

Chapter 2: Injective and Surjective Functions and Cardinality

2.1 Definition: Let X and Y be sets and let $f : X \rightarrow Y$. Recall that the **domain** of f and the **range** of f are the sets

$$\text{Domain}(f) = X, \text{ Range}(f) = f(X) = \{f(x) \mid x \in X\}.$$

For $A \subseteq X$, the **image** of A under f is the set

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

For $B \subseteq Y$, the **inverse image** of B under f is the set

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

2.2 Definition: Let X , Y and Z be sets, let $f : X \rightarrow Y$ and let $g : Y \rightarrow Z$. We define the **composite** function $g \circ f : X \rightarrow Z$ by $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

2.3 Definition: We say that f is **injective** (or **one-to-one**, written as $1:1$) when for every $y \in Y$ there exists at most one $x \in X$ such that $f(x) = y$. Equivalently, f is injective when for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$. We say that f is **surjective** (or **onto**) when for every $y \in Y$ there exists at least one $x \in X$ such that $f(x) = y$. Equivalently, f is surjective when $\text{Range}(f) = Y$. We say that f is **bijective** (or **invertible**) when f is both injective and surjective, that is when for every $y \in Y$ there exists exactly one $x \in X$ such that $f(x) = y$. When f is bijective, we define the **inverse** of f to be the function $f^{-1} : Y \rightarrow X$ such that for all $y \in Y$, $f^{-1}(y)$ is equal to the unique element $x \in X$ such that $f(x) = y$. Note that when f is bijective so is f^{-1} , and in this case we have $(f^{-1})^{-1} = f$.

2.4 Theorem: Let $f : X \rightarrow Y$ and let $g : Y \rightarrow Z$. Then

- (1) if f and g are both injective then so is $g \circ f$,
- (2) if f and g are both surjective then so is $g \circ f$, and
- (3) if f and g are both invertible then so is $g \circ f$, and in this case $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof: To prove Part (1), suppose that f and g are both injective. Let $x_1, x_2 \in X$. If $g(f(x_1)) = g(f(x_2))$ then since g is injective we have $f(x_1) = f(x_2)$, and then since f is injective we have $x_1 = x_2$. Thus $g \circ f$ is injective.

To prove Part (2), suppose that f and g are surjective. Given $z \in Z$, since g is surjective we can choose $y \in Y$ so that $g(y) = z$, then since f is surjective we can choose $x \in X$ so that $f(x) = y$, and then we have $g(f(x)) = g(y) = z$. Thus $g \circ f$ is surjective.

Finally, note that Part (3) follows from Parts (1) and (2).

2.5 Definition: For a set X , we define the **identity function** on X to be the function $I_X : X \rightarrow X$ given by $I_X(x) = x$ for all $x \in X$. Note that for $f : X \rightarrow Y$ we have $f \circ I_X = f$ and $I_Y \circ f = f$.

2.6 Definition: Let X and Y be sets and let $f : X \rightarrow Y$. A **left inverse** of f is a function $g : Y \rightarrow X$ such that $g \circ f = I_X$. Equivalently, a function $g : Y \rightarrow X$ is a left inverse of f when $g(f(x)) = x$ for all $x \in X$. A **right inverse** of f is a function $h : Y \rightarrow X$ such that $f \circ h = I_Y$. Equivalently, a function $h : Y \rightarrow X$ is a right inverse of f when $f(h(y)) = y$ for all $y \in Y$.

2.7 Theorem: Let X and Y be nonempty sets and let $f : X \rightarrow Y$. Then

- (1) f is injective if and only if f has a left inverse,
- (2) f is surjective if and only if f has a right inverse, and
- (3) f is bijective if and only if f has a left inverse g and a right inverse h , and in this case we have $g = h = f^{-1}$.

Proof: To prove Part (1), suppose first that f is injective. Since $X \neq \emptyset$ we can choose $a \in X$ and then define $g : Y \rightarrow X$ as follows: if $y \in \text{Range}(f)$ then (using the fact that f is 1:1) we define $g(y)$ to be the unique element $x_y \in X$ with $f(x_y) = y$, and if $y \notin \text{Range}(f)$ then we define $g(y) = a$. Then for every $x \in X$ we have $y = f(x) \in \text{Range}(f)$, so $g(y) = x_y = x$, that is $g(f(x)) = x$. Conversely, if f has a left inverse, say g , then f is 1:1 since for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$.

