

0. Preliminaries

Definition 0.1.

$\mathbb{N} = \{0, 1, 2, \dots, n \dots\}$ is the set of *non-negative integers*;

$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots -n, n, \dots\}$ is the set of *integers*;

$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z} \ \& \ n \neq 0\}$ is the set of *rational numbers*;

\mathbb{R} is the set of *real numbers*.

Set Notation and Functions

Suppose that $P(x)$ is a mathematical statement about x . $\{x : P(x)\}$ is the set of objects x such that $P(x)$ is true. For example, suppose that $P(x)$ is the statement: $x \in \mathbb{N}$ & (x is divisible by 2). In this case,

$$\{x : x \in \mathbb{N} \ \& \ (x \text{ is divisible by } 2)\}$$

is the set of those non-negative integers which are even. This same set may also be written as

$$\{x \in \mathbb{N} : x \text{ is divisible by } 2\}.$$

Quantifier abbreviations are often useful here. For example,

$$\{x \in \mathbb{N} : \exists y \in \mathbb{N}(x = 2 \times y)\}$$

is also the set of even non-negative integers. We also have sets whose members are ordered pairs of objects. One example is

$$\{(x, y) : x, y \in \mathbb{R} \ \& \ y < x^2\}.$$

A member of this set is an ordered pair of real numbers. (What does this set look like if we draw its picture on the x, y coordinate system?)

Definition 0.2. Let A and B be two sets.

i) $A \cup B = \{x : x \in A \text{ or } x \in B\}$; (the *union of A and B*)

ii) $A \cap B = \{x : x \in A \text{ and } x \in B\}$; (the *intersection of A and B*).

- iii) $A \setminus B = \{x : x \in A \ \& \ x \notin B\}$;
 iv) $A \times B = \{(x, y) : x \in A \ \& \ y \in B\}$ (the *cartesian product of A and B*) is the set of ordered pairs whose first coordinate is in A and whose second coordinate is in B ;
 Similarly,

$$A \times B \times C = \{(x, y, z) : x \in A \ \& \ y \in B \ \& \ z \in C\}$$

- v) $A \subseteq B$ if every member of A is a member of B (A is a *subset* of B).
 vi) $A \subset B$ if $A \subseteq B$ but $A \neq B$ (A is a *proper subset* of B).
 vii) If A_n is a set for each $n \in \mathbb{N}$ then $\bigcup\{A_n : n \in \mathbb{N}\}$ (the *union* of the sets A_n) is the set:

$$\bigcup\{A_n : n \in \mathbb{N}\} = \{x : \exists n \in \mathbb{N} \ x \in A_n\} .$$

An object x belongs to this union iff x belongs to at least one of the sets A_n . Note that $\{A_n : n \in \mathbb{N}\}$ is a set each of whose members is a set, i.e. it is a set of sets. More generally:

- viii) Suppose X is a set of sets. Then

$$\bigcup X = \{x : \exists y \in X \ [x \in y]\}$$

is the union of the sets in X .

Definition 0.3 (Informal Definition). A *function* f consists of

- i) A set called the *domain* of f , written $\text{dom}(f)$, and
 ii) a ‘‘correspondence’’ which associates with each member x of $\text{dom}(f)$ a unique *value* $f(x)$.¹

Suppose f is a function. In the expression $f(x)$, x is called the *argument*, and $f(x)$ is called the *value* of the function f at argument x . The set

$$\{f(x) : x \in \text{dom}(f)\}$$

of values of the function f is called the *range* of f and is written $\text{ran}(f)$ (or sometimes $\text{rng}(f)$).

Suppose f is a function. The *graph* of f is the set of pairs

$$\{(x, f(x)) : x \in \text{dom}(f)\} .$$

Note that from the graph of f we can determine both $\text{dom}(f)$ and $\text{ran}(f)$. Members of the domain of f are the first coordinates of pairs belonging to the graph of f , and members of the range of f are second coordinates of pairs

¹ This is not a good mathematical definition since the word ‘correspondence’ has not been defined.

belonging to f . Since the graph of f uniquely determines f , it is customary to identify a function with its graph. A precise definition of ‘function’ can then be given as follows:

Definition 0.3' A function is a set of ordered pairs f such that:

$$\forall x \forall y \forall z [(x, y) \in f \ \& \ (x, z) \in f \implies y = z] .$$

If f is a function, then

$$\begin{aligned} \text{dom}(f) &= \{x : \exists y (x, y) \in f\} ; \\ \text{ran}(f) &= \{y : \exists x (x, y) \in f\} . \end{aligned}$$

Note that the statement $f(x) = y$ is equivalent to the statement $(x, y) \in f$.

