Appendix 1. Cardinality

1.1 Definition: Let A and B be sets and let $f : A \to B$. Recall that the **domain** of f and the **range** (or **image**) of f are the sets

$$\text{Domain}(f) = A \ , \ \text{Range}(f) = f(A) = \big\{ f(x) \big| x \in A \big\} .$$

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

$$f(S) = \big\{ f(x) \big| x \in S \big\}.$$

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

$$f^{-1}(T) = \big\{ x \in A \big| f(x) \in T \big\}.$$

1.2 Definition: Let A, B and C be sets, let $f : A \to B$ and let $g : B \to C$. We define the **composite** function $g \circ f : A \to C$ by $(g \circ f)(x) = g\big(f(x)\big)$ for all $x \in A$.

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

1.4 Theorem: *Let $f : A \to B$ and let $g : B \to C$. 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 $x_1, x_2 \in A$. 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 $z \in C$, since g is surjective we can choose $y \in B$ so that $g(y) = z$, then since f is surjective we can choose $x \in A$ 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.

1.5 Definition: For a set A, we define the **identity function** on A to be the function $I_A : A \to A$ given by $I_A(x) = x$ for all $x \in A$. Note that for $f : A \to B$ we have $f \circ I_A = f$ and $I_B \circ f = f$.

1.6 Definition: Let A and B be sets and let $f : A \to B$. A **left inverse** of f is a function $g : B \to A$ such that $g \circ f = I_A$. Equivalently, a function $g : B \to A$ is a left inverse of f when $g\big(f(x)\big) = x$ for all $x \in A$. A **right inverse** of f is a function $h : B \to A$ such that $f \circ h = I_B$. Equivalently, a function $h : B \to A$ is a right inverse of f when $f\big(h(y)\big) = y$ for all $y \in B$.

1.7 Theorem: *Let A and B be nonempty sets and let $f : A \to B$. 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 $A \neq \emptyset$ we can choose $a \in A$ and then define $g : B \to A$ 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 $x_y \in A$ with $f(x_y) = y$, and if $y \notin \text{Range}(f)$ then we define $g(y) = a$. Then for every $x \in A$ we have $y = f(x) \in \text{Range}(f)$, so $g(y) = x_y = x$, that is $g\big(f(x)\big) = x$. Conversely, if f has a left inverse, say g, then f is 1:1 since for all $x_1, x_2 \in A$, if $f(x_1) = f(x_2)$ then $x_1 = g\big(f(x_1)\big) = g\big(f(x_2)\big) = x_2$.

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

To prove Part 3, suppose first that f is bijective. The inverse function $f^{-1} : B \to A$ is a left inverse for f because given $x \in A$ we can let $y = f(x)$ and then $f^{-1}(y) = x$ so that $f^{-1}\big(f(x)\big) = f^{-1}(y) = x$. Similarly, f^{-1} is a right inverse for f because given $y \in B$ we can let x be the unique element in A with $y = f(x)$ and then we have $x = f^{-1}(y)$ so that $f\big(f^{-1}(y)\big) = f(x) = y$. 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 $y \in B$ we have

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

1.8 Corollary: *Let A and B be nonempty sets. Then there exists an injective map $f : A \to B$ if and only if there exists a surjective map $g : B \to A$.*

Proof: Suppose $f : A \to B$ is an injective map. Then f has a left inverse. Let g be a left inverse of f. Since $g \circ f = I_A$, 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 $g : B \to A$. Similarly, if $g : B \to A$ is surjective, then it has a right inverse $f : A \to B$ which is injective.

1.9 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 $f : A \to B$ (or equivalently when there exists a bijective map $g : B \to A$). 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 $f : A \to B$ (or equivalently when there exists a surjective map $g : B \to A$). 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 $f : A \to B$ but there does not exist a bijective map $g : A \to B$). We also write $|A| \geq |B|$ when $|B| \leq |A|$ and $|A| > |B|$ when $|B| < |A|$.