To prove Part (2), suppose first that f is onto. For each $y \in Y$, choose $x_y \in X$ with $f(x_y) = y$, then define $g : X \rightarrow Y$ by $g(y) = x_y$ (we need the Axiom of Choice for this). Then g is a right inverse of f since for every $y \in Y$ we have $f(g(y)) = f(x_y) = y$. Conversely, if f has a right inverse, say g , then f is onto since given any $y \in Y$ we can choose $x = g(y)$ and then we have $f(x) = f(g(y)) = y$.

To prove Part (3), suppose first that f is bijective. The inverse function $f^{-1} : Y \rightarrow X$ is a left inverse for f because given $x \in X$ we can let $y = f(x)$ and then $f^{-1}(y) = x$ so that $f^{-1}(f(x)) = f^{-1}(y) = x$. Similarly, f^{-1} is a right inverse for f because given $y \in Y$ we can let x be the unique element in X with $y = f(x)$ and then we have $x = f^{-1}(y)$ so that $f(f^{-1}(y)) = f(x) = y$. Conversely, suppose that g is a left inverse for f and h is a right inverse for f . Since f has a left inverse, it is injective by Part (1). Since f has a right inverse, it is surjective by Part (2). Since f is injective and surjective, it is bijective. As shown above, the inverse function f^{-1} is both a left inverse and a right inverse. Finally, note that $g = f^{-1} = h$ because for all $y \in Y$ we have

$$g(y) = g(f(f^{-1}(y))) = f^{-1}(y) = f^{-1}(f(h(y))) = h(y).$$

2.8 Corollary: Let X and Y be sets. Then there exists an injective map $f : X \rightarrow Y$ if and only if there exists a surjective map $g : Y \rightarrow X$.

Proof: Suppose $f : X \rightarrow Y$ is an injective map. Then f has a left inverse. Let g be a left inverse of f . Since $g \circ f = I_X$, we see that f is a right inverse of g . Since g has a right inverse, g is surjective. Thus there is a surjective map $g : Y \rightarrow X$. Similarly, if $g : Y \rightarrow X$ is surjective, then it has a right inverse $f : X \rightarrow Y$ which is injective.

2.9 Definition: Let A and B be sets. We say that A and B have the **same cardinality**, and we write $|A| = |B|$, when there exists a bijective map $f : A \rightarrow B$ (or equivalently when there exists a bijective map $g : Y \rightarrow X$). We say that the cardinality of A is **less than or equal to** the cardinality of B , and we write $|A| \leq |B|$, when there exists an injective map $f : A \rightarrow B$ (or equivalently when there exists a surjective map $g : Y \rightarrow X$). We say that the cardinality of A is **less than** the cardinality of B , and we write $|A| < |B|$, when $|A| \leq |B|$ and $|A| \neq |B|$, (that is when there exists an injective map $f : A \rightarrow B$ but there does not exist a bijective map $g : A \rightarrow B$). We also write $|A| \geq |B|$ when $|B| \leq |A|$ and $|A| > |B|$ when $|B| < |A|$.

2.10 Example: The map $f : \mathbf{N} \rightarrow 2\mathbf{N}$ given by $f(k) = 2k$ is bijective, so $|2\mathbf{N}| = |\mathbf{N}|$. The map $g : \mathbf{N} \rightarrow \mathbf{Z}$ given by $g(2k) = k$ and $g(2k+1) = -k-1$ for $k \in \mathbf{N}$ is bijective, so we have $|\mathbf{Z}| = |\mathbf{N}|$. The map $h : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ given by $h(k, l) = 2^k(2l+1)-1$ is bijective, so we have $|\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$.

2.11 Theorem: For all sets A , B and C ,

- (1) $|A| = |A|$,
- (2) if $|A| = |B|$ then $|B| = |A|$,
- (3) if $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$,
- (4) $|A| \leq |B|$ if and only if $(|A| = |B| \text{ or } |A| < |B|)$, and
- (5) if $|A| \leq |B|$ and $|B| \leq |C|$ then $|A| \leq |C|$.