Definition 0.4. Suppose f is a function.

i) f is *one-to-one* (or 1-1) if for all $x \in \text{dom}(f)$,

$$f(x) = f(y) \implies x = y .$$

- ii) $f: A \rightarrow B$ (f maps A into B) means $A = \text{dom}(f)$ and $\text{ran}(f) \subseteq B$;
- iii) $f: A \rightarrow B$ (f maps A onto B) means $A = \text{dom}(f)$ and $\text{ran}(f) = B$;
- iv) $f: \subseteq A \rightarrow B$ means $\text{dom}(f) \subseteq A$ and $\text{ran}(f) \subseteq B$.
- v) $f: A \xrightarrow{1-1} B$ means $f: A \rightarrow B$ and f is one-to-one.

Functions of two or more variables are actually special cases of the above definition. A function of two variables is a function f whose domain is a set of ordered pairs. For example the function $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ (the addition function on \mathbb{N}) is really the set $\{(x, y, z) : x, y \in \mathbb{N} \ \& \ x + y = z\}$. A member of the domain of this function $+$ is a pair (x, y) where x and y are in \mathbb{N} .

Let A be a subset of some set U .² The *characteristic function* of A (with respect to the set U) is the function C_A , where³ for all $x \in U$,

$$C_A(x) = \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{otherwise.} \end{cases}$$

² Neither A nor U need be subsets of \mathbb{N} or indeed have any connection with \mathbb{N} whatsoever.

³ The characteristic function is sometimes defined with values 0 and 1 interchanged.

One-To-One Correspondence

Definition 0.5. Let A and B be two sets. A *one-to-one* (1-1) *correspondence* between A and B is a function f such that $f: A \xrightarrow{1-1} B$.

Example 0.6. Let

$$f = \{(3, \sqrt{2}), (-\pi, 0), (6, -2/3)\}.$$

Then:

- a) f is function (check the definition!)
- b) $\text{dom}(f) = \{3, -\pi, 6\}$, and $\text{ran}(f) = \{\sqrt{2}, 0, -2/3\}$.
- c) f is 1-1.

It follows that f is a 1-1 correspondence between $A = \{3, -\pi, 6\}$ and $B = \{\sqrt{2}, 0, -2/3\}$. Note that both A and B have 3 members. In general, if A is a set with n members (where $n \in \mathbb{N}$), and there exists a one-to-one correspondence between A and B , then B will also have n members.

Definition 0.7. The set A is

- empty* if A has no members (The empty set is denoted by \emptyset);
- finite* if for some $n \in \mathbb{N}$, A has n members;⁴
- infinite* if A is not finite;
- enumerable* if there exists a 1-1 correspondence between \mathbb{N} and A ;⁵
- countable* if A is finite or enumerable;
- uncountable* if A is not countable.

Remark.

- 1) If A is enumerable there is a *listing* $a_0, a_1, \dots, a_n, \dots$ *without repetitions* of the members of A (the subscripts are the members of \mathbb{N}). There are of course many different such listings of the same enumerable set, and each such listing might be very complicated.
- 2) Conversely, if there is a listing $a_0, a_1, \dots, a_n, \dots$ without repetitions of the members of A , then A is enumerable. (The one-to-one correspondence between \mathbb{N} and A is given by the function f , where $f(n) = a_n$.)
- 3) If A is countable and non-empty, then there is a listing $a_0, a_1, \dots, a_n, \dots$ of the members of A (*with repetitions* if A is finite)

Proposition 0.8.

- 1) If A is enumerable and $B \subseteq A$ then B is countable.
- 2) If A is finite and $B \subseteq A$, then B is finite.

⁴ So the empty set \emptyset is finite.

⁵ Enumerable sets are also called *denumerable*.

