

IV. FUNCTIONS (The Book, chapter 15) In the previous chapters, we have been measuring the size of certain sets of integers, using infinite series. Now we see how to compare different sets, not necessarily of integers or numbers, using functions.

19. Injections, Surjections, Bijections —

Definition 19.1. A function $f : S \rightarrow T$ is a **bijection** if, for every $t \in T$, there exists a unique $s \in S$ such that $f(s) = t$.

Note that the phrase “there exists a unique” is really two assertions: existence and uniqueness. We can have one without the other.

Definition 19.1’. A function $f : S \rightarrow T$ is **surjective** if, for every $t \in T$, there is some $s \in S$ such that $f(s) = t$.

Definition 19.1”. A function $f : S \rightarrow T$ is **injective** if, for every $t \in T$, there is at most one $s \in S$ such that $f(s) = t$.

So a bijection is a function which is both injective and surjective. Some people use “onto” to mean “surjective” and “one-to-one” to mean “injective”.

The **image** of $f : S \rightarrow T$ is the set

$$f(S) = \{t \in T : t = f(s) \text{ for some } s \in S\}.$$

To say that f is surjective is to say that $f(S) = T$. Note that f may be regarded as a function $f : S \rightarrow f(S)$, and the latter function is automatically surjective.

Let $t \in T$. The **fiber** of f over t is the set

$$f^{-1}(t) = \{s \in S : f(s) = t\}.$$

Note that $f^{-1}(t)$ is a subset of S , not an element of S . In general, there is no function “ f^{-1} ”. The fiber $f^{-1}(t)$ could contain zero, one, or more than one elements of S . To say that $f : S \rightarrow T$ is surjective is to say that $f^{-1}(t)$ is non-empty for all $t \in T$. To say that $f : S \rightarrow T$ is injective is to say that $f^{-1}(t)$ contains at most one element for every $t \in T$. To say that $f : S \rightarrow T$ is bijective is to say that $f^{-1}(t)$ contains exactly one element for every $t \in T$. In this case, f^{-1} may be regarded as a function whose value at $t \in T$ is the unique element of the fiber $f^{-1}(t)$.

How to prove it —

- To prove that a given function $f : S \rightarrow T$ is surjective, begin by saying “Suppose $t \in T$ ”. Then find, somehow, an element $s \in S$ such that $f(s) = t$.
- To prove that $f : S \rightarrow T$ is not surjective it suffices to find a single element $t \in T$ for which there is no $s \in S$ having $f(s) = t$. (I.e., for which the fiber $f^{-1}(t)$ is empty.)
- To prove that $f : S \rightarrow T$ is injective, begin by saying “Suppose $f(s_1) = f(s_2)$ ”. Then show, somehow, that $s_1 = s_2$.
- To prove that $f : S \rightarrow T$ is not injective, it suffices to find a single pair of distinct elements $s_1, s_2 \in S$ such that $f(s_1) = f(s_2)$.
- To prove that $f : S \rightarrow T$ is bijective, you must prove that it is both surjective and injective.

The following more sophisticated method is often convenient.

Lemma 19.2. Suppose $f : S \rightarrow T$ and $g : T \rightarrow S$ are functions such that $g(f(s)) = s$ for all $s \in S$. Then f is injective and g is surjective. If, in addition, $f(g(t)) = t$ for all $t \in T$, then f and g are bijective and $g = f^{-1}$.

Proof. To prove that f is injective, let $s_1, s_2 \in S$, and suppose $f(s_1) = f(s_2)$. Apply g to both sides, and get

$$s_1 = g(f(s_1)) = g(f(s_2)) = s_2.$$

So $s_1 = s_2$. This proves that f is injective.

To prove that $g : T \rightarrow S$ is surjective, we suppose $s \in S$ (since S is the target space for g). Define $t \in T$ by $t = f(s)$. Then $g(t) = g(f(s)) = s$. Hence $g(t) = s$. This proves that g is surjective.