Proof: Part (1) holds because the identity function $I_A : A \rightarrow A$ is bijective. Part (2) holds because if $f : A \rightarrow B$ is bijective then so is $f^{-1} : B \rightarrow A$. Part (3) holds because if $f : A \rightarrow B$ and $g : B \rightarrow C$ are bijective then so is the composite $g \circ f : A \rightarrow C$. The rest of the proof is left as an exercise.

2.12 Definition: Let A be a set. For each $n \in \mathbf{N}$, let $S_n = \{0, 1, 2, \dots, n-1\}$. For $n \in \mathbf{N}$, we say that the cardinality of A is equal to n , or that A has n elements, and we write $|A| = n$, when $|A| = |S_n|$. We say that A is finite when $|A| = n$ for some $n \in \mathbf{N}$. We say that A is infinite when A is not finite. We say that A is countable when $|A| = |\mathbf{N}|$.

2.13 Note: When a set A is finite with $|A| = n$, and when $f : A \rightarrow S_n$ is a bijection, if we let $a_k = f^{-1}(k)$ for each $k \in S_n$ then we have $A = \{a_0, a_1, \dots, a_{k-1}\}$ with the elements a_k distinct. Conversely, if $A = \{a_0, a_1, \dots, a_{k-1}\}$ with the elements a_k all distinct, then we define a bijection $f : A \rightarrow S_n$ by $f(a_k) = k$. Thus we see that A is finite with $|A| = n$ if and only if A is of the form $A = \{a_0, a_1, \dots, a_{n-1}\}$ with the elements a_k all distinct. Similarly, a set A is countable if and only if A is of the form $A = \{a_0, a_1, a_2, \dots\}$ with the elements a_k all distinct.

2.14 Note: For $n \in \mathbf{N}$, if A is a finite set with $|A| = n+1$ and $a \in A$ then $|A \setminus \{a\}| = n$. Indeed, if $A = \{a_0, a_1, \dots, a_n\}$ with the elements a_i distinct, and if $a = a_k$ so that we have $A \setminus \{a\} = \{a_0, a_1, \dots, a_{k-1}, a_{k+1}, \dots, a_n\}$, then we can define a bijection $f : S_n \rightarrow A \setminus \{a\}$ by $f(i) = a_i$ for $0 \leq i < k$ and $f(i) = a_{i+1}$ for $k \leq i < n$.

2.15 Theorem: Let A be a set. Then the following are equivalent.

- (1) A is infinite.
- (2) A contains a countable subset.
- (3) $|\mathbf{N}| \leq |A|$
- (4) There exists a map $f : A \rightarrow A$ which is injective but not surjective.

Proof: To prove that (1) implies (2), suppose that A is infinite. Since $A \neq \emptyset$ we can choose an element $a_0 \in A$. Since $A \neq \{a_0\}$ we can choose an element $a_1 \in A \setminus \{a_0\}$. Since $A \neq \{a_0, a_1\}$ we can choose $a_3 \in A \setminus \{a_0, a_1\}$. Continue this procedure: having chosen distinct elements $a_0, a_1, \dots, a_{n-1} \in A$, since $A \neq \{a_0, a_1, \dots, a_{n-1}\}$ we can choose $a_n \in A \setminus \{a_0, a_1, \dots, a_{n-1}\}$. In this way, we obtain a countable set $\{a_0, a_1, a_2, \dots\} \subseteq A$.

Next we show that (2) is equivalent to (3). Suppose that A contains a countable subset, say $\{a_0, a_1, a_2, \dots\} \subseteq A$ with the element a_i distinct. Since the a_i are distinct, the map $f : \mathbf{N} \rightarrow A$ given by $f(k) = a_k$ is injective, and so we have $|\mathbf{N}| \leq |A|$. Conversely, suppose that $|\mathbf{N}| \leq |A|$, and chose an injective map $f : \mathbf{N} \rightarrow A$. Considered as a map from \mathbf{N} to $f(\mathbf{N})$, f is bijective, so we have $|\mathbf{N}| = |f(\mathbf{N})|$ hence $f(\mathbf{N})$ is a countable subset of A .

