1 Sets and Functions

1.1 Introduction to Set Theory

In this section we will consider some basic concepts in Set Theory. We will start with the definition of a set:

Definition 1.1. A *set* is a collection of objects. These objects are called the *elements* of the set.

Example 1.2. The *Natural numbers* $\mathbb{N} = \{1,\ 2,\ 3,\ ...\ \}$ is a set and the number 20 is an element of this set. Note that 0 is not an element of $\mathbb{N}$.

Notation:

- We will usually use capital letters for sets and lowercase letters for elements of sets.
- We write $a \in A$ if a is an element of the set A.
- If b is not an element of A, we write $b \notin A$.

It is not always easy to specify the elements of a set. If the set A has a small number of elements, we could list them: for example if A has three elements $a,\ b$, and c then we write

$$A = \{a,\ b,\ c\}$$

We also took this approach with the set $\mathbb{N}$ above. However, sometimes it is not useful or practical to take this approach and it is clearer to describe a property that specifies the elements of the set: for example we could describe the set $A = \{5,\ 6,\ 7,\ ...\ \}$ as

$$A = \{x \in \mathbb{N} | x > 4\}.$$

Example 1.3. There are often many ways of describing the same set.
Let $C = \{x \in \mathbb{N} | x^2 - 3x + 2 = 0\}$. We can check that $C = \{1,\ 2\}$. We can also see that we could describe C as $\{x \in \mathbb{N} | x < 3\}$.

Definition 1.4. Define the set of *Integers* as

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, ...\}.$$

The set of *Rational numbers* as

$$\mathbb{Q} = \{p/q\ | p, q \in \mathbb{Z}, q \neq 0\}.$$

It is not so easy to give a precise definition of the set of Real numbers. For the moment we will say that the set of real numbers $\mathbb{R}$ is the set of all numbers on the number line.

Notice that given a set A and an element x then exactly one of the following holds: $x \in A$; $x \notin A$.

Definition 1.5. Suppose A and B are both sets and suppose that all elements of A are also elements of B (that is if $x \in A$ then $x \in B$), then we say A is a *subset* of B and write $A \subset B$. If in addition there is an element $y \in B$ which is not an element of A then we say that A is a *proper subset* of B.

Example 1.6.

1. The even whole numbers $E = \{2,\ 4,\ 6,\ 8, \dots\ \}$ is a proper subset of $\mathbb{N}$.
2. Consider the set $D = \{0, 1\}$. Then $D \subset \mathbb{Z}$ but D is not a subset of $\mathbb{N}$.
3. We have $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Note: If $A \subset B$ and $B \subset A$ then $A = B$. (Can you explain why this is true?)

Set Operations

Definition 1.7. If A and B are sets then their *intersection* is the set of all elements that belong to both A and to B. We write $A \cap B$.

Example 1.8. Let $A = \{2, 4, 6, 8, 10\}$, $B = \{6, 10, 13\}$ and $C = \{1, 13\}$. Then $A \cap B = \{6, 10\}$, $B \cap C = \{13\}$ and there are no elements in $A \cap C$.
We write $\emptyset$ for the empty set so we have $A \cap C = \emptyset$.

Definition 1.9. If $A \cap B = \emptyset$ we say that they are *non-intersecting* or *disjoint*.

Definition 1.10. If A and B are sets then their *union* is the set of all elements that belong to either A or to B or to both. We write $A \cup B$.

Example 1.11. If we return to the last example we have $A \cup B = \{2, 4, 6, 8, 10, 13\}$, $B \cup C = \{1, 6, 10, 13\}$ and $A \cup C = \{1, 2, 4, 6, 8, 10, 13\}$.

Definition 1.12. If A and B are sets then the *complement* of B in A is the set of elements of A that are not in B. We denote it as $A - B$. That is

$$A - B = \{x \in A | x \notin B\}.$$

Note: In general $A - B \neq B - A$. For example if $B = \{6, 10, 13\}$ and $C = \{1, 13\}$ then $B - C = \{6, 10\}$ but $C - B = \{1\}$. If $A - B = B - A$, what can you say about A and B?

Definition 1.13. If A is a set then the *complement* of A is

$$C(A) = \{x | x \notin A\}.$$

Theorem 1.14. *Let A, B and C be any sets then*

1. $A \cap A = A$ *and* $A \cup A = A$ *(The Idempotent Law)*
2. $A \cap B = B \cap A$ *and* $A \cup B = B \cup A$ *(The Commutative Law)*

3. $(A \cap B) \cap C = A \cap (B \cap C)$ *and* $(A \cup B) \cup C = A \cup (B \cup C)$ *(The Associative Law)*

4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(The Distributive Law)*

Proof: Let's prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ from part *4*. We will use the fact that if X and Y are sets with $X \subset Y$ and $Y \subset X$ then $X = Y$. So here we need to show that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$ and that $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Recall that to show $X \subset Y$ we need to show that for all elements $x \in X$ we have $x \in Y$.

Let $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$. So $x \in A$, and either $x \in B$ or $x \in C$.
Case 1: If $x \in B$, then $x \in A$ and $x \in B$ so $x \in A \cap B$.
Case 2: If $x \in C$, then $x \in A$ and $x \in C$ so $x \in A \cap C$.
So either $x \in A \cap B$ or $x \in A \cap C$. In other words $x \in (A \cap B) \cup (A \cap C)$.
So we have shown that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$.

Now we need to show that $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.
Let $y \in (A \cap B) \cup (A \cap C)$ then either $y \in A \cap B$ or $y \in A \cap C$.
Case 1: If $y \in A \cap B$, then $y \in A$ and $y \in B$.
Case 2: If $y \in A \cap C$, then $y \in A$ and $y \in C$.
In any case $y \in A$ and either $y \in B$ or $y \in C$. So $y \in A$ and $y \in B \cup C$. In other words $y \in A \cap (B \cup C)$.
Thus $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$, as required.

We have shown that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$ and that $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. We conclude that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

□

Exercise 1.15. *Your turn:* Prove the rest of the theorem above. Remember to use the fact that if $A \subset B$ and $B \subset A$ then $A = B$.

