{N} \cup \mathbb{N}_0 \cup \{0\}$.
By part a), $\mathbb{N}_0$ is countable and $\{0\}$ is finite, and they are disjoint, hence $\mathbb{N}_0 \cup \{0\}$ is countable.
By part b), $\mathbb{N}$ is countable and $\mathbb{N}_0 \cup \{0\}$ is countable, and they are disjoint, hence $\mathbb{N} \cup \mathbb{N}_0 \cup \{0\}$ is countable. Therefore, $\mathbb{Z}$ is countable.

QED

d) Suppose that $A_1, A_2, \dots$ are sets such that A_i is countable for each $i \in \mathbb{N}$. Show that, for each n,

$$\bigcup_{i=1}^{n} A_i$$

is countable.

Proof. Case 1: $n = 1$, i.e., $\bigcup_{i=1}^n A_i = \bigcup_{i=1}^1 A_i = A_1$. Then, by definition, A_1 is countable.
Case 2: $n > 1$. First, we rewrite this to construct a finite union of disjoint countable sets, so that we can use the result from part b) by induction on n.
Let $C = \bigcap_{i=1}^n A_i$, then we know that C is countable. Then, $\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n (A_i \setminus C) \cup C$.
By part b), we know that if $\bigcup_{i=1}^n (A_i \setminus C)$ is countable, then so is $\bigcup_{i=1}^n (A_i \setminus C) \cup C$.
For all $i \geq 1, i \leq n$, let $A_i \setminus C$ be denoted by M_i. Hence, we want to show that $\bigcup_{i=1}^n M_i$ is countable, where each M_i is countable and $\bigcap_{i=1}^n M_i = \emptyset$.
We prove this by induction on n. By part b), the base case is true for $n = 2$.
Next, we want to show that if $\bigcup_{i=1}^n M_i$ is countable, then $\bigcup_{i=1}^{n+1} M_i$ is countable.
We know that $\bigcup_{i=1}^{n+1} M_i = \bigcup_{i=1}^n M_i \cup M_{n+1}$. By the inductive hypothesis, $\bigcup_{i=1}^n M_i$ is countable and M_{n+1} is countable, hence by part b), $\bigcup_{i=1}^{n+1} M_i$ is countable.
This completes the proof.

QED

e) Prove that a countable union of countable sets is countable. That is, if $\{A_i\}_{i\in\mathbb{N}}$ is a countable collection of countable sets, then

$$\bigcup_{i\in\mathbb{N}} A_i$$

is countable.

Proof. Let the countable sets A_i be indexed by i and let the elements of each of the countable sets A_i be indexed by j. Then, every element in the countable union of countable sets (i.e., every element in $\bigcup_{i\in\mathbb{N}} A_i$) can be specified as a_{ij} (i.e., the jth element of the ith set). For example, $A_1 = \{a_{11}, a_{12}, a_{13}, \dots\}$.
Let $M = \bigcup_{i\in\mathbb{N}} A_i$, then it suffices to show that there exists an injection $f\colon M \to \mathbb{N} \times \mathbb{N}$, since we know that $\mathbb{N} \times \mathbb{N}$ is countable.
For all $m \in M$, let $f(m) = (i, j)$. We want to show that f is injective.
Case 1: $m, m' \in A_i, m \neq m'$. It follows that $m = a_{ij}$ and $m' = a_{ij'}$ for some j, j'. Then, $f(m) = (i, j) \neq (i, j') = f(m')$.
Case 2: $m \in A_i, m' \in A_{i'}$. It follows that $m \neq m'$. We know that $m = a_{ij}$ and $m' = a_{i'j'}$.
Subcase 2a: $j = j'$. Then, $f(m) = (i, j) \neq (i', j) = f(m')$.
Subcase 2b: $j \neq j'$. Then, $f(m) = (i, j) \neq (i', j') = f(m')$.
Therefore, f is injective and this completes the proof.

QED

f) Prove that if A and B are countable then $A \times B$ is countable.