Next, let us show that (2) implies (4). Suppose that A has a countable subset, say $\{a_0, a_1, a_2, \dots\} \subseteq A$ with the element a_i distinct. Define $f : A \rightarrow A$ by $f(a_k) = a_{k+1}$ for all $k \in \mathbf{N}$ and by $f(b) = b$ for all $b \in A \setminus \{a_0, a_1, a_2, \dots\}$. Then f is injective but not surjective (the element a_0 is not in the range of f).

Finally, to prove that (4) implies (1) we shall prove that if A is finite then every injective map $f : A \rightarrow A$ is surjective. We prove this by induction on the cardinality of A . The only set A with $|A| = 0$ is the set $A = \emptyset$, and then the only function $f : A \rightarrow A$ is the empty function, which is surjective. Since that base case may appear too trivial, let us consider the next case. Let $n = 1$ and let A be a set with $|A| = 1$, say $A = \{a\}$. The only function $f : A \rightarrow A$ is the function given by $f(a) = a$, which is surjective. Let $n \geq 1$ and suppose, inductively, that for every set A with $|A| = n$, every injective map $f : A \rightarrow A$ is surjective. Let B be a set with $|B| = n + 1$ and let $g : B \rightarrow B$ be injective. Suppose, for a contradiction, that g is not surjective. Choose an element $b \in B$ which is not in the range of g so that we have $g : B \rightarrow B \setminus \{b\}$. Let $A = B \setminus \{b\}$ and let $f : A \rightarrow A$ be given by $f(x) = g(x)$ for all $x \in A$. Since $g : B \rightarrow A$ is injective and $f(x) = g(x)$ for all $x \in A$, f is also injective. Again since g is injective, there is no element $x \in B \setminus \{b\}$ with $g(x) = g(b)$, so there is no element $x \in A$ with $f(x) = g(b)$, and so f is not surjective. Since $|A| = n$ (by the above note), this contradicts the induction hypothesis. Thus f must be surjective. By the Principle of Induction, for every $n \in \mathbf{N}$ and for every set A with $|A| = n$, every injective function $f : A \rightarrow A$ is surjective.

2.16 Corollary: *Let A and B be sets.*

- (1) *If A is countable then A is infinite.*
- (2) *When $|A| \leq |B|$, if B is finite then so is A (equivalently if A is infinite then so is B).*
- (3) *If $|A| = n$ and $|B| = m$ then $|A| = |B|$ if and only if $n = m$.*
- (4) *If $|A| = n$ and $|B| = m$ then $|A| \leq |B|$ if and only if $n \leq m$.*
- (5) *When one of the two sets A and B is finite, if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

Proof: Part (1) is immediate: if A is countable then $|\mathbf{N}| = |A|$, hence $|\mathbf{N}| \leq |A|$, and so A is infinite, by Theorem 2.15..

To prove Part (2), suppose that $|A| \leq |B|$ and that $|A|$ is infinite. Since A is infinite, we have $|\mathbf{N}| \leq |A|$ (by Theorem 2.15). Since $|\mathbf{N}| \leq |A|$ and $|A| \leq |B|$ we have $|\mathbf{N}| \leq |B|$ (by Theorem 2.11). Since $|\mathbf{N}| \leq |B|$, B is infinite (by Theorem 2.15 again).

To Prove Part (3), suppose that $|A| = n$ and $|B| = m$. If $n = m$ then we have $S_n = S_m$ and so $|A| = |S_n| = |S_m| = |B|$. Conversely, suppose that $|A| = |B|$. Suppose, for a contradiction, that $n \neq m$, say $n > m$, and note that $S_m \subsetneq S_n$. Since $|A| = |B|$ we have $|S_n| = |A| = |B| = |S_m|$ so we can choose a bijection $f : S_n \rightarrow S_m$. Since $S_m \subsetneq S_n$, we can consider f as a function $f : S_n \rightarrow S_n$ which is injective but not surjective. This contradicts Theorem 2.16, and so we must have $n = m$. This proves Part (3).