Notation: Since by part *3.* of the previous theorem $A \cap (B \cap C) = (A \cap B) \cap C$ we often write it as $A \cap B \cap C$. Similarly we write $A \cup B \cup C$ for $A \cup (B \cup C) = (A \cup B) \cup C$.
We can generalise and write:

$$\cap_{k=1}^{n} A_k = A_1 \cap A_2 \cap A_3 \cap ... \cap A_n = \{x | x \in A_k \text{ for all } k = 1, ..., n\}.$$

$$\cup_{k=1}^{n} A_k = A_1 \cup A_2 \cup A_3 \cup ... \cup A_n = \{x | x \in A_k \text{ for some } k = 1, ..., n\}.$$

Similarly we write

$$\cap_{k=1}^{\infty} A_k = \cap_{k \in \mathbb{N}} A_k = \{x | x \in A_k \text{ for all } k \in \mathbb{N}\}.$$

$$\cup_{k=1}^{\infty} A_k = \cup_{k \in \mathbb{N}} A_k = \{x | x \in A_k \text{ for some } k \in \mathbb{N}\}.$$

Example 1.16. For each $k \in \mathbb{N}$ let $A_k = [0,k]$. So $A_1 = [0,1]$, $A_2 = [0,2]$ etc. Then

$$\cup_{k=1}^{n} A_k = [0,n]$$

and

$$\cap_{k=1}^{n} A_k = [0,1].$$

Also $\cup_{k\in\mathbb{N}} A_k = [0,\infty)$ and $\cap_{k\in\mathbb{N}} A_k = [0,1]$. Can you explain why?

Exercise 1.17. *Your turn:* For each $k \in \mathbb{N}$ let $A_k = [1/k, 1]$. Find:

1. $\cup_{k\in\mathbb{N}} A_k$;
2. $\cap_{k\in\mathbb{N}} A_k$.

Theorem 1.18. *Let A, B and C be any sets then*

$$A - (B \cup C) = (A - B) \cap (A - C)$$

$$A - (B \cap C) = (A - B) \cup (A - C)$$

Proof: We will prove that $A - (B \cup C) = (A - B) \cap (A - C)$ and leave the proof of the second statement as an exercise.
If $x \in A - (B \cup C)$ then $x \in A$ and $x \notin B \cup C$. That means that $x \in A$ and $x \notin B$, $x \notin C$.
Now $x \in A$ and $x \notin B$ means that $x \in A - B$.
And $x \in A$ and $x \notin C$ means that $x \in A - C$.
Thus $x \in (A - B) \cap (A - C)$.
So we have shown that $A - (B \cup C) \subset (A - B) \cap (A - C)$. (*)

Now suppose that $y \in (A - B) \cap (A - C)$. Then $y \in A - B$ and $y \in A - C$.
This means that $y \in A$ and $y \notin B$ and $y \notin C$. So $y \in A$ and $y \notin B \cup C$.
Thus $y \in A - (B \cup C)$. Thus we have shown that $(A - B) \cap (A - C) \subset A - (B \cup C)$. (**)
From (*) and (**) we have $A-(B\cup C) \subset (A-B)\cap(A-C)$ and $(A-B)\cap(A-C) \subset A-(B\cup C)$, thus $A - (B \cup C) = (A - B) \cap (A - C)$.

□

Definition 1.19. If A and B are two non-empty sets then the *Cartesian product* $A \times B$ of A and B is the set of all ordered pairs (a,b) with $a \in A$ and $b \in B$.

Note that you have seen the Cartesian product of sets many times before. For example $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x,y) | x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$ is the usual xy-plane. Similarly $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

Example 1.20. Let $A = \{1,2,3\}$ and $B = \{-1,0\}$. Then

$$A \times B = \{(1,-1),(1,0),(2,-1),(2,0),(3,-1),(3,0)\}.$$

1.2 Functions

You are already very familiar with the concept of functions. The definition given in Calculus courses is usually:

Definition 1.21. Given two sets A and B, a *function* from A to B is a rule that associates to each element of A a single element of B. We write $f : A \to B$. Given $x \in A$, we write $f(x)$ for the unique element of B associated to it. The set A is called the *domain* of f and the *range* or *image* of f is the subset of B given by $\{y \in B | y = f(x) \text{ for some } x \in A\}$.

Sometimes we can write down a specific formula for a function. For example:

$$f : \mathbb{R} \to \mathbb{R} \quad f(x) = x^2 - 3.$$

Sometimes we need more than one formula to describe the function. For example, Dirichlet's function is:

$$g : \mathbb{R} \to \mathbb{R} \quad g(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \in \mathbb{R} - \mathbb{Q} \end{cases}$$

Similarly the absolute value function is described as

$$h(x) = |x| = \begin{cases} -x & x < 0 \\ x & x \geq 0 \end{cases}$$

Sometimes we have no 'formula' at all. For example, let $A = \{\text{cat, dog, mouse}\}$ and let $B = \{\text{house, garden}\}$, then we can define a function $f : A \to B$ by $f(\text{cat}) = \text{house}$, $f(\text{dog}) = \text{garden}$, and $f(\text{mouse}) = \text{house}$. (*Check that this satisfies the definition of a function, and find a different function $g : A \to B$. Can you find an example of a mapping $h : A \to B$ which is not a function?*)

There are some problems with the definition of a function given above. It is not precise enough and therefore open to interpretation. We have a more formal version:

Definition 1.22. Let A and B be sets. A *function* from A to B is a set f of ordered pairs in $A \times B$ with the property that if (a, b) and (a, b') are elements of f then $b = b'$.

Note: here the domain of f is the set $\{a \in A | \ a$ appears as the first member of an element of $f\}$. We usually think of f as a set of pairs $(a, f(a))$.

Definition 1.23. Suppose $f : A \to B$ is a function. Suppose $C \subset A$. We can define the *restriction* of f to C as

$$f|_C : C \to B \text{ given by } f|_C(x) = f(x) \ \ \forall x \in C.$$

Example 1.24. Consider the following examples:

1. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = 3x + 7$. Then since $\mathbb{Z} \subset \mathbb{R}$ we can define the restriction $f|_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{R}$. We have $f|_Z(x) = 3x + 7$ for all $x \in \mathbb{Z}$.