1.10 Example: Let $\mathbb{N} = \{0, 1, 2, \cdots\}$, let $\mathbf{Z}^+ = \{1, 2, 3, \cdots\}$, and let $2\mathbf{N} = \{0, 2, 4, 6, \cdots\}$. The map $f : \mathbb{N} \to \mathbb{Z}^+$ given by $f(k) = k+1$ is bijective, so $|\mathbb{Z}^+| = |\mathbb{N}|$. The map $g : \mathbb{N} \to 2\mathbb{N}$ given by $g(k) = 2k$ is bijective, so $|2\mathbb{N}| = |\mathbb{N}|$. The map $h : \mathbb{N} \to \mathbb{Z}$ given by $h(2k) = k$ and $h(2k+1) = -k-1$ for $k \in \mathbb{N}$ is bijective, so we have $|\mathbb{Z}| = |\mathbb{N}|$. The map $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $p(k, l) = 2^k(2l+1) - 1$ is bijective, so we have $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

1.11 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* ($|A| = |B|$ *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 $I_A : A \to A$ is bijective. Part 2 holds because if $f : A \to B$ is bijective then so is $f^{-1} : B \to A$. Part 3 holds because if $f : A \to B$ and $g : B \to C$ are bijective then so is the composite $g \circ f : A \to C$. The rest of the proof is left as an exercise.

1.12 Definition: Let A be a set. For each $n \in \mathbb{N}$, let $S_n = \{0, 1, 2, \cdots, n-1\}$. For $n \in \mathbb{N}$, 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 $n \in \mathbb{N}$, we say A is **infinite** when A is not finite, and we say A is **countably infinite** when $|A| = |\mathbb{N}|$.

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

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

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

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

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

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

Next, let us show that (2) implies (4). Suppose that A has a countably infinite subset, say $\{a_0, a_1, a_2, \cdots\} \subseteq A$ with the element a_i distinct. Define $f : A \to A$ by $f(a_k) = a_{k+1}$ for all $k \in \mathbb{N}$ and by $f(b) = b$ for all $b \in A \setminus \{a_0, a_1, a_2, \cdots\}$. 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 $f : A \to A$ 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 $f : A \to A$ 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 $f : A \to A$ 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 $f : A \to A$ is surjective. Let B be a set with $|B| = n + 1$ and let $g : B \to B$ 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 $g : B \to B \setminus \{b\}$. Let $A = B \setminus \{b\}$ and let $f : A \to A$ be given by $f(x) = g(x)$ for all $x \in A$. Since $g : B \to A$ 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 g must be surjective. By the Principle of Induction, for every $n \in \mathbb{N}$ and for every set A with $|A| = n$, every injective function $f : A \to A$ is surjective.

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

(1) If A is countably infinite 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 countably infinite then A contains a countably infinite subset (itself), so A is infinite, by Theorem 1.15.

To prove Part 2, suppose that $|A| \leq |B|$ and that $|A|$ is infinite. Since A is infinite, we have $|\mathbb{N}| \leq |A|$ (by Theorem 1.15). Since $|\mathbb{N}| \leq |A|$ and $|A| \leq |B|$ we have $|\mathbb{N}| \leq |B|$ (by Theorem 1.11). Since $|\mathbb{N}| \leq |B|$, B is infinite (by Theorem 1.15 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 $S_m \subsetneqq S_n$. Since $|A| = |B|$ we have $|S_n| = |A| = |B| = |S_m|$ so we can choose a bijection $f : S_n \to S_m$. Since $S_m \subsetneqq S_n$, we can consider f as a function $f : S_n \to S_n$ which is injective but not surjective. This contradicts Theorem 1.15, 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 $I : S_n \to S_m$ 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 $f : S_n \to S_m$. Since $n > m$ we have $S_m \subsetneqq S_n$ so we can consider f as a map $f : S_n \to S_n$, and this map is injective but not surjective. This contradicts Theorem 1.15, 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.