To prove Part (4), we again suppose that $|A| = n$ and $|B| = m$. If $n \leq m$ then $S_n \subseteq S_m$ so the inclusion map $I : S_n \rightarrow S_m$ is injective and we have $|A| = |S_n| \leq |S_m| = |B|$. Conversely, suppose that $|A| \leq |B|$ and suppose, for a contradiction, that $n > m$. Since $|A| \leq |B|$ we have $|S_n| = |A| \leq |B| = |S_m|$ so we can choose an injective map $f : S_n \rightarrow S_m$. Since $n > m$ we have $S_m \subsetneq S_n$ so we can consider f as a map $f : S_n \rightarrow S_n$, and this map is injective but not surjective. This contradicts Theorem 2.16, and so $n \leq m$.

Finally, to prove Part (5) we suppose that one of the two sets A and B is finite, and that $|A| \leq |B|$ and $|B| \leq |A|$. If A is finite then, since $|B| \leq |A|$, Part (2) implies that B is finite. If B is finite then, since $|A| \leq |B|$, Part (2) implies that A is finite. Thus, in either case, we see that A and B are both finite. Since A and B are both finite with $|A| \leq |B|$ and $|B| \leq |A|$, we must have $|A| = |B|$ by Parts (3) and (4).

2.17 Theorem: Let A be a set. Then $|A| \leq |\mathbf{N}|$ if and only if A is finite or countable.

Proof: First we claim that every subset of \mathbf{N} is either finite or countable. Let $A \subseteq \mathbf{N}$ and suppose that A is not finite. Since $A \neq \emptyset$, we can set $a_0 = \min A$ (using the Well-Ordering Property of \mathbf{N}). Note that $\{0, 1, \dots, a_0\} \cap A = \{a_0\}$. Since $A \neq \{a_0\}$ (so the set $A \setminus \{a_0\}$ is nonempty) we can set $a_1 = \min A \setminus \{a_0\}$. Then we have $a_0 < a_1$ and $\{0, 1, 2, \dots, a_1\} \cap A = \{a_0, a_1\}$. Since $A \neq \{a_0, a_1\}$ we can set $a_2 = \min A \setminus \{a_0, a_1\}$. Then we have $a_0 < a_1 < a_2$ and $\{0, 1, 2, \dots, a_2\} \cap A = \{a_0, a_1, a_2\}$. We continue the procedure: having chosen $a_0, a_1, \dots, a_{n-1} \in A$ with $a_0 < a_1 < \dots < a_{n-1}$ such that $A \cap \{0, 1, \dots, a_{n-1}\} = \{a_0, a_1, \dots, a_{n-1}\}$, since $A \neq \{a_0, a_1, \dots, a_{n-1}\}$ we can set $a_n = \min A \setminus \{a_0, a_1, \dots, a_{n-1}\}$, and then we have $a_0 < a_1 < \dots < a_{n-1} < a_n$ and $A \cap \{0, 1, 2, \dots, a_n\} = \{a_0, a_1, \dots, a_n\}$. In this way, we obtain a countable set $\{a_0, a_1, a_2, \dots\} \subseteq A$ with $a_0 < a_1 < a_2 < \dots$ with the property that for all $m \in \mathbf{N}$, $\{0, 1, 2, \dots, a_m\} \cap A = \{a_0, a_1, \dots, a_m\}$. Since $0 \leq a_0 < a_1 < a_2 < \dots$, it follows (by induction) that $a_k \geq k$ for all $k \in \mathbf{N}$. It follows in turn that $A \subseteq \{a_0, a_1, a_2, \dots\}$ because given $m \in A$, since $m \leq a_m$ we have

$$m \in \{0, 1, 2, \dots, m\} \cap A \subseteq \{0, 1, 2, \dots, a_m\} \cap A = \{a_0, a_1, \dots, a_m\}.$$

Thus $A = \{a_0, a_1, a_2, \dots\}$ and the elements a_i are distinct, so A is countable. This proves our claim that every subset of \mathbf{N} is either finite or countable.