2. Recall Dirichlet's Function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \in \mathbb{R} - \mathbb{Q} \end{cases}$.

   It is easy to see that $g|_{\mathbb{Q}}(x) = 1$ for all $x \in \mathbb{Q}$.

Definition 1.25. Suppose $f : A \to B$ and $g : B \to C$. We can define the *composition* $g \circ f : A \to C$ as $g \circ f(x) = g(f(x))$ for all x such that $f(x)$ is in the domain of g.

Example 1.26. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = 3x + 7$. Let $g : [0, \infty) \to \mathbb{R}$ be given by $g(x) = \sqrt{x}$. We can define $g \circ f(x) = \sqrt{3x + 7}$ if $f(x) = 3x + 7$ is in the domain of g; that is if $3x + 7 \geq 0$ or $x \in [-7/3, \infty)$.

Injections, Surjections, and Bijections

The concept of a bijection will be very important later in this chapter. We will first consider the notions of injections and surjections.

Definition 1.27. Let $f : A \to B$ be a function. We say that f is *injective* or *one-to-one* (1-1) if whenever $f(a_1) = f(a_2)$ for any two elements $a_1, a_2 \in A$ then $a_1 = a_2$. We say that f is an injection.

Example 1.28.

1. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x + 7$ is a one-to-one function since if $f(a_1) = f(a_2)$ then $3(a_1) + 7 = 3(a_2) + 7$ or $3(a_1) = 3(a_2)$ which means that $a_1 = a_2$. Therefore by the definition above we see that f is a one-to-one function.

2. The function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ is a not one-to-one function since it is possible to find $a_1, a_2 \in \mathbb{R}$ where $g(a_1) = g(a_2)$ but $a_1 \neq a_2$. For instance, let $a_1 = -5, a_2 = 5$ then $g(a_1) = 25 = g(a_2)$ but $a_1 = -5 \neq 5 = a_2$.

3. In the example above we could restrict g to the set $C = [0, \infty)$ to get a one to one function $g|_C : [0, \infty) \to \mathbb{R}$. (Check!)

4. Let $A = \{\text{cat, dog, mouse}\}$ and $B = \{\text{house, garden}\}$, and define a function $f : A \to B$ by $f(\text{cat}) = \text{house}$, $f(\text{dog}) = \text{garden}$, and $f(\text{mouse}) = \text{house}$. Then f is not one-to-one because $f(\text{cat}) = f(\text{mouse})$, but 'cat' is not equal to 'mouse'.

Remark: Note that in order to prove that a function f is one-to-one we need to show that the definition holds for *any* pair of elements of the domain of f. However to prove that f is not one-to-one we just need to find a *single* pair of elements a and b in A for which $f(a) = f(b)$ but $a \neq b$.

Exercise 1.29. *Your turn:*

1. Find a one-to-one function from $\mathbb{N}$ to the set of even numbers $E = \{2, 4, 6, 8, ...\}$. Now find another one!

2. Find a one-to-one function from $\mathbb{N}$ to the set of odd numbers $O = \{1, 3, 5, 7, ...\}$.

Definition 1.30. Let $f : A \to B$ be a function. We say that f is *surjective* or *onto* if for all $b \in B$ there exists $a \in A$ such that$f(a) = b$. We say that f is an surjection.

Note: If f is an onto function then the range of f is all of B.

Example 1.31.

1. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x + 7$ is an onto function since if $y \in \mathbb{R}$ then there exists $x \in \mathbb{R}$ such that $f(x) = y$ i.e. $x = \frac{y-7}{3}$. Therefore by the definition above we see that f is an onto function.

2. The function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ is a not onto function since it is possible to find $y \in \mathbb{R}$ which is not in the range of g; for example if $y = -1$ then there is no $x \in \mathbb{R}$ such that $g(x) = y$.

3. We could modify the example above by considering $h : \mathbb{R} \to [0, \infty)$, $h(x) = x^2$. Check that h is onto!

Remark: To prove that a function $f : A \to B$ is onto we need to show that *every* $y \in B$ is in the image of f i.e. that there exists $x \in A$ such that $f(x) = y$. To show that f is not onto we just need to find *one* $y \in B$ which is not in the image of f.

Note: It is possible to find examples of functions which are a) both one-to-one and onto b) neither one-to-one nor onto c) onto but not one-to-one and d) one-to-one but not onto. Try to come up with examples in each of these categories yourself before looking at the next example.

Example 1.32. Find examples of functions $f : \mathbb{R} \to \mathbb{R}$ in the following categories:

1. One-to-one and onto: From our work above we see that $f(x) = 3x + 7$ is one-to-one and onto. It is not hard to prove that any non-constant linear function ($f(x) = ax + b$ where $a \neq 0$) is one-to-one and onto.

2. Neither 1-1 nor onto: If we let $f(x) = \sin(x)$ then f is not onto (since the range is $[-1, 1]$) and is not one-to-one (since $f(0) = f(2\pi)$ etc.)

3. Onto but not one-to-one: The function $f(x) = x(x - 1)(x - 2) = x^3 - 3x^2 + 2x$ is not one-to-one since $f(0) = f(1) = f(2) = 0$. From its graph we can see that it is onto.

4. One-to-one but not onto: The function $f(x) = e^x$ is one-to-one but not onto (from its graph we can see that it is always increasing and so never takes the same value twice, and its range is $(0, \infty)$).

Definition 1.33. A function $f : A \to B$ is called a *bijection* if it is one-to-one and onto.

Example 1.34. We have seen above that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x+7$ is one-to-one and onto, therefore it is a bijection. We can also check that the function $f : \mathbb{N} \to E = \{2, 4, 6, ...\}$ given by $f(x) = 2x$ is a bijection. So we have an example of a bijection between a set and one of its proper subsets.

Exercise 1.35. Your turn: Suppose A and B are finite sets (that is they each contain a finite number of elements).

1. Suppose that $f : A \to B$ is onto. What can you say about the number of elements in A and B?
2. Suppose that $f : A \to B$ is one-to-one. What can you say about the number of elements in A and B?
3. Suppose that $f : A \to B$ is a bijection. What can you say about the number of elements in A and B?