1.17 Theorem: *Let A be a set. Then $|A| \leq |\mathbb{N}|$ if and only if A is finite or countably infinite.*

Proof: First we claim that every subset of $\mathbb{N}$ is either finite or countably infinite. Let $A \subseteq \mathbb{N}$ and suppose that A is not finite. Since $A \neq \emptyset$, we can set $a_0 = \min A$ (using the Well-Ordering Property of $\mathbb{N}$). Note that $\{0, 1, \cdots, a_0\} \cap A = \{a_0\}$. 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 $\{0, 1, 2, \cdots, a_1\} \cap A = \{a_0, a_1\}$. 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 $\{0, 1, 2, \cdots, a_3\} \cap A = \{a_0, a_1, a_2\}$. We continue the procedure: having chosen $a_0, a_1, \cdots, a_{n-1} \in A$ with $a_0 < a_1 < \cdots < a_{n-1}$ such that $A \cap \{0, 1, \cdots, a_{n-1}\} = \{a_0, a_1, \cdots, a_{n-1}\}$, since $A \neq \{a_0, a_1, \cdots, a_{n-1}\}$ we can set $a_n = \min A \setminus \{a_0, a_1, \cdots, a_{n-1}\}$, and then we have $a_0 < a_1 < \cdots < a_{n-1} < a_n$ and $A\{0, 1, 2, \cdots, a_n\} \cap A = \{a_0, a_1, \cdots, a_n\}$. In this way, we obtain a countably infinite set $\{a_0, a_1, a_2, \cdots\} \subseteq A$ with $a_0 < a_1 < a_2 < \cdots$ with the property that for all $m \in \mathbb{N}$, $\{0, 1, 2, \cdots, a_m\} \cap A = \{a_0, a_1, \cdots, a_m\}$. Since $0 \leq a_0 < a_1 < a_2 < \cdots$, it follows (by induction) that $a_k \geq k$ for all $k \in \mathbb{N}$. It follows in turn that $A \subseteq \{a_0, a_1, a_2 \cdots\}$ because given $m \in A$, since $m \leq a_m$ we have

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

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

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

1.18 Theorem: *Let A be a set. Then*

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

Proof: Part 1 follows from Theorem 1.15 because

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

and Part 2 follows from Theorem 1.17 because

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

To prove Part 3, suppose that $|A| \leq |\mathbb{N}|$ and $|\mathbb{N}| \leq |A|$. Since $|A| \leq |\mathbb{N}|$, we know that A is finite or countably infinite by Theorem 1.17. Since $|\mathbb{N}| \leq |A|$, we know that that A is infinite by Theorem 1.15. Since A is finite or countably infinite and A is not finite, it follows that A is countably infinite. Thus $|A| = |\mathbb{N}|$.

1.19 Definition: Let A be a set. When A is countably infinite 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 countably infinite we write $|A| \leq \aleph_0$ and we say that A is **at most countable**. when A is neither finite nor countably infinite we write $|A| > \aleph_0$ and we say that A is **uncountable** (or **uncountably infinite**).

1.20 Theorem:

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

Proof: To prove both Parts 1 and 2, let $A = \{a_0, a_1, a_2, \cdots\}$ with the a_i distinct and let $B = \{b_0, b_1, b_2, \cdots\}$ with the b_i distinct. Since every positive integer can be written uniquely in the form $2^k(2l+1)$ with $k, l \in \mathbb{N}$, the map $f : A \times B \to \mathbb{N}$ given by $f(a_k, b_l) = 2^k(2l+1)-1$ is bijective, and so $|A \times B| = |\mathbb{N}|$. This proves Part 1. Since the map $g : \mathbb{N} \to A \cup B$ given by $g(k) = a_k$ is injective, we have $|\mathbb{N}| \leq |A \cup B|$. Since the map $h : \mathbb{N} \to A \cup B$ given by $h(2k) = a_k$ and $h(2k+1) = b_k$ is surjective, we have $|A \cup B| \leq |N|$. Since $|\mathbb{N}| \leq |A \cup B|$ and $|A \cup B| \leq |\mathbb{N}|$, we have $|A \cup B| = |\mathbb{N}|$ by Part 3 of Theorem 1.18. This proves 2.