Now suppose that $|A| \leq |N|$ and choose an injective map $f : A \rightarrow \mathbf{N}$. Since f is injective, when we consider it as a map $f : A \rightarrow f(A)$, it is bijective, and so $|A| = |f(A)|$. Since $f(A) \subseteq \mathbf{N}$, the previous paragraph shows that $f(A)$ is either finite or countable. If $f(A)$ is finite with $|f(A)| = n$ then $|A| = |f(A)| = |S_n|$, and if $f(A)$ is countable then we have $|A| = |f(A)| = |\mathbf{N}|$. Thus A is finite or countable.

2.18 Theorem: Let A be a set. Then

- (1) $|A| < |\mathbf{N}|$ if and only if A is finite,
- (2) $|\mathbf{N}| < |A|$ if and only if A is neither finite nor countable, and
- (3) if $|A| \leq |\mathbf{N}|$ and $|\mathbf{N}| \leq |A|$ then $|A| = |\mathbf{N}|$.

Proof: Part (1) follows from Theorem 2.15 because

$$\begin{aligned} |A| < |\mathbf{N}| &\iff (|A| \leq |\mathbf{N}| \text{ and } |A| \neq |\mathbf{N}|) \\ &\iff (A \text{ is finite or countable and } A \text{ is not countable}) \\ &\iff A \text{ is finite} \end{aligned}$$

and Part (2) follows from Theorem 2.17 because

$$\begin{aligned} |\mathbf{N}| < |A| &\iff (|\mathbf{N}| \leq |A| \text{ and } |\mathbf{N}| \neq |A|) \\ &\iff (A \text{ is not finite and } A \text{ is not countable.}) \end{aligned}$$

To prove Part (3), suppose that $|A| \leq |\mathbf{N}|$ and $|\mathbf{N}| \leq |A|$. Since $|A| \leq |\mathbf{N}|$, we know that A is finite or countable by Theorem 2.17. Since $|\mathbf{N}| \leq |A|$, we know that A is infinite by Theorem 2.15. Since A is finite or countable and A is not finite, it follows that A is countable. Thus $|A| = |\mathbf{N}|$.

2.19 Definition: Let A be a set. When A is countable we write $|A| = \aleph_0$. When A is finite we write $|A| < \aleph_0$. When A is infinite we write $|A| \geq \aleph_0$. When A is either finite or countable we write $|A| \leq \aleph_0$ and we say that A is **at most countable**. When A is neither finite nor countable we write $|A| > \aleph_0$ and we say that A is **uncountable**.

2.20 Theorem:

- (1) If A and B are countable sets, then so is $A \times B$.
- (2) If A and B are countable sets, then so is $A \cup B$.
- (3) If A_0, A_1, A_2, \dots are countable sets, then so is $\bigcup_{k=0}^{\infty} A_k$.
- (4) \mathbf{Q} is countable.

Proof: To prove Parts (1) and (2), let $A = \{a_0, a_1, a_2, \dots\}$ with the a_i distinct and let $B = \{b_0, b_1, b_2, \dots\}$ with the b_i distinct. Since every positive integer can be written uniquely in the form $2^k(2l+1)$ with $k, l \in \mathbf{N}$, the map $f : A \times B \rightarrow \mathbf{N}$ given by $f(a_k, b_l) = 2^k(2l+1)-1$ is bijective, and so $|A \times B| = |\mathbf{N}|$. This proves Part (1). Since the map $g : \mathbf{N} \rightarrow A \cup B$ given by $g(k) = a_k$ is injective, we have $|\mathbf{N}| \leq |A \cup B|$. Since the map $h : \mathbf{N} \rightarrow A \cup B$ given by $h(2k) = a_k$ and $h(2k+1) = b_k$ is surjective, we have $|A \cup B| \leq |\mathbf{N}|$. Since $|\mathbf{N}| \leq |A \cup B|$ and $|A \cup B| \leq |\mathbf{N}|$, we have $|A \cup B| = |\mathbf{N}|$ by Part (3) of Theorem 2.18. This proves (2).

