## 1.1 CONTINUED

**Definition 1.** If $A \neq \emptyset$ and $B \neq \emptyset$, then the Cartesian product, $A \times B$, contains all $(a, b)$ such that $a \in A$ and $b \in B$; i.e. $A \times B := \{(a, b) : a \in A, b \in B\}$.

For example $A = \{1, 2, 3\}, B = \{4, 5\} \Rightarrow A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$.

**Definition 2.** A function $f : A \mapsto B$ is a set of ordered pairs $(a, b) \in A \times B$ such that for all $a \in A$, there is a unique $b \in B$; i.e. if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$. The set $A$ is said to be the domain and $f(A)$ is said to be the range. The set $B$ is said to be the codomain and $f(A) \subseteq B$.

We discussed examples of this in class.

**Definition 3.** Consider $f : A \mapsto B$. If $E \subseteq A$, then the image of $E$ under $f$ is $f(E) := \{f(x) : x \in E\} \subseteq B$. Further, if $H \subseteq B$, then the inverse image of $H$ under $f$ is $f^{-1}(H) := \{x \in A : f(x) \in H\} \subseteq A$, where $f^{-1}$ is called the inverse.

**Definition 4.** Consider $f : A \mapsto B$.

(1) If $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, then $f$ is said to be injective (one-to-one) and we call $f$ an injection.
(2) If $f(A) = f(B)$, then $f$ is said to be surjective (onto) and we call $f$ a surjection.
(3) If $f$ is both injective and surjective, it is said to be bijective and called a bijection.

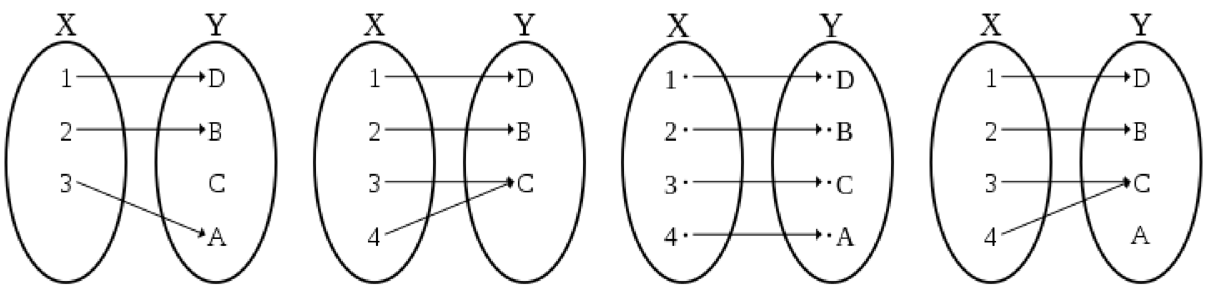


FIGURE 1. Injection, Surjection, Bijection, Neither

**Example 1.** *The function* $f : (0, \infty) \mapsto (0, 1)$ *defined as*

$$f := \frac{1}{1 + x^2} \tag{1}$$

*is a bijection.*

The strategy for injection is to show $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, and the strategy for surjection is to show for all $y \in (0, 1)$ there is an $x \in (0, \infty)$ such that $f(x) = y$.

*Proof.* We do the proof in two parts,

Injection: Suppose $f(x_1) = f(x_2)$, then

$$\frac{1}{1 + x_1^2} = \frac{1}{1 + x_2^2} \Rightarrow 1 + x_1^2 = 1 + x_2^2 \Rightarrow x_1^2 = x_2^2,$$

and since $x_1, x_2 \in (0, \infty)$; i.e. positive, $x_1 = x_2$.

Surjection: Consider $y \in (0, 1)$ then if $f(x) = y$, $x = \sqrt{(1/y) - 1} \in (0, \infty)$.

Since the function is both an injection and a surjection, it is a bijection. ∎

**Definition 5.** If $f : A \mapsto B$ is bijective, then the inverse is $f^{-1} := \{(b, a) \in B \times A : (a, b) \in f\}$.

For example, for $f : (0, \infty) \mapsto (0, 1)$, where $f(x) := 1/(1 + x^2)$, we write $x = 1/(1 + y^2)$ and solve for $y$, which gives us $y = \sqrt{1/x - 1}$, which means $f^{-1}(x) = \sqrt{1/x - 1}$.

**Definition 6.** Consider $f : A \mapsto B$ and $g : B \mapsto C$, then the composition $g \circ f : A \mapsto C$ is defined as $(g \circ f)(x) := g(f(x))$ for all $x \in A$.

**Theorem 1.** *Consider $f : A \mapsto B$ and $g : B \mapsto C$, and $H \subseteq C$, then $(g \circ f)^{-1}(H) = f^{-1}(g^{-1}(H))$.*

Here, instead of trying to prove one is a subset of the other and vice-versa, we shall use a more direct approach using the definition of the inverse, which gives us $h(h^{-1}(x)) = x$.

*Proof.* Notice that by definition of the inverse (first) and the composition (second), $(g \circ f)((g \circ f)^{-1}(H)) = g(f((g \circ f)^{-1}(H))) = H$. Therefore, $f^{-1}(g^{-1}(H)) = f^{-1}(g^{-1}(g(f((g \circ f)^{-1}(H))))) = f^{-1}(f((g \circ f)^{-1}(H))) = (g \circ f)^{-1}(H)$. □

**Caveat:** You may be tempted to work on both sides of the equation $(g \circ f)^{-1}(H) = f^{-1}(g^{-1}(H))$ simultaneously to massage it into a statement that is true. However, this would mean that you are already assuming the statement you are trying to prove is true (this type of fallacy is called "Begging the question"). What you must do is go from a true statement and massage that into the statement you would like to prove.