Exercise 1.36. Is it possible to find a bijection between $\mathbb{N}$ and $\mathbb{Z}$? If so, find it. If not, explain why it is impossible.

Definition 1.37. Let A be a set. Then the identity function id_A is the function given by $id_A : A \to A$ where $id_A(x) = x$ for all $x \in A$.

Definition 1.38. Let A and B be sets. Let $f : A \to B$ and $g : B \to A$ be functions. We say that g is the *inverse* of f if $f \circ g = id_B$ and $g \circ f = id_A$. We write $g = f^{-1}$. (That is $g = f^{-1}$ if $f(g(b)) = b$ for all $b \in B$, and $g(f(a)) = a$ for all $a \in A$.)

We might ask which functions have inverses. The next theorem tells us that all bijections have inverses.

Theorem 1.39. *Let $f : A \to B$ be a bijection. Then $g = f^{-1}$ exists.*

Proof: We need to define $g : B \to A$ such that $g(f(a)) = a$ for all $a \in A$ and $f(g(b)) = b$ for all $b \in B$.

Let $b \in B$, then since f is onto there exists $a \in A$ such that $f(a) = b$. Since f is one-to-one, there is only one such a. So define $g(b) = a$.

Then $g(f(a)) = g(b) = a$ for all $a \in A$. And $f(g(b)) = f(a) = b$ for all $b \in B$. Therefore $g = f^{-1}$.

□

Example 1.40. We saw previously that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x + 7$ is a bijection and so it has an inverse function. The inverse is $g(x) = \frac{x-7}{3}$. Check that $f(g(y)) = y$ and $g(f(x)) = x$ for all $x, y \in \mathbb{R}$.

Example 1.41. We have seen above that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \sin(x)$ is not a bijection since it is neither one-to-one nor onto. However if we restrict the domain and the range by considering $f : [-\pi/2, \pi/2] \to [-1, 1]$ we can check that f is a bijection between the sets $[-\pi/2, \pi/2]$ and $[-1, 1]$. Therefore it has an inverse $g(x) = \sin^{-1}(x) = \arcsin(x)$ which is defined on $[-1, 1]$.

Theorem 1.42. *Let $f : A \to B$ be a bijection and $g : B \to C$ be a bijection. Then $g \circ f : A \to C$ is a bijection.*

Proof: We need to show that $g \circ f : A \to C$ is one-to-one and onto.

To show that it is one-to-one: Suppose $g \circ f(a_1) = g \circ f(a_2)$ then $g(f(a_1)) = g(f(a_2))$.

But since g is one-to-one on B this means that $f(a_1) = f(a_2)$. But since f is one-to-one on A we have $a_1 = a_2$. Thus $g \circ f$ is one-to-one.

To show that $g \circ f : A \to C$ is onto: Let $z \in C$, then there exists $y \in B$ such that $g(y) = z$ since $g : B \to C$ is onto. There exists $x \in A$ such that $f(x) = y$ since $f : A \to B$ is onto. Thus $g \circ f(x) = g(f(x)) = g(y) = z$, and so $g \circ f : A \to C$ is onto.

□

1.3 Equivalence Relations

Equivalence relations are important in many areas of mathematics. They will be useful to us when we look at cardinality of sets. We will start with some definitions:

Definition 1.43. A *relation* on a set A is a subset of $A \times A$.

Example 1.44. Let P be the set of all people in the world. Remember that a relation on P is just a subset of $P \times P$. Let's consider some relations on P:

- $D = \{(x, y) \in P \times P \mid x \text{ is a descendant of } y\}$;
- $B = \{(x, y) \in P \times P \mid x \text{ has an ancestor who is an ancestor of } y\}$;
- $S = \{(x, y) \in P \times P \mid x \text{ has the same parents as } y\}$;

If (x, y) is an element of a relation we usually write $x \sim y$. We will concentrate on relations with some nice properties:

Definition 1.45. An *equivalence relation* on a set A is a relation $\sim$ which satisfies:

1. $x \sim x$ for all $x \in A$ (Reflexivity);
2. If $x \sim y$ then $y \sim x$ for all $x, y \in A$ (Symmetry);
3. If $x \sim y$ and $y \sim z$ then $x \sim z$ for all $x, y, z \in A$ (Transitivity).

Let's consider the relations in Example 1.44 above. Are any of them equivalence relations?

Example 1.44 (continued). Let's start with the relation D. We need to check if it is reflexive, symmetric and transitive.

In order to be reflexive we need $x \sim x$ for all $x \in P$. But $x \sim x$ means that x is a descendant of themselves (which is clearly impossible!) so this relation is not reflexive. This tells us that the relation D is not an equivalence relation.

Is D symmetric? We need to check that if $x \sim y$ then $y \sim x$, for all $x, y \in P$. If $x \sim y$ then x is a descendant of y, but that means that y could not be a descendant of x so D is not symmetric.

Is D transitive? We need to check that if $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in P$. If $x \sim y$ then x is a descendant of y, and if $y \sim z$ then y is a descendant of z, so therefore x is a descendant of z also and so $x \sim z$. Thus D is transitive.

We have seen that D is transitive but not reflexive or symmetric and so it is not an equivalence relation.

What about the relation B? Is it reflexive? Is $x \sim x$ for all $x \in P$? Well, this is true since every person x has an ancestor who is an ancestor of x. So B is reflexive.

Is B symmetric? We need to check that if $x \sim y$ then $y \sim x$, for all $x, y \in P$. If $x \sim y$ then x has an ancestor who is an ancestor of y, but then clearly y has an ancestor who is an ancestor of x so $y \sim x$ and B is symmetric.

Is B transitive? We need to check that if $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in P$. If x has an ancestor who is an ancestor of y, y has an ancestor who is an ancestor of z it is not always true that x has an ancestor who is an ancestor of z. For example, suppose y has parents x and z. Then $x \sim y$ and $y \sim z$ but x and z do not have to have a common ancestor so we are not guaranteed that $x \sim z$. We have shown that B is not transitive.

We have seen that B is reflexive and symmetric but not transitive, and so it is not an equivalence relation.