To prove Part (3), for each $k \in \mathbf{N}$, let $A_k = \{a_{k0}, a_{k1}, a_{k2}, \dots\}$ with the a_{ki} distinct. Since the map $f : \mathbf{N} \rightarrow \bigcup_{k=0}^{\infty} A_k$ given by $f(k) = a_{k0}$ is injective, $|\mathbf{N}| \leq |\bigcup_{k=0}^{\infty} A_k|$. Since $\mathbf{N} \times \mathbf{N}$ is countable by Part (1), and since the map $g : \mathbf{N} \times \mathbf{N} \rightarrow \bigcup_{k=0}^{\infty} A_k$ given by $g(k, l) = a_{kl}$ is surjective, we have $|\bigcup_{k=0}^{\infty} A_k| \leq |\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$. By Part (3) of Theorem 2.18, we have $|\bigcup_{k=0}^{\infty} A_k| = |\mathbf{N}|$, as required.

Finally, we prove Part (4). Since the map $f : \mathbf{N} \rightarrow \mathbf{Q}$ given by $f(k) = k$ is injective, we have $|\mathbf{N}| \leq |\mathbf{Q}|$. Since the map $g : \mathbf{Q} \rightarrow \mathbf{Z} \times \mathbf{Z}$, given by $g\left(\frac{a}{b}\right) = (a, b)$ for all $a, b \in \mathbf{Z}$ with $b > 0$ and $\gcd(a, b) = 1$, is injective, and since $\mathbf{Z} \times \mathbf{Z}$ is countable, we have $|\mathbf{Q}| \leq |\mathbf{Z} \times \mathbf{Z}| = |\mathbf{N}|$. Since $|\mathbf{N}| \leq |\mathbf{Q}|$ and $|\mathbf{Q}| \leq |\mathbf{N}|$, we have $|\mathbf{Q}| = |\mathbf{N}|$, as required.

2.21 Definition: For a set A , let $\mathcal{P}(A)$ denote the **power set** of A , that is the set of all subsets of A , and let 2^A denote the set of all functions from A to $S_2 = \{0, 1\}$.

2.22 Theorem:

- (1) For every set A , $|\mathcal{P}(A)| = |2^A|$.
- (2) For every set A , $|A| < |\mathcal{P}(A)|$.
- (3) \mathbf{R} is uncountable.

Proof: Let A be any set. Define a map $g : \mathcal{P}(A) \rightarrow 2^A$ as follows. Given $S \in \mathcal{P}(A)$, that is given $S \subseteq A$, we define $g(S) \in 2^A$ to be the map $g(S) : A \rightarrow \{0, 1\}$ given by

$$g(S)(a) = \begin{cases} 1 & \text{if } a \in S, \\ 0 & \text{if } a \notin S. \end{cases}$$

Define a map $h : 2^A \rightarrow \mathcal{P}(A)$ as follows. Given $f \in 2^A$, that is given a map $f : A \rightarrow \{0, 1\}$, we define $h(f) \in \mathcal{P}(A)$ to be the subset

$$h(f) = \{a \in A \mid f(a) = 1\} \subseteq A.$$

The maps g and h are the inverses of each other because for every $S \subseteq A$ and every $f : A \rightarrow \{0, 1\}$ we have

$$\begin{aligned} f = g(S) &\iff \forall a \in A \quad f(a) = g(S)(a) \iff \forall a \in A \quad f(a) = \begin{cases} 1 & \text{if } a \in S, \\ 0 & \text{if } a \notin S, \end{cases} \\ &\iff \forall a \in A \quad (f(a) = 1 \iff a \in S) \iff \{a \in A \mid f(a) = 1\} = S \iff h(f) = S. \end{aligned}$$

This completes the proof of Part (1).

Let us prove Part (2). Again we let A be any set. Since the the map $f : A \rightarrow \mathcal{P}(A)$ given by $f(a) = \{a\}$ is injective, we have $|A| \leq |\mathcal{P}(A)|$. We need to show that $|A| \neq |\mathcal{P}(A)|$. Let $g : A \rightarrow \mathcal{P}(A)$ be any map. Let $S = \{a \in A \mid a \notin g(a)\}$. Note that S cannot be in the range of g because if we could choose $a \in A$ so that $g(a) = S$ then, by the definition of S , we would have $a \in S \iff a \notin g(a) \iff a \notin S$ which is not possible. Since S is not in the range of g , the map g is not surjective. Since g was an arbitrary map from A to $\mathcal{P}(A)$, it follows that there is no surjective map from A to $\mathcal{P}(A)$. Thus there is no bijective map from A to $\mathcal{P}(A)$ and so we have $|A| \neq |\mathcal{P}(A)|$, as desired.