If, in addition, we have $f(g(t)) = t$ for all $t \in T$, then we can use what has just been proved, with f and g interchanged, to see that f and g are both injective and surjective, hence bijective. Since $g(t)$ is the unique element in the fiber of f over t , we see that $g = f^{-1}$. \square

Lemma 19.3. The composition of two bijections $f : S \rightarrow T$, $g : T \rightarrow U$ is a bijection $g \circ f : S \rightarrow U$.

Proof. Exercise. \square

20. Permutations — A bijection $\sigma : X \rightarrow X$ from a set X to itself is called a **permutation**. Let \mathcal{S}_X be the set of permutations of X . This set forms a group, where the multiplication law is composition. The identity element of the group \mathcal{S}_X is the identity function $\sigma(t) = t$.

If X is finite, say $X = \{1, 2, \dots, n\}$, then we write \mathcal{S}_n instead of \mathcal{S}_X . The group \mathcal{S}_n is finite, of order

$$|\mathcal{S}_n| = n!.$$

Every element in $\sigma \in \mathcal{S}_n$ can be represented by the array

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

For example, the arrays

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ n & 1 & 2 & \dots & n-1 \end{pmatrix}$$

represent the identity and the cycle $n \rightarrow n-1 \rightarrow \dots \rightarrow 2 \rightarrow 1 \rightarrow n$.

The group \mathcal{S}_X is non-abelian (non-commutative) if $|X| \geq 3$, or if $|X|$ is infinite.

21. General functions — A function $f : S \rightarrow T$ may be neither injective nor surjective, even if $S = T$. However, any f can be modified into a bijection as follows. First replace T by $f(S)$. The “new” function $f : S \rightarrow f(S)$ is automatically surjective. Next let \bar{S} be the set of non-empty fibers of f . These fibers are the equivalence classes for the equivalence relation on S defined by $s \sim s'$ if $f(s) = f(s')$. Thus, every element $x \in \bar{S}$ is an equivalence class, and f takes a unique value on this class. We define $\bar{f}(x) \in T$ to be the unique value that f takes on x . In other words, if x is the fiber $f^{-1}(t)$, then $\bar{f}(x) = t$.

Lemma 21.1. *The function $\bar{f} : \bar{S} \rightarrow f(S)$ just defined is a bijection.*

Proof. Let $t \in f(S)$. Then there is some $s \in S$ such that $f(s) = t$. Hence the fiber $x = f^{-1}(t)$ is non-empty, and $\bar{f}(x) = t$. This proves \bar{f} is surjective. Suppose that $\bar{f}(x_1) = \bar{f}(x_2)$. This means that f takes the same value, say t , on the fibers x_1 and x_2 . Hence $x_1 = f^{-1}(t) = x_2$. This means that \bar{f} is injective. \square

For example, let $f : \mathbb{R} \rightarrow \mathbf{C}$ be the function $f(x) = e^{2\pi ix}$. Then $f(\mathbb{R})$ is the unit circle C , and the equivalence relation on \mathbb{R} is defined by $x \sim x'$ if $x' - x$ is an integer. For this equivalence relation we denote the set of equivalence classes by \mathbb{R}/\mathbb{Z} . Each class looks like $\{t, t + 1, t - 1, t + 2, t - 2, \dots\}$. Lemma 20.1 says there is exactly one equivalence class for every point in C . More precisely, the original function $f : \mathbb{R} \rightarrow \mathbf{C}$ becomes a bijection $\bar{f} : \mathbb{R}/\mathbb{Z} \rightarrow C$.

22. Countable Sets — A set S is called **countable** if there is a bijection

$$f : \mathbb{N} \rightarrow S.$$

If we let $s_1 = f(1)$, $s_2 = f(2)$, etc, then

$$S = \{s_1, s_2, \dots\}.$$

Conversely, given such a listing, we can define f , so a set is countable if and only if it can be listed.