Proof. We know that there exists a bijection $f\colon A \to \mathbb{N}$ and there exists a bijection $g\colon B \to \mathbb{N}$.
Then, define $h\colon A \times B \to \mathbb{N} \times \mathbb{N}$ by $h(a, b) = (f(a), g(b))$. We know that $\mathbb{N} \times \mathbb{N}$ is countable, hence it suffices to show that h is injective.

Suppose $a \neq a'$, then $h(a,b) = (f(a), g(b)) \neq (f(a'), g(b)) = h(a', b)$ since f is injective. Analogously, suppose $b \neq b'$, then $h(a,b) = (f(a), g(b)) \neq (f(a), g(b')) = h(a, b')$ since g is injective.

Similarly, if $a \neq a'$ and $b \neq b'$, then $f(a) \neq f(a')$ and $g(b) \neq g(b')$, therefore $h(a,b) = (f(a), g(b)) \neq (f(a'), g(b')) = h(a', b')$.

Therefore, h is injective and this completes the proof.

QED

g) Prove that if $A_1, A_2, \cdots, A_n$ are countable, then so is $A_1 \times A_2 \times \cdots \times A_n$.

Proof. We prove this by induction on n.

For the base case, we want to show that if A_1 and A_2 are countable, then so is $A_1 \times A_2$. This is established in part f).

For the inductive step, we want to show that if $A_1 \times A_2 \times \cdots \times A_n$ is countable and A_{n+1} is countable, then $A_1 \times A_2 \times \cdots \times A_n \times A_{n+1}$ is countable.

Let $M = A_1 \times A_2 \times \cdots \times A_n$, where M is countable. By part f), if A_{n+1} is countable, then $M \times A_{n+1}$ is countable.

This completes the proof.

QED

h) Let $A_n = \{0, 1\}$, for every n. Show that $A_1 \times A_2 \times \cdots \times A_n \times \cdots$ is uncountable.

Proof. We know that $\wp(\mathbb{N})$ is uncountable, hence it suffices to show that there exists a bijection $f\colon A_1 \times A_2 \times \cdots \times A_n \times \cdots \to \wp(\mathbb{N})$. We prove this by induction on n.

Define $f_n\colon A_1 \times A_2 \times \cdots \times A_n \to \wp([n])$ as $f_n(a_i) = \{i \in [n] \mid a_i = 1\}$.

(Side note: The intuition behind this formalism is that every element of $\wp(\mathbb{N})$ is mapped by the string of the ordered pair such that if the ith element of the ordered pair is 0, that element is not in $L \subset \mathbb{N}, L \in \wp(\mathbb{N})$; and if the ith element of the ordered pair is 1, that element is in $L \subset \mathbb{N}, L \in \wp(\mathbb{N})$. Here, I use the term ordered pair even though it has more than 2 elements and so is not strictly speaking a pair).

For the base case, $f_2\colon A_1 \times A_2 \to \wp([2])$. Then, $f_2(0,0) = \varnothing, f_2(0,1) = \{2\}, f_2(1,0) = \{1\}, f_2(1,1) = \{1,2\}$. Hence, f is bijective.

For the inductive step, we want to show that if $f_n\colon A_1 \times A_2 \times \cdots \times A_n \to \wp([n])$ is bijective, then $f_{n+1}\colon A_1 \times A_2 \times \cdots \times A_{n+1} \to \wp([n+1])$ is bijective.

We note that $f_{n+1}(a_i) = \{i \in [n+1] \mid a_i = 1\}$.

Case 1: $a_{n+1} = 0$. Then, $f_{n+1}(a) = f_n(a)$ for all $a \in A_1 \times A_2 \times \cdots \times A_{n+1}$. Hence, if f_n is bijective then f_{n+1} is bijective.

Case 2: $a_{n+1} = 1$. Then, $f_{n+1}(a) = \{f_n(a) \cup a_{n+1}\}$ for all $a \in A_1 \times A_2 \times \cdots \times A_{n+1}$. Hence, if f_n is bijective then f_{n+1} is bijective.

This completes the proof.

QED