To prove Part 3, for each $k \in \mathbb{N}$, let $A_k = \{a_{k0}, a_{k1}, a_{k2}, \cdots\}$ with the a_{ki} distinct. Since the map $f : \mathbb{N} \to \bigcup_{k=0}^{\infty} A_k$ given by $f(k) = a_{0,k}$ is injective, $|\mathbb{N}| \leq \left|\bigcup_{k=0}^{\infty} A_k\right|$. Since $\mathbb{N} \times \mathbb{N}$ is countably infinite by Part (1), and since the map $g : \mathbb{N} \times \mathbb{N} \to \bigcup_{k=0}^{\infty} A_k$ given by $g(k, l) = a_{k,l}$ is surjective, we have $\left|\bigcup_{k=0}^{\infty} A_k\right| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. By Part 3 of Theorem 1.18, we have $\left|\bigcup_{k=0}^{\infty} A_k\right| = |\mathbb{N}|$, as required.

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

1.21 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 $S_2 = \{0, 1\}$.

1.22 Theorem:

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

Proof: Let A be any set. Define a map $g : \mathcal{P}(A) \to 2^A$ 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 $g(S) : A \to \{0, 1\}$ given by

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

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

$$h(f) = \left\{a \in A \middle| f(a) = 1\right\} \subseteq A.$$

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

$$f = g(S) \iff \forall a \in A \;\; f(a) = g(S)(a) \iff \forall a \in A \;\; f(a) = \begin{cases} 1 \text{ if } a \in S, \\ 0 \text{ if } a \notin S, \end{cases}$$

$$\iff \forall a \in A \; \big(f(a) = 1 \iff a \in S\big) \iff \left\{a \in A \middle| f(a) = 1\right\} = S \iff h(f) = S.$$

This completes the proof of Part 1.

Let us prove Part 2. Again we let A be any set. Since the the map $f : A \to \mathcal{P}(A)$ given by $f(a) = \{a\}$ is injective, we have $|A| \leq \big|\mathcal{P}(A)\big|$. We need to show that $|A| \neq \big|\mathcal{P}(A)\big|$. Let $g : A \to \mathcal{P}(A)$ be any map. Let $S = \big\{a \in A \big| a \notin g(a)\big\}$. 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 $|A| \neq \big|\mathcal{P}(A)\big|$, as desired.

Finally, we shall prove that $\mathbb{R}$ is uncountably infinite using the fact that every real number has a unique decimal expansion which does not end with an infinite string of 9's. Define a map $g : 2^{\mathbb{N}} \to \mathbb{R}$ as follows. Given $f \in 2^{\mathbb{N}}$, that is given a map $f : \mathbb{N} \to \{0, 1\}$, we define $g(f)$ to be the real number $g(f) \in [0, 1)$ with the decimal expansion $g(f) = 0.f(0)f(1)f(2)f(3)\cdots$, that is $g(f) = \sum_{k=0}^{\infty} f(k)10^{-k-1}$. By the uniqueness of decimal expansions, the map g is injective, so we have $\big|2^{\mathbb{N}}\big| \leq |\mathbb{R}|$. Thus $|\mathbb{N}| < \big|\mathcal{P}(\mathbb{N})\big| = \big|2^{\mathbb{N}}\big| \leq |\mathbb{R}|$, and so $\mathbb{R}$ is uncountably infinite, by Part 2 of Theorem 1.18.