For example, $\mathbb{N} \times \mathbb{N}$ is countable. One way to see this is to view $\mathbb{N} \times \mathbb{N}$ as the array of dots in the first quadrant of the xy plane. Starting at $(1, 1)$ we draw a path snaking back and forth on the diagonals, so that every point in $\mathbb{N} \times \mathbb{N}$ is on the path. Let $f : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ be the function $f(n) = n^{\text{th}}$ point visited on the path. So

$$\begin{aligned} f(1) &= (1, 1), & f(2) &= (1, 2), & f(3) &= (2, 1), & f(4) &= (3, 1), & f(5) &= (2, 2), \\ f(6) &= (1, 3), & f(7) &= (1, 4), & \text{etc.} \end{aligned}$$

Then f is a bijection because every point in $\mathbb{N} \times \mathbb{N}$ equals $f(n)$ for a unique n . It follows that the product of two countable sets is countable. By induction, it is then easy to prove

Lemma 22.1. *The product of any finite number of countable sets is countable.*

Sometimes it is not necessary to have a bijection $f : \mathbb{N} \rightarrow S$ in order to conclude that S is countable.

Lemma 22.2. *If S is an infinite set, T is a countable set, and there is an injection $g : S \rightarrow T$ then S is countable.*

Proof. Since T is countable, we can suppose $T = \mathbb{N}$. Since $g : S \rightarrow g(S)$ is a bijection, it suffices to show that any infinite subset $A \subset \mathbb{N}$ is countable. Let a_1 be the smallest element of A , let a_2 be the smallest element of $A - \{a_1\}$, and recursively, let a_n be the smallest element in $A - \{a_1, \dots, a_{n-1}\}$. Note that the latter set is non-empty for every n , since A is infinite. Then $A = \{a_1, a_2, \dots\}$ is a listing of A , so A is countable. \square

Lemma 22.3. *If S is a countable set, and there is a surjection $f : S \rightarrow T$, then T is countable.*

Proof. Again, we may suppose $S = \mathbb{N}$. Note the given surjection may not be a bijection, as required in the original definition of countability. We instead use f to construct an injection $g : T \rightarrow \mathbb{N}$. Let $t \in T$, and consider the fiber $f^{-1}(t) \subset \mathbb{N}$. Note that every fiber of f is non-empty, since f is surjective. Define $g(t) \in \mathbb{N}$ be the smallest number in the fiber $f^{-1}(t)$. Note that $f(g(t)) = t$ for every $t \in T$. Hence g is injective by Lemma 19.2. \square

For example, let \mathbb{Q}_+ be the set of positive rational numbers. Consider the function

$$f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Q}_+$$

defined by $f(x, y) = \frac{x}{y}$. Then f is surjective, by the definition of rational number. We have seen that $\mathbb{N} \times \mathbb{N}$ is countable. By 22.3 it follows that \mathbb{Q}_+ is countable.

The most powerful theorem of this sort is the following.

Theorem 22.4. *A countable union of countable sets is countable.*

Proof. The theorem says that if I is a countable set, and for each element $i \in I$ we are given a countable set A_i , then the union

$$A = \bigcup_{i \in I} A_i$$

is countable. Once again we may suppose in the proof that $I = \mathbb{N}$, although in applications of this theorem, the set I is in bijection with \mathbb{N} , but not usually equal to \mathbb{N} .

So assume we have countable sets A_1, A_2, \dots . We want to show that their union

$$A = A_1 \cup A_2 \cup \dots$$

is countable. Let us write

$$A_i = \{a_{ij} : j \in \mathbb{N}\}.$$

Define $f : \mathbb{N} \times \mathbb{N} \rightarrow A$ by $f(i, j) = a_{ij}$. Clearly f is surjective, and we know $\mathbb{N} \times \mathbb{N}$ is countable, so A is countable by 22.3. \square

If some of the sets A_i are finite, instead of countable, the proof and conclusion of 22.4 still hold. Just allow repetitions among the a_{ij} 's. It is also clear that if I is finite, and each A_i is countable or finite, then A is countable except that if all A_i are finite, and then of course A is finite.