What about the relation S? Is it reflexive? Is $x \sim x$ for all $x \in P$? Well, this is true since every person x has the same parents as themselves. So S is reflexive.

Is S symmetric? We need to check that if $x \sim y$ then $y \sim x$, for all $x, y \in P$. If $x \sim y$ then x has the same parents as y, but then clearly y has the same parents as x so $y \sim x$ and S is symmetric.

Is S transitive? We need to check that if $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in P$. If x has the same parents as y, and y has the same parents as z then$x$ has the same parents as z. So S is transitive.

We have seen that S is reflexive, symmetric and transitive, and so it is an equivalence relation.

Example 1.46. We can put a relation on $\mathbb{R}$ as follows: $x \sim y$ if $x - y \in \mathbb{Z}$. Note that under this relation we have $1.1 \sim 2.1$, $1.1 \sim 2.1$, $1.1 \sim 3.1$ etc. and also $1.1 \sim -0.9$, $1.1 \sim -1.9$ ...

Is this an equivalence relation on $\mathbb{R}$?

We need to check if $\sim$ is reflexive, symmetric and transitive.

Reflexivity: Is $x \sim x$ for all $x \in \mathbb{R}$? Yes, because $x - x = 0 \in \mathbb{Z}$ for all $x \in \mathbb{R}$.

Symmetry: If $x \sim y$ is $y \sim x$ for all $x, y \in \mathbb{R}$? Yes, because $x \sim y$ means that $x - y \in \mathbb{Z}$ so there exists $n \in \mathbb{Z}$ such that $x - y = n$, but then $y - x = -n \in \mathbb{Z}$ and so $y \sim x$.

Transitivity: If $x \sim y$ and $y \sim z$ is it true that $x \sim z$? Yes, if $x \sim y$ then there exists $n \in \mathbb{Z}$ such that $x - y = n$, and $y \sim z$ so there exists $m \in \mathbb{Z}$ such that $y - z = m$. Then $x - z = x - y + y - z = n + m \in \mathbb{Z}$ and so $x \sim z$.

Thus our relation $\sim$ is an equivalence relation on $\mathbb{R}$.

Exercise 1.47. Let A be the set of all books in the Maynooth University Library. Define an equivalence relation on A. Define a relation on A which is not an equivalence relation.

Definition 1.48. Given an equivalence relation $\sim$ on a set A and an element $x \in A$ we define the *equivalence class* of x to be

$$[x] = \{y \in A \mid x \sim y\}.$$

So the equivalence class of x is the set of all elements of A which is related to x.

Note: Since $x \sim x$ for all $x \in A$ if $\sim$ is an equivalence relation on A then we always have $x \in [x]$, which means that equivalence classes are never empty.

What do the equivalence classes for the relation S above look like? What about the equivalence classes for the relation you put on the set of books in MU Library?
In Example 1.45 we can see that $[1.1] = \{0.1, 1.1, 2.1, ...\} \cup \{-0.9, -1.9, -2.9, ...\}$. Note here that $2.1 \sim 0.1 \sim 3.1 \sim 4.1...$ and $2.1 \sim -0.9 \sim -1.9...$, and in fact $[2.1] = [1.1]$. The next theorem tells us about equality of equivalence classes:

Theorem 1.49. *Let A be a set and let $\sim$ be an equivalence relation on A. If $x, z \in A$ then $[x] = [z]$ if and only if $x \sim z$.*

Proof: (*Note:* We need to show that if $[x] = [z]$ then $x \sim z$, and if $x \sim z$ then $[x] = [z]$.)
Suppose that $[x] = [z]$ then since $x \in [x]$ we have $x \in [z]$. By the definition of the equivalence class, this means that $x \sim z$.
Let's show now that if $x \sim z$ then $[x] = [z]$. Recall that $[x]$ and $[z]$ are sets and that if we want to prove that two sets B and C are equal then we must show that $B \subset C$ and $C \subset B$. So here we need to show that $[x] \subset [z]$ and $[z] \subset [x]$.
Suppose that $x \sim z$ and let $y \in [x]$. Then $y \sim x$ and $x \sim z$ so by transitivity we have $y \sim z$. This means that $y \in [z]$. So $[x] \subset [z]$.
Suppose that $x \sim z$ and let $w \in [z]$. Then $w \sim z$ and $z \sim x$ (since $x \sim z$ and $\sim$ is symmetric). By transitivity we have $w \sim x$ which means that $w \in [x]$. So $[z] \subset [x]$.
Since $[x] \subset [z]$ and $[z] \subset [x]$, we have that $[x] = [z]$ if $x \sim z$.

□

We can use this theorem to prove that two equivalence classes are either equal or have no overlap:

Corollary 1.50. *Let A be a set and let $\sim$ be an equivalence relation on A. Let $x, z \in A$ then either $[x] = [z]$ or $[x] \cap [z] = \emptyset$.*

Proof: Suppose that $x, z \in A$ and $[x] \cap [z] \neq \emptyset$. Then there exists $y \in [x] \cap [z]$, that is $y \sim x$ and $y \sim z$. Since $\sim$ is an equivalence relation it is symmetric so $y \sim x$ means that $x \sim y$. Now $x \sim y$ and $y \sim z$ so by transitivity we have $x \sim z$ and $[x] = [z]$.

□

Let's consider the set E of all equivalence classes of a relation $\sim$ on A, that is

$$E = \{[x] \mid x \in A\}.$$

What can we say about E? Since for any $x \in A$ we have $x \in [x]$ we have that $\cup_{x \in A}[x] = A$ (why?).Thus it is clear that the union of all elements of E is A. We also know, from the corollary above, that different elements of E are disjoint. So we can think of E as a way of partitioning the set A into disjoint pieces.

Definition 1.51. A *partition* of a set A is a collection of disjoint subsets of A whose union is all of A.

Example 1.52. 1. Let A be the set of counties in Ireland.