1.23 Note: Part 2 of the above theorem shows that there is an infinite sequence of infinite sets with strictly increasing cardinalities, namely

$$|\mathbb{N}| < \big|2^{\mathbb{N}}\big| < \big|2^{2^{\mathbb{N}}}\big| < \Big|2^{2^{2^{\mathbb{N}}}}\Big| < \cdots$$

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

Proof: Since $|A| \leq |B|$ and $|B| \leq |A|$ we can choose injective functions $f : A \to B$ and $g : B \to A$. Since $g : B \to A$ is injective, the map $g : B \to g(B)$ is bijective so that $|B| = |g(B)|$, and so it suffices to show that $|A| = |g(B)|$. Note that $f(A) \subseteq B$ and $g(f(A)) \subseteq g(B) \subseteq A$. Note that since $f : A \to B$ and $g : B \to A$ are injective, so is the composite $h = g \circ f : A \to A$. Define sets A_n and B_n recursively by $A_0 = A$, $B_0 = g(B)$, $A_{n+1} = h(A_n)$ and $B_{n+1} = h(B_n)$. Since $A \supseteq g(B) \supseteq g(f(A))$ we have $A_0 \supseteq B_0 \supseteq A_1$, and if $A_n \supseteq B_n \supseteq A_{n+1}$ then we have $h(A_n) \supseteq h(B_n) \supseteq h(A_{n+1})$ so that $A_{n+1} \supseteq B_{n+1} \supseteq A_{n+2}$. It follows, by induction, that

$$A_0 \supseteq B_0 \supseteq A_1 \supseteq B_1 \supseteq A_2 \supseteq B_2 \supseteq \cdots$$

Let $U = \bigcup_{n=0}^{\infty}(A_n \setminus B_n)$ and $V = \bigcup_{n=1}^{\infty}(A_n \setminus B_n)$ and $W = A_0 \setminus U$ and note that A_0 is the disjoint union $A_0 = U \cup W$ and B_0 is the disjoint union $B_0 = V \cup W$. Since h is injective, the maps $h : A_n \to h(A_n) = A_{n+1}$ and $h : B_n \to h(B_n) = B_{n+1}$ are bijective for each $n \in \mathbb{N}$, and so the maps $h : (A_n \setminus B_n) \to (A_{n+1} \setminus B_{n+1})$ are bijective for each $n \in \mathbb{Z}^+$, and hence the map $h : U \to V$ is bijective, say $k = h^{-1} : V \to U$. We have a bijection $F : A_0 \to B_0$ and its inverse $G = F^{-1} : B_0 \to A_0$ given by

$$F(x) = \left\{ \begin{array}{c} h(x) \text{ if } x \in U \\ x \quad \text{if } x \in W \end{array} \right\}, \; G(y) = \left\{ \begin{array}{c} k(y) \text{ if } y \in V \\ y \quad \text{if } y \in W \end{array} \right\}$$

and hence $|A_0| = |B_0|$, that is $|A| = |g(B)|$, as required.

1.25 Exercise: Let A be a countably infinite set. Show that the set of finite sequences with terms in A is countably infinite. Show that the set of all finite subsets of A is countably infinite.

1.26 Example: Show that $|\mathbb{R}| = \left|2^{\mathbb{N}}\right|$.

Solution: Define $g : 2^{\mathbb{N}} \to \mathbb{R}$ as follows: for $f \in 2^{\mathbb{N}}$ we let $g(f)$ be the real number $g(f) \in [0,1)$ with decimal expansion $g(f) = 0.f(0)f(1)f(2)\cdots$. Then g is injective so $\left|2^{\mathbb{N}}\right| \leq |\mathbb{R}|$. Define $h : 2^{\mathbb{N}} \to [0,1]$ as follows: for $f \in 2^{\mathbb{N}}$ let $h(f)$ be the real number $h(f) \in [0,1]$ with binary expansion $h(f) = 0.f(0)f(1)f(2)\cdots$. Then h is surjective so we have $\left|[0,1]\right| \leq \left|2^{\mathbb{N}}\right|$. The map $k : \mathbb{R} \to [0,1]$ given by $k(x) = \frac{1}{2} + \frac{1}{\pi}\tan^{-1} x$ is injective so we have $|\mathbb{R}| \leq \left|[0,1]\right|$. Since $|\mathbb{R}| \leq \left|[0,1]\right| \leq \left|2^{\mathbb{N}}\right|$ and $\left|2^{\mathbb{N}}\right| \leq |\mathbb{R}|$, we have $|\mathbb{R}| = \left|2^{\mathbb{N}}\right|$ by the Cantor-Schroeder-Bernstein Theorem.