As a simple example,

$$\mathbb{Q} = \mathbb{Q}_+ \cup \{0\} \cup (-\mathbb{Q}_+),$$

and \mathbb{Q}_+ is countable, so the set of all rational numbers is countable. But much more is true.

Consider the set $\bar{\mathbb{Q}}$ of algebraic numbers. Recall that these are the complex roots of polynomials with rational coefficients. Let P_n be the set of polynomials of the form $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, with all $a_i \in \mathbb{Q}$. There is an obvious bijection

with $\mathbb{Q}^n \rightarrow P_n$. Since \mathbb{Q} is countable, we know \mathbb{Q}^n is countable by 19.1. Hence P_n is countable. Now the set of all polynomials is the union

$$P = \bigcup_{n \in \mathbb{N}} P_n,$$

so P is countable. For any polynomial p , let $Z(p)$ be the set of zeros of p . Then $Z(p)$ contains at most n elements, where n is the degree of p . Finally,

$$\bar{\mathbb{Q}} = \bigcup_{p \in P} Z(p),$$

so the set of all algebraic numbers is countable.

23. Uncountable Sets —

A set S is called **uncountable** if it is infinite and not countable. There are two ways to prove that a set S is uncountable. Either try to list S , and find a contradiction, or find a bijection between S and a known uncountable set. The basic uncountable set is given in the following theorem, called the “Cantor diagonal argument”.

Theorem 23.1. *The interval $(0, 1)$ is uncountable.*

Proof. Every element in $(0, 1)$ can be expressed uniquely as a decimal with infinitely many nonzero digits (eg, $.5 = .4999999 \dots$). Assume $(0, 1)$ is countable, say

$$(0, 1) = \{\alpha_1, \alpha_2, \dots\},$$

where

$$\alpha_i = .a_{i1}a_{i2}\dots,$$

with infinitely many $a_{ij} \neq 0$. For each i , choose an integer b_i between 1 and 9, such that $b_i \neq a_{ii}$. Then the decimal $\beta = .b_1b_2\dots$ is not on the list because it differs from α_i in the i th decimal place. So we have found a number in $(0, 1)$ which is not on the list. This is a contradiction to the assumed countability of $(0, 1)$. \square

Any subset of an uncountable set is uncountable, as follows from 22.2. Hence any subset of real numbers containing $(0, 1)$ is uncountable. Since it is easy to find a bijection from any open interval to $(0, 1)$, it follows that any subset of \mathbb{R} containing an open interval, no matter how small, is uncountable. In particular, \mathbf{C} is uncountable. Now, we have proved that the rational and algebraic numbers are countable. This proves

Theorem 23.2. *The sets of irrational and transcendental numbers are each uncountable.*

Thus, there are “many more” transcendental numbers than algebraic numbers. However, only a handful of numbers have been proved to be transcendental, and all these proofs are too hard for this course.

Here are other examples of uncountable sets.

Example 23.3. The set S of all infinite sequences $s = (s_1, s_2, \dots)$, where $s_i \in \{0, 1\}$ for all i , is uncountable.

Proof. The Cantor diagonal argument works here too. Or we could define a map

$$f : S \longrightarrow [0, 1]$$

by $f(s) = \sum_{i=1}^{\infty} s_i 2^{-i}$. Then f is surjective, since every number in $(0, 1)$ has a binary representation. Since we know $(0, 1)$ is uncountable, it follows from 22.3 that S is uncountable. \square

Example 23.4. The set \hat{S} of all permutations of \mathbb{N} is uncountable.