Finally, we shall prove that \mathbf{R} is uncountable using the fact (which we did not prove) that every real number has a unique decimal expansion which does not end with an infinite string of 9's. We define a map $g : 2^{\mathbf{N}} \rightarrow \mathbf{R}$ as follows. Given $f \in 2^{\mathbf{N}}$, that is given a map $f : \mathbf{N} \rightarrow \{0, 1\}$, we define $g(f)$ to be the real number $g(f) \in [0, 1)$ with the decimal expansion $g(f) = .f(0)f(1)f(2)f(3)\dots$ (for those who have seen infinite series, this is the number $g(f) = \sum_{k=0}^{\infty} f(k)10^{-k-1}$). By the uniqueness of decimal expansions, the map g is injective, so we have $|2^{\mathbf{N}}| \leq |\mathbf{R}|$. Thus $|\mathbf{N}| < |\mathcal{P}(\mathbf{N})| = |2^{\mathbf{N}}| \leq |\mathbf{R}|$, and so \mathbf{R} is uncountable, by Part (2) of Theorem 2.18.

2.23 Theorem: (Cantor - Schroeder - Bernstein) *Let A and B be sets. Suppose that $|A| \leq |B|$ and $|B| \leq |A|$. Then $|A| = |B|$*

Proof: We sketch a proof. Choose injective functions $f : A \rightarrow B$ and $g : B \rightarrow A$. Since the functions $f : A \rightarrow f(A)$, $g : B \rightarrow g(B)$ and $f : g(B) \rightarrow f(g(B))$ are bijective we have $|A| = |f(A)|$ and $|B| = |g(B)| = |f(g(B))|$. Also note that $f(g(B)) \subseteq f(A) \subseteq B$. Let $X = f(g(B))$, $Y = f(A)$ and $Z = B$. Then we have $X \subseteq Y \subseteq Z$ and we have $|X| = |Z|$ and we need to show that $|Y| = |Z|$. The composite $h = f \circ g : Z \rightarrow X$ is a bijection. Define sets Z_n and Y_n for $n \in \mathbf{N}$ recursively by

$$Z_0 = Z, \quad Z_n = h(Z_{n-1}) \quad \text{and} \quad Y_0 = Y, \quad Y_n = h(Y_{n-1}).$$

Since $Y_0 = Y$, $Z_0 = Z$, $Z_1 = h(Z_0) = h(Y_0) = X$ and $X \subseteq Y \subseteq Z$, we have

$$Z_1 \subseteq Y_0 \subseteq Z_0.$$

Also note that for $1 \leq n \in \mathbf{N}$,

$$Z_n \subseteq Y_{n-1} \subseteq Z_{n-1} \implies h(Z_n) \subseteq h(Y_{n-1}) \subseteq h(Z_{n-1}) \implies Z_{n+1} \subseteq Y_n \subseteq Z_n.$$

By the Induction Principle, it follows that $Z_n \subseteq Y_{n-1} \subseteq Z_{n-1}$ for all $n \geq 1$, so we have

$$Z_0 \supseteq Y_0 \supseteq Z_1 \supseteq Y_1 \supseteq Z_2 \supseteq Y_2 \supseteq \dots$$

Let $U_n = Z_n \setminus Y_n$, $U = \bigcup_{n=1}^{\infty} U_n$ and $V = Z \setminus U$. Define $H : Z \rightarrow Y$ by

$$H(x) = \begin{cases} h(x) & \text{if } x \in U, \\ x & \text{if } x \in V. \end{cases}$$

Verify that H is bijective.

2.24 Exercise: Show that $|\mathbf{R}| = |2^{\mathbf{N}}|$.

Solution: We may include a solution later.