1.27 Notation: For sets A and B, we write A^B to denote the set of functions $f : B \to A$.

1.28 Theorem: *Let A, B, C and D be sets with $|A| = |C|$ and $|B| = |D|$. Then*
(1) if $A \cap B = \emptyset$ and $C \cap D = \emptyset$ then $\left|A \cup B\right| = \left|C \cup D\right|$,
(2) $\left|A \times B\right| = \left|C \times D\right|$, and
(3) $\left|A^B\right| = \left|C^D\right|$.

Proof: We prove Part 3 and leave the proofs of Parts 1 and 2 as an exercise. Since $|A| = |C|$ and $|B| = |D|$ we can choose bijections $f : A \to C$ and $g : B \to D$. Define $F : A^B \to C^D$ by $F(k) = f \circ k \circ g^{-1}$, where $k \in A^B$, that is $k : B \to A$. Define $G : C^D \to A^B$ by $G(\ell) = f^{-1} \circ \ell \circ g$, where $\ell \in C^D$, that is $\ell : D \to C$. Then for all $\ell \in A^B$ we have $F(G(\ell)) = F(f^{-1} \circ \ell \circ g) = f \circ f^{-1} \circ \ell \circ g \circ g^{-1} = \ell$ and for all $k \in A^B$ we have $G(F(k)) = G(f \circ k \circ g^{-1}) = f^{-1} \circ f \circ k \circ g^{-1} \circ g = k$. Thus F and G are inverses of one another.

1.29 Definition: Note that, although we have defined what it means for two sets to have the same cardinality, and what it means for one set to have a smaller cardinality than another, we have not actually defined what the cardinality of a set is (we have defined the meaning of the expressions $|A| = |B|$, $|A| \leq |B|$ and $|A| < |B|$, but we have not defined the meaning of the term $|A|$). It is possible (but we shall not do it in this course) to define certain specific sets called **cardinals** such that for every set A there exists a unique cardinal κ with $|A| = |\kappa|$. We can then define the **cardinality** of a set A to be equal to the unique cardinal κ such that $|A| = |\kappa|$ and, in this case, we define the **cardinality** of the set A to be $|A| = \kappa$. In foundational set theory, the natural numbers are defined, formally, to be equal to the sets $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0,1\} = \big\{\emptyset, \{\emptyset\}\big\}$ and, in general, $n+1 = n \cup \{n\}$ so that the natural number n is equal to the set that we previously denoted by S_n, that is $n = S_n = \big\{0, 1, \cdots, n-1\big\}$. The finite cardinals are equal to the natural numbers and the countably infinite cardinal $\aleph_0$ is equal to the set of natural numbers. The previous theorem allows us to define **arithmetic operations** on cardinals which extend the usual arithmetic operations on the natural numbers. Given cardinals κ and λ we define $\kappa + \lambda$, $\kappa \cdot \lambda$ and κ^λ to be the cardinals such that

$$\begin{aligned} \kappa + \lambda &= \left|(\kappa \times \{0\}) \cup (\lambda \times \{1\})\right|, \\ \kappa \cdot \lambda &= \left|\kappa \times \lambda\right|, \\ \kappa^\lambda &= \left|\kappa^\lambda\right|. \end{aligned}$$

1.30 Theorem: *(Rules of Cardinal Arithmetic) Let κ, λ and μ be cardinals. Then*
(1) $\kappa + \lambda = \lambda + \kappa$,
(2) $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$,
(3) $\kappa + 0 = \kappa$,
(4) $\lambda \leq \mu \Longrightarrow \kappa + \lambda \leq \kappa + \mu$,
(5) $\kappa \cdot \lambda = \lambda \cdot \kappa$,
(6) $(\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$,
(7) $\kappa \cdot 1 = \kappa$,
(8) $\kappa \cdot (\lambda + \mu) = (\kappa \cdot \lambda) + (\kappa \cdot \mu)$,
(9) $\lambda \leq \mu \Longrightarrow \kappa \cdot \lambda \leq \kappa \cdot \mu$,
(10) $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$,
(11) $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$,
(12) $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$,
(13) $\lambda \leq \mu \Longrightarrow \kappa^\lambda \leq \kappa^\mu$, *and*
(14) $\kappa \leq \lambda \Longrightarrow \kappa^\mu \leq \lambda^\mu$.