3) If B is infinite and $B \subseteq A$, then A is infinite.

Theorem 0.9.

- a) If A and B are both countable, then $A \times B$ is countable.
 b) If each of A_1, \dots, A_k is countable then $A_1 \times \dots \times A_k$ is countable.

Theorem 0.10. \mathbb{Q} is enumerable.

Theorem 0.11. If each of the sets $A_0, A_1, \dots, A_n, \dots$, $n \in \mathbb{N}$, is countable, then $\bigcup \{A_n : n \in \mathbb{N}\}$ is countable.

Let A be an arbitrary set. We look at the set of all finite sequences from A . For example, if $a, b, c \in A$, then (a, b, c) is a sequence from A of length three. We also find it convenient to consider the *empty* sequence (the sequence of length 0) as being a finite sequence.

Theorem 0.12. If $A \neq \emptyset$ is countable then the set of all finite sequences from A is enumerable.

If A and B are finite sets, where A has n members and B has m members, then B is 'bigger' than A iff $m > n$. The following definition gives us an appropriate definition of 'bigger' which works for both finite and infinite sets.

Definition 0.13.

- i) $A \preceq B$ if there is some function f such that $f: A \xrightarrow{1-1} B$; that is, $A \preceq B$ if there is a 1-1 correspondence between A and some subset of B .
 ii) $A \prec B$ if $A \preceq B$, but *not* $B \preceq A$.
 iii) $A \equiv B$ if $A \preceq B$ and $B \preceq A$.

We may think of:

$A \preceq B$ as a way of saying 'B is at least as big as A' (or 'A is not bigger than B').

$A \prec B$ as a way of saying 'B is bigger than A.'

$A \equiv B$ as a way of saying 'A and B are the same size.'

Exercise 0.14. Show that if B is countable and $A \preceq B$ then A is countable.

There is another reasonable way of saying two sets are the same size: One might say that the sets A and B are the same size if there is a one-to-one correspondence between A and B . Is this equivalent to saying $A \equiv B$? Fortunately, we have the following result. We do not give a proof here.

However, the proof is not *too* hard and you are encouraged to try to show why it is true.

Theorem 0.15 (Cantor-Bernstein). $A \equiv B$ iff there is a one-to-one correspondence between A and B .

It is quite possible that $A \equiv B$ even though A is a *proper* subset of B . The following is an example.

Example 0.16. Let $E = \{x \in \mathbb{N} : x \text{ is even}\}$. Then $E \equiv \mathbb{N}$.

Is there a ‘largest’ set?

Definition 0.17. For any set A ,

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

$\mathcal{P}(A)$ is called the *power set* of A .

Exercise 0.18 (Counting Subsets). We count the number of subsets of a given finite set. Note that every set is a subset of itself; that is, for every set A , we have $A \subseteq A$.⁶

- a) List all the subsets of:
 - 1) \emptyset (the set with no members);
 - 2) A , where $A = \{a\}$ is a set with one member;
 - 3) B , where $B = \{a, b\}$ is a set with two members (i.e. $a \neq b$);
 - 4) C , where $C = \{a, b, c\}$ is a set with three members;
- b) Let A be a set of objects, and b be an object not in A . Suppose A has n subsets. How many subsets has $A \cup \{b\}$? (*Hint:* How many subsets of $A \cup \{b\}$ are there which have b as a member? How many subsets of $A \cup \{b\}$ are there which do *not* have b as a member?)
- c) Show by induction: For each $n \in \mathbb{N}$, if A has n members, then $\mathcal{P}(A)$ has 2^n members.

Theorem 0.19 (Cantor). For every set A ,

$$A \prec \mathcal{P}(A).$$

Corollary 0.20.

- i) For every A there is a B such that $A \prec B$.
- ii) $\mathcal{P}(\mathbb{N})$ is uncountable.

⁶ So every set has at least one subset.

The following notation is convenient.

Definition 0.21. For any sets A and B ,

${}^A B$ is the set of all functions f such that $f: A \rightarrow B$.

Theorem 0.22. ${}^{\mathbb{N}}\mathbb{N}$ is uncountable.