Let $A_1 = \{$ All counties in Munster $\}$

Let $A_2 = \{$ All counties in Connacht $\}$

Let $A_3 = \{$ All counties in Ulster $\}$

Let $A_4 = \{$ All counties in Leinster $\}$

Then $\{A_1, A_2, A_3, A_4\}$ is a partition of A, since $A = A_1 \cup A_2 \cup A_3 \cup A_4$ (that is every county is in at least one province) and the A_i's are disjoint (that is there are no counties that are in more than one province).

2. Let $A = \mathbb{R}$ and let $A_i = [i, i+1)$ for $i \in \mathbb{Z}$. (So $A_{-1} = [-1, 0)$, $A_0 = [0, 1)$, $A_1 = [1, 2)$ etc.) It is clear that $\cup_{i \in \mathbb{Z}} A_i = \mathbb{R}$ and that the A_i's are disjoint. Therefore $\{A_i\}_{i \in \mathbb{Z}}$ is a partition of $\mathbb{R}$.

3. Let $A = \mathbb{R}$ and $B_i = [i, i+1]$ for $i \in \mathbb{Z}$. Then $\{B_i\}_{i \in \mathbb{Z}}$ is not a partition of $\mathbb{R}$ since the B_i's are not all disjoint as we have $B_i \cap B_{i+1} = \{i+1\}$.

Exercise 1.53. Let A be the set of all books in the MU Library. Can you find a partition of A?

We saw earlier that the set of equivalence classes of an equivalence relation on a set A gives us a partition of the set A. It is not hard to see that every partition of A determines an equivalence relation on A. To see why, suppose that $D = \{A_i\}$ is a partition of A into disjoint subsets and define a relation $\sim_D$ on A by $x \sim_D y$ if $x, y \in A_i$ for some i (that is x and y are in the same part of the partition as each other). We need to check that this is an equivalence relation:

Is $x \sim_D x$ for all $x \in A$? Yes, since x is in the same part of the partition as itself.

If $x \sim_D y$, is $y \sim_D x$? Yes, since if $x \sim_D y$ then there exists j such that $x, y \in A_j$ but then $y, x \in A_j$ and so $y \sim_D x$.

If $x \sim_D y$ and $y \sim_D z$, is $x \sim_D z$? Yes, since if $x \sim_D y$ then there exists j such that $x, y \in A_j$, and $y \sim_D z$ means that y and z are in the same part of the partition. But since $y \in A_j$ that means that $z \in A_j$ also. Thus $x, z \in A_j$ (i.e. they are in the same part of the partition) so $x \sim_D z$.

We have shown that $\sim_D$ is an equivalence relation on A.

1.4 Cardinality

In this section we will look at the problem of 'counting' the number of elements in a set. (Cardinality refers to the size of a set.) In some cases this is easy: If $A = \{\text{cat, dog, mouse}\}$ then it is clear that A has three elements, and if B is the set of counties in Munster then B

has 6 elements. However, we will be interested in the cardinality of infinite sets such as $\mathbb{N}$ and $\mathbb{R}$.

Question: Consider $\mathbb{N}$ and $E = \{2, 4, 6, 8, ...\}$. Does $\mathbb{N}$ have more elements than E?

We might intuitively say yes here because E is a proper subset of $\mathbb{N}$, but the function $F : \mathbb{N} \to E$ given by $f(x) = 2x$ is a bijection from $\mathbb{N}$ to E. Thus we can put the elements of $\mathbb{N}$ into one-to-one correspondence with the elements of E i.e. $1 \to 2$, $2 \to 4$, $3 \to 6$, $4 \to 8$ etc. And so we might conjecture that these two sets have the same 'size'. We will try to formalise this notion:

Definition 1.54. Let X and Y be two sets. We say that X is *numerically equivalent* to Y (or that X and Y have the same *cardinality*) if there is a bijection between X and Y.

Example 1.55.

1. The sets $\mathbb{N}$ and E are numerically equivalent since we can find a bijection between them. In other words, they have the same cardinality. Similarly $\mathbb{N}$ and $O = \{1, 3, 5, 7, 9, ...\}$ are numerically equivalent to each other.

2. The set B of counties in Munster is numerically equivalent to the set $C = \{1, 2, 3, 4, 5, 6\}$. It is easy to check that the function $f : B \to C$ given by $f(Cork) = 1$, $f(Kerry) = 2$, $f(Clare) = 3$, $f(Tipperary) = 4$, $f(Waterford) = 5$ and $f(Limerick) = 6$ is a bijection between these sets. Therefore they have the same cardinality. [Note that this resembles the way that children count objects in a set, that is by pointing to each one while counting.)

Example 1.56. Show that $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality.

In order to prove this we need to find a bijection $f : \mathbb{N} \to \mathbb{Z}$. Define f as follows:

$$f(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ -\frac{n}{2} & \text{if } n \text{ is even} \end{cases}$$

Check that this function is one-to-one and onto.

Example 1.57. The interval $(-1, 1)$ has the same cardinality as $\mathbb{R}$.

To prove this we need to find a bijection $f : (-1, 1) \to \mathbb{R}$. Define $f(x) = \dfrac{x}{x^2 - 1}$. If you look at the graph of f on the interval $(-1, 1)$, it is easy to see that f is strictly decreasing on this interval (and so one-to-one) and takes every real value. Thus it is also onto $\mathbb{R}$.

We have seen that finite sets cannot be numerically equivalent to proper subsets but the examples above show us that this seems not to be true of infinite sets. We have not given a definition of 'finite' or 'infinite' yet so let's do that here:

Definition 1.58. A set A is *finite* if there is a bijection $f : \{1, ..., n\} \to A$ for some $n \in \mathbb{N}$. A set is *infinite* if it is not finite.

Next let's suppose that U is a set and let S be the set of all non-empty subsets of U. Then we can define an equivalence relation on S as follows: We say $X \sim Y$ if X is numerically equivalent to Y (i.e. there is a bijection from X to Y). Let's check that this is an equivalence relation:

- Is $X \sim X$ for all $X \in S$? Yes, since $id_X : X \to X$ is a bijection from X to X.
- If $X \sim Y$, is $Y \sim X$? Yes, since if $X \sim Y$ then there exists a bijection $f : X \to Y$. But then $g = f^{-1}$ exists and is a bijection from Y to X. Thus $Y \sim X$.
- If $X \sim Y$ and $Y \sim Z$, is $X \sim Z$? Yes, since if $X \sim Y$ then there exists a bijection $f : X \to Y$ and if $Y \sim Z$ then there exists a bijection $g : Y \to Z$. Then $g \circ f : X \to Z$ is a bijection by Theorem 1.42, so $X \sim Z$.