Proof: We sketch a proof for Parts 9 and 11 and leave the rest as an exercise. To prove Part 9, let A, B and C be sets with $|A| = \kappa$, $|B| = \lambda$ and $|C| = \mu$ and suppose that $|B| \leq |C|$. We need to show that $|A \times B| \leq |A \times C|$. Let $f : B \to C$ be an injective map. Define $F : A \times B \to A \times C$ by $F(a, b) = \big(a, f(b)\big)$ then verify that F is injective.

To prove Part 11, let A, B and C be sets with $|A| = \kappa$, $|B| = \lambda$ and $|C| = \mu$. We need to show that $\big|(A^B)^C\big| = \big|A^{B\times C}\big|$. Define $F : (A^B)^C \to A^{B\times C}$ by $F(f)(b, c) = f(c)(b)$. Verify that F is bijective with inverse $G : A^{B\times C} \to (A^B)^C$ given by $G(g)(c)(b) = g(b, c)$.

1.31 Example: Let $\mathbb{R}^\omega$ be the set of all sequences $a = (a_k)_{k\geq 1} = (a_1, a_2, a_3, \cdots)$ of real numbers and let $\mathbb{R}^\infty$ be the set of eventually zero sequences in $\mathbb{R}^\omega$, that is the sequences $(a_k)_{k\geq 1}$ for which there exists $n \in \mathbb{Z}^+$ such that $a_k = 0$ for all $k \geq n$. Show that for all $n \in \mathbb{Z}^+$ we have

$$|\mathbb{R}| = |\mathbb{R}^n| = |\mathbb{R}^\infty| = |\mathbb{R}^\omega| = 2^{\aleph_0}.$$

Solution: It is clear that $2^{\aleph_0} = |\mathbb{R}| \leq |\mathbb{R}^n| \leq |\mathbb{R}^\infty| \leq |\mathbb{R}^\omega|$ so it suffices (by the Cantor-Schröder-Bernstein Theorem) to show that $|\mathbb{R}^\omega| \leq 2^{\aleph_0}$. By Part 1 of Theorem 1.20, we have $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ so that $\aleph_0 \cdot \aleph_0 = \aleph_0$, and so

$$|\mathbb{R}^\omega| = |\mathbb{R}^{\mathbb{N}}| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}.$$

1.32 Example: Find $\big|\mathbb{R}^{\mathbb{R}}\big|$.

Solution: First, let us explain the meaning of the question. As mentioned in Note 1.23, we have an infinite sequence of infinite cardinals

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < 2^{2^{2^{\aleph_0}}} < \cdots.$$

It has been shown that it is not possible to prove (using the ZFC axioms of set theory) that there exist any cardinals which lie strictly between any two consecutive cardinals on this list. For this reason, if you are asked to find the cardinality of an infinite set A, then you are really being asked to determine which of the cardinals in the above list is equal to the cardinality of the set A. Now let us answer the question.

Since $2 \leq 2^{\aleph_0}$ and $\aleph_0 \leq 2^{\aleph_0}$ and $\aleph_0 + \aleph_0 = \aleph_0$ (by Part 2 of Theorem 1.20), we have

$$2^{2^{\aleph_0}} \leq (2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} \leq 2^{2^{\aleph_0} \cdot 2^{\aleph_0}} = 2^{2^{\aleph_0 + \aleph_0}} = 2^{2^{\aleph_0}},$$

and so $|\mathbb{R}^{\mathbb{R}}| = (2^{\aleph_0})^{2^{\aleph_0}} = 2^{2^{\aleph_0}}$ by the Cantor-Schröder-Bernstein Theorem.