The idea behind the proof of Cantor's Theorem will be used in this course a number of times in different contexts. It is called a *diagonal argument*. In order to understand the idea behind the proof, we look at the proof in a simpler setting, namely that of Corollary 20(ii).

Proof of 20(ii). We give a proof by contradiction. Suppose that $\mathcal{P}(\mathbb{N})$ is countable. Since each of $\{0\}, \{1\}, \dots, \{n\}, \dots$ is in $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathbb{N})$ must be infinite, and hence enumerable. Thus there is a listing $A_0, A_1, \dots, A_n, \dots$ of the members of $\mathcal{P}(\mathbb{N})$. The contradiction will be found by defining a subset B of \mathbb{N} which is different from each of the sets A_0, A_1, \dots . Let C_0 be the characteristic function of the set A_0 , C_1 be the characteristic function of A_1 , and in general, C_n be the characteristic function of A_n . For $i, j \in \mathbb{N}$, let $c_{i,j} = C_i(j)$. So, for each i and j ,

$$c_{i,j} = \begin{cases} 1, & \text{if } j \in A_i; \\ 0, & \text{otherwise.} \end{cases}$$

Think of the numbers $c_{i,j}$ as being arranged in an infinite square with the number $c_{i,j}$ in the $i + 1$ -st row and $j + 1$ -st column. So the numbers $c_{n,n}$ appear on a diagonal of the infinite square (the diagonal running from the upper left towards the lower right). Now let

$$d(n) = \begin{cases} 1, & \text{if } c_{n,n} = 0, \\ 0, & \text{if } c_{n,n} = 1. \end{cases}$$

d is called a *diagonal* function since it changes the values of the numbers on the diagonal of the square. Let

$$B = \{n : d(n) = 1\}.$$

Then $B \subseteq \mathbb{N}$, i.e. $B \in \mathcal{P}(\mathbb{N})$, and for all n ,

$$\begin{aligned} n \in B &\iff d(n) = 1 \\ &\iff c_{n,n} = 0 \\ &\iff n \notin A_n. \end{aligned}$$

It follows that B is different from each of the sets A_0, A_1, \dots ; for suppose that for some n_0 , $B = A_{n_0}$. This gives the contradiction:

$$\begin{aligned} n_0 \in A_{n_0} &\iff n_0 \in B \\ &\iff n_0 \notin A_{n_0}. \end{aligned} \quad \square$$

Exercise 0.23. Let A be an enumerable set. By definition, there is a function

$$f: \mathbb{N} \xrightarrow{1-1} A. \quad (*)$$

But there is not a unique such function f . Let \mathcal{F} be the set of all functions which satisfy (*). Is \mathcal{F} countable? Explain why.

Relations on a set

Definition 0.24 Let A be a set.

- a) A subset of $A \times A$ is a *2-ary (binary) relation on A* .
- b) A subset of $A \times A \times A$ is a *3-ary (ternary) relation on A* .
- c) More generally, a subset of $\underbrace{A \times \cdots \times A}_n$ is an *n -ary relation on A* .

Notation 0.24. If R is an n -ary relation on A , then $R(a_1, \dots, a_n)$ means $(a_1, \dots, a_n) \in R$. If R is a binary relation on A , we sometimes write aRb to mean $R(a, b)$.

Example 0.25. The sets

$$\begin{aligned} &\{(m, n) : m \in \mathbb{N} \ \& \ n \in \mathbb{N} \ \& \ m < n\} \\ &\{(m, n) : m \in \mathbb{N} \ \& \ n \in \mathbb{N} \ \& \ m > n\} \\ &\{(m, n) : m \in \mathbb{N} \ \& \ n \in \mathbb{N} \ \& \ m = n\} \end{aligned}$$

are binary relations on \mathbb{N} called respectively the *less than* relation on \mathbb{N} , the *greater than* relation on \mathbb{N} , and the *equality* (or *identity*) relation on \mathbb{N} , and are abbreviated, respectively as $<^{\mathbb{N}}$, $>^{\mathbb{N}}$, and $=^{\mathbb{N}}$. Thus, for example,

$$a <^{\mathbb{N}} b \iff <^{\mathbb{N}}(a, b) \iff (a, b) \in \mathbb{N} \times \mathbb{N} \ \& \ a < b.$$