The equivalence classes of this equivalence relation are the collections of subsets of U which have the same cardinality. For example, if $U = \mathbb{R}$ then we have seen that $\mathbb{Z} \in [\mathbb{N}]$ (by Example 1.56) and also that $E \in [\mathbb{N}]$. We can then deduce that $Z \sim E$ also. We also know that $(-1, 1) \in [\mathbb{R}]$ (by Example 1.57).

We would like to know if $[\mathbb{N}] = [\mathbb{R}]$. We will return to this fundamental question soon. In the meantime, ask yourselves if $\mathbb{Q} \in [\mathbb{N}]$?

The next theorem will be an important tool for us:

Theorem 1.59 (The Schroeder-Bernstein Theorem)**.** *If X and Y are two sets each of which are numerically equivalent to a subset of the other, then all of X is numerically equivalent to all of Y.*

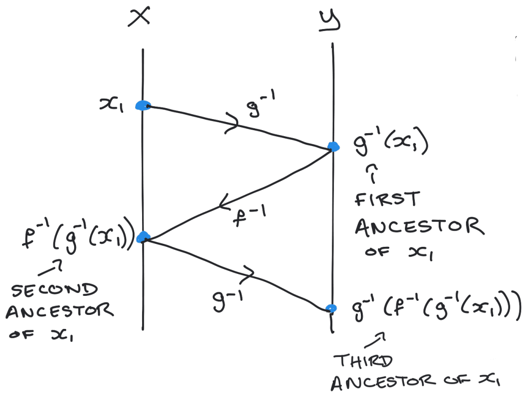
Proof: We need to find a bijection $F : X \to Y$. By assumption there exist functions $f : X \to Y$ and $g : Y \to X$ which are one-to-one (but not necessarily onto). If f is onto then let $F = f$, and if g is onto let $F = g^{-1}$. In either case, we are done.

Suppose then that neither f nor g are onto functions. Since f and g are both one-to-one we can define $f^{-1} : f(X) \to X$ and $g^{-1} : g(Y) \to Y$. We will divide X and Y into subsets as follows:

Take $x \in X$. Now either $x \in g(Y)$ or $x \notin g(Y)$. If $x \in g(Y)$ apply g^{-1} to it to get $g^{-1}(x) \in Y$. If $g^{-1}(x)$ exists we call it the first ancestor of x. We call x the zero-th ancestor of x. Now apply f^{-1} to $g^{-1}(x)$ (if possible) to get $f^{-1}(g^{-1}(x))$ - we call this the second ancestor of x if it exists. Now apply g^{-1} to $f^{-1}(g^{-1}(x))$ (if possible) to get $g^{-1}(f^{-1}(g^{-1}(x)))$ - we call this the third ancestor of x if it exists. [Note that the first ancestor of x belongs to Y, the second to X, and the third to Y.] See the illustration below.

It is clear that one of three things can happen:

1. x has infinitely many ancestors. We denote the subset of X which contains all elements with infinitely many ancestors by X_i.
2. x has an even number of ancestors (here we include 0 as an even number). This means that x has a last ancestor in X which is not in $g(Y)$. We denote the subset of X which contains all elements with an even number of ancestors by X_e.
3. x has an odd number of ancestors. This means that x has a last ancestor in Y which is not in $f(X)$. We denote the subset of X which contains all elements with an odd number of ancestors by X_o.



Clearly $X = X_i \cup X_e \cup X_o$ and X_i, X_e and X_o are disjoint.

Now decompose Y in the same way into the disjoint sets Y_i, Y_e and Y_o. To see that f maps X_i onto Y_i, recall that if $y \in Y_i$ then y has infinitely many ancestors. Thus $y \in f(X)$, that is there exists $x \in X$ such that $f(x) = y$ or $x = f^{-1}(y)$. In other words x is the first ancestor of y. The first ancestor of x is $g^{-1}(x) = g^{-1}(f^{-1}(y))$ and so is the second ancestor of y etc. Since y has infinitely many ancestors then so does x i.e. $x \in X_i$. So $f : X_i \to Y_i$ is onto.

We can show that $F : X_e \to Y_o$ is onto also, since if $y \in Y_o$ then it must have at least one ancestor so there exists $x \in X$ such that $f(x) = y$ or $x = f^{-1}(y)$. As in the paragraph above we see that x will have one less ancestor than y. Since y has an odd number of ancestors, then x must have an even number of ancestors and so $x \in X_e$. So $f : X_e \to Y_o$ is onto.

Since we are assuming that $f : X \to Y$ is not onto, we have no hope that $f : X_o \to Y_e$ is onto. However we will show that $g^{-1} : X_o \to Y_e$ is onto. To see this, let $y \in Y_e$ then since $g : Y \to X$ is one-to-one there exists $x \in X$ such that $g(y) = x$ or $g^{-1}(x) = y$. If y has no ancestors then $y \notin f(X)$ so $f^{-1}(y)$ or $f^{-1}(g^{-1}(x))$ does not exist and then x has one ancestor i.e. $x \in X_o$. If y has at least one ancestor then y's first ancestor will be x's second ancestor and so x will have exactly one more ancestor than y. Since y has an even number of ancestors, we have that $x \in X_o$. So $g^{-1} : X_o \to Y_e$ is onto.

Now define $F : X \to Y$ by

$$F(x) = \begin{cases} f(x) & x \in X_i \cup X_e \\ g^{-1}(x) & x \in X_o \end{cases}$$

Since f and g^{-1} are both one-to-one functions our analysis above has shown that F is one-to-one and onto. Thus X and Y are numerically equivalent to each other.