Proof. Let S be as in 23.3. Define a function $f : S \longrightarrow \hat{S}$ such that $f(s)$ is the permutation switching $(2i - 1, 2i)$ if $s_i = 1$, and leaving $(2i - 1, 2i)$ unchanged if $s_i = 0$. Then f is clearly injective. Since we have proved S is uncountable, it follows that \hat{S} is uncountable as well. \square

Example 23.4. The set T of all subsets of \mathbb{N} is uncountable.

Proof. Let S be as in 23.3 again. Define $f : S \longrightarrow T$ by

$$f(s) = \{i \in \mathbb{N} : s_i = 1\}.$$

Then f is injective, so T is uncountable. \square

On the other hand, if we take the set of all sequences in S with all but finitely many $s_i = 0$, or the set of all finite subsets of \mathbb{N} , or the set of all permutations of \mathbb{N} that fix all but finitely many $n \in \mathbb{N}$, then in each case, we get a countable set.

24. The Cantor set — This is an example of a sparse-looking set of real numbers, with zero “length” which is nevertheless uncountable.

Start with the interval

$$\Delta_0 = [0, 1].$$

Remove the open middle third, leaving a union of two intervals

$$\Delta_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1].$$

Remove the open middle third of each of these intervals, leaving a union of four intervals

$$\Delta_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{3}{9}] \cup [\frac{6}{9}, \frac{7}{9}] \cup [\frac{8}{9}, 1].$$

Repeat this indefinitely. At the k th stage we have a union of 2^k intervals

$$\Delta_k = [0, \frac{1}{3^k}] \cup [\frac{2}{3^k}, \frac{3}{3^k}] \cup \dots \cup [\frac{3^k - 1}{3^k}, 1],$$

each of length $\frac{1}{3^k}$. These intervals are “nested” in the sense that

$$\Delta_0 \supset \Delta_1 \supset \Delta_2 \supset \dots$$

The Cantor set \mathcal{C} is the set of points in $[0, 1]$ which belong to every interval Δ_k :

$$\mathcal{C} = \bigcap_{k=0}^{\infty} \Delta_k.$$

In other words, \mathcal{C} is what remains after you remove all the open middle thirds. The total length of what is removed equals 1 (a geometric series calculation) so \mathcal{C} has length zero. In fact, it is hard to see any elements in \mathcal{C} , besides the endpoints of the intervals, which are rational, hence form a countable subset of \mathcal{C} .

However, turns out that \mathcal{C} is uncountable. We will prove this by finding a bijection $f : S \rightarrow \mathcal{C}$, where S is the set of all 0/1 sequences, as in 23.3. Given $s \in S$, we define a sequence of connected subintervals $\Delta_k(s) \subset \Delta_k$ which are nested

$$\Delta_0(s) \supset \Delta_1(s) \supset \Delta_2(s) \supset \dots$$

as follows. Let $\Delta_0(s) = [0, 1]$. Assume $\Delta_{k-1}(s)$ has been defined, for $k \geq 1$. Let $\Delta_k(s)$ be the left closed third of $\Delta_{k-1}(s)$ if $s_k = 0$, and the right closed third of $\Delta_{k-1}(s)$ if $s_k = 1$. Thus s is used to make a sequence of binary decisions as to which interval to choose, at each step. Finally, $f(s)$ is the unique number contained in every $\Delta_k(s)$:

$$\{f(s)\} = \bigcap_{k=1}^{\infty} \Delta_k(s).$$

It is not hard to see that f is bijective. Since S is known to be uncountable, this proves \mathcal{C} is uncountable.

One can also show fairly easily that \mathcal{C} consists of those numbers in $[0, 1]$ which can be written in base 3 using only 0's and 2's. In fact, the first middle third consists of those numbers requiring a 1 in their first base 3 digit, the next middle thirds consist of those numbers requiring a 1 in the second digit, and so on. Replacing each 2 by a 1, and the base 3 by the base 2, we get a bijection from \mathcal{C} to $(0, 1)$, so in fact after removing all the middle thirds, we have just as many (in the sense of bijections) points as we started with.