## 1.2 Induction

Lets first discuss the properties of $\mathbb{N}$.

**Property 1** (Well-ordering of $\mathbb{N}$)**.** Every nonempty subset of $\mathbb{N}$ has a least element.

**Property 2** (Weak induction)**.** Suppose the following statements hold

(1) $P(1)$ is true, and
(2) For all $k > 1$, $P(k) \Rightarrow P(k + 1)$, then

$P(n)$ is true for all $n \in \mathbb{N}$.

**Example 2.**

$$\sum_{n=1}^{N} n = \frac{1}{2}N(N + 1).$$

*Proof.*

- $\sum_{n=1}^{1} n = 1$ ✓
- $$\sum_{n=1}^{k+1} n = \sum_{n=1}^{k} n + (k + 1) = \frac{1}{2}k(k + 1) + \frac{1}{2}(2(k + 1)) = \frac{1}{2}(k + 1)(k + 2). \checkmark$$

□

**Property 3** (Strong induction)**.** Suppose the following statements hold

(1) $P(1)$ is true, and
(2) For all $k > 1$, $P(1), P(2), \ldots, P(k) \Rightarrow P(k + 1)$, then

$P(n)$ is true for all $n \in \mathbb{N}$.

**Example 3.** *The $n^{th}$ term of the Fibonacci sequence ($\{1, 1, 2, 3, 5, 8, \ldots, n + 1 = n + (n - 1)\}$) is given by the following formula,*

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right] \tag{2}$$

*Proof.* (1) $F_1 = 1$, $F_2 = 1$ ✓

(2) Suppose $F_k$ and $F_{k-1}$ hold, then

$$F_{k+1} = F_k + F_{k-1} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right] + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\right] - \frac{1}{\sqrt{5}}\left[\left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}+1\right)\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}+1\right)\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right].$$

Notice that

$$\frac{1+\sqrt{5}}{2}+1 = \frac{3+\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^2,$$

and

$$\frac{1-\sqrt{5}}{2}+1 = \frac{3-\sqrt{5}}{2} = \left(\frac{1-\sqrt{5}}{2}\right)^2,$$

hence

$$F_{k+1} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right]$$

Therefore, the formula (2) is true.

□

## 1.3 Finite and Infinite Sets

**Definition 7.** We call the amount of elements in a set $A$ the cardinality of $A$, denoted as $\text{Card}(A)$.

**Properties of infinite sets.**

- If $C$ is an infinite set and $B$ is a finite set, then $C \setminus B$ is infinite.
- If $A \subseteq B$ is an infinite set, then so is $B$.
- $\mathbb{N}$ is said to be denumerable (countably infinite). $\text{Card}(\mathbb{N} = \aleph_0)$

**Definition 8.** A set $S$ is said to be countably infinite if there is a bijection $f : \mathbb{N} \mapsto S$. A set is countable if it is finite or countably infinite. A set that is not countable is said to be uncountable.

It should be noted that I generally call countably infinite sets simply countable since finite sets are trivially countable.

Here are some examples below:

- $S = \{1, 4, 9, 16, \ldots\}$ is countable since $f : \mathbb{N} \mapsto S$ with the mapping $f(n) = n^2$ for all $n \in \mathbb{N}$.
- $\mathbb{Z}$ is countable since $f : \mathbb{N} \mapsto \mathbb{Z}$ such that $f(n) = n/2$ for all even $n \in \mathbb{N}$, $f(n) = -(n-1)/2$ for all odd $n \in \mathbb{N}$, and $f(1) = 0$.
- Any sequence $A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\}$ is countable because by definition a sequence is a function for $\mathbb{N}$ onto the elements of the sequence; i.e. $f : \mathbb{N} \mapsto A$ such that $f(n) = a_n$.
- A finite union of countable sets are countable. Consider $B = \{b_1, b_2, b_3, \ldots, b_n, \ldots\}$. Then $f : \mathbb{N} \mapsto A \cup B$ such that $f(n) = a_{n/2}$ for $n \in \mathbb{N}$ even and $f(n) = b_{(n+1)/2}$ for $n \in \mathbb{N}$ odd.
- We can also take Cartesian products of countable sets to make countable sets. $f : \mathbb{N} \mapsto \mathbb{N} \times \mathbb{N}$ such that $f^{-1}(n, m) := \frac{1}{2}(m+n-2)(m+n-1) + m$.
- For the irrationals it gets a bit tricky, but notice that $f : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{Q}^+$ such that $f(n, m) = n/m$ for all $n, m \in \mathbb{N}$ by definition. We can do the same thing for $\mathbb{Q}^-$ by $f(n, m) = -n/m$. And $\{0\}$ is finite, so that is already countable. Therefore $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$.

Here are some other properties of infinite sets

- If $T \subseteq S$, If $S$ is countable then so is $T$ and if $T$ is uncountable then so is $S$.
- If $A_m$ is countable $A := \cup_{m=1}^{\infty} A_m$ is countable.

- Also, bijections are not always necessary. Both $f : \mathbb{N} \mapsto S$ (surjective) and $f : S \mapsto \mathbb{N}$ (injective) also work. This is because an infinite subset of $\mathbb{N}$ had the same number of elements as $\mathbb{N}$ as we showed in our first example. So a subset of $\mathbb{N}$ works just as well as $\mathbb{N}$.