□

Let's return to our discussion of cardinality. We have already seen that $\mathbb{N}$ and $E = \{2, 4, 6, 8, ...\}$ are numerically equivalent, i.e. they have the same cardinality. To show that a set X is numerically equivalent to $\mathbb{N}$ we need to find a bijection $\mathbb{N}$ to that set. If we think of the image of 1 under the bijection as the 'first' element of X, the image of 2 as the 'second' element of X etc the bijection gives us a way to list the elements of X. This corresponds to our earlier experience of counting the elements of a finite set.

Definition 1.60. A *countably infinite* set is a set which is numerically equivalent to $\mathbb{N}$. We say a set is *countable* if it is finite or countably infinite. A set which is not countable is said to be *uncountable.*

Example 1.61. We have already seen that the sets $\mathbb{N}$, $\mathbb{Z}$, $\{2, 4, 6, 8...\}$ and $\{1, 3, 5, 7, ...\}$ are countably infinite and so are countable.

Questions: Is every infinite set countable? Is $\mathbb{Q}$ countable? What about $\mathbb{R}$?

In order to answer these questions, we will need some results:

Theorem 1.62. *Every subset of a countable set is countable.*

Proof: Let A be a countable set and suppose $B \subset A$. If B is finite then it is countable and we are done. So suppose that B is not finite. We want to show that B is countably infinite.

Since A is countably infinite we can list all the elements of A as follows: $x_1, x_2, x_3, ...$ (in other words since there exists $g : \mathbb{N} \to A$ a bijection, denote $g(k)$ by x_k for all $k \in \mathbb{N}$ so $A = \{x_1, x_2, ...\}$).

Let n_1 be the smallest positive integer such that $x_{n_1} \in B$.

Let n_2 be the smallest positive integer such that $n_2 > n_1$ and $x_{n_2} \in B$.

Let n_3 be the smallest positive integer such that $n_3 > n_2$ and $x_{n_3} \in B$.

Now define $f : \mathbb{N} \to B$ by $f(k) = x_{n_k}$ for $k \in \mathbb{N}$. Since every element of B appears in the list $x_1, x_2, x_3, ...$, we can see that f is onto, and no element of B appears more than once on the list we have that f is one-to-one. Thus we have found a bijection from $\mathbb{N}$ to B and so B is countably infinite as required.

□

This theorem says that a countable set cannot have an uncountable subset. This means that countably infinite sets are the 'smallest' infinite sets.

We will need to consider unions of countable sets next. First we need some notation: Let A be a set and suppose that associated to each element $\alpha \in A$ there is a set E_α, then

$$S = \cup_{\alpha \in A} E_\alpha = \{x \mid x \in E_\alpha \text{ for some } \alpha \in A\}.$$

If $A = \mathbb{N}$ we have already seen that we write $\cup_{n \in N} E_n = \cup_{n=1}^{\infty} E_n$.

Theorem 1.63. *Let $\{E_n\}_{n\in\mathbb{N}}$ be a collection of countable sets and let $S = \cup_{n\in N} E_n$. Then S is countable.*

Proof: Since each E_n is countable, we can denote each of them as

$$E_k = \{x_{k_1}, x_{k_2}, x_{k_3}, ...\}$$

So let's consider the array where we list all the elements of E_1 in the first row, the elements of E_2 in the second row, the elements of E_n in the n^{th} row, etc:

$$\begin{array}{cccccc}
x_{1_1} & x_{1_2} & x_{1_3} & x_{1_4} & x_{1_5} & \dots \\
x_{2_1} & x_{2_2} & x_{2_3} & x_{2_4} & x_{2_5} & \dots \\
x_{3_1} & x_{3_2} & x_{3_3} & x_{3_4} & x_{3_5} & \dots \\
x_{4_1} & x_{4_2} & x_{4_3} & x_{4_4} & x_{4_5} & \dots \\
. & . & . & . & . & \dots \\
. & . & . & . & . & \dots \\
x_{n_1} & x_{n_2} & x_{n_3} & x_{n_4} & x_{n_5} & \dots \\
. & . & . & . & . & \dots \\
. & . & . & . & . & \dots
\end{array}$$

This array contains all of the elements of S. Now arrange them by sweeping diagonally through the array starting at the top left-hand corner:

$$x_{1_1}, x_{2_1}, x_{1_2}, x_{3_1}, x_{2_2}, x_{1_3}, x_{4_1}, x_{3_2}, x_{2_3}, x_{1_4}, ...$$

Now if any two of the sets E_n have elements in common then these elements will appear more than once on this list. So there exists a subset $T \subset \mathbb{N}$ such that T is numerically equivalent to S. Since T is a subset of a countable set (i.e. $\mathbb{N}$) it is countable by the last theorem. Therefore S is countable too.

□

We can prove that any countable union of countable sets is countable:

Corollary 1.64. *Let A be a countable set and suppose for each $\alpha \in A$ the set B_α is countable then $\cup_{\alpha\in A} B_\alpha$ is countable.*

Proof: We can adapt the proof of the previous theorem. I will leave this to you as an exercise.

We are now ready to show that $\mathbb{Q}$ is countable:

Theorem 1.65. *The set of rational numbers $\mathbb{Q}$ is a countable set.*

Proof: To prove this let's form the sets $A_k = \{0, \frac{1}{k}, \frac{-1}{k}, \frac{2}{k}, \frac{-2}{k}, ...\}$ for $k \in \mathbb{N}$. We have:

$$\begin{array}{cccccccc}
A_1 = \{0, & \frac{1}{1}, & \frac{-1}{1}, & \frac{2}{1}, & \frac{-2}{1}, & \frac{3}{1}, & \frac{-3}{1}, & ...\} \\
A_2 = \{0, & \frac{1}{2}, & \frac{-1}{2}, & \frac{2}{2}, & \frac{-2}{2}, & \frac{3}{2}, & \frac{-3}{2}, & ...\} \\
A_3 = \{0 & \frac{1}{3}, & \frac{-1}{3}, & \frac{2}{3}, & \frac{-2}{3}, & \frac{3}{3}, & \frac{-3}{3}, & ...\} \\
. & . & . & . & . & . & . & \\
A_n = \{0, & \frac{1}{n}, & \frac{-1}{n}, & \frac{2}{n}, & \frac{-2}{n}, & \frac{3}{n}, & \frac{-3}{n}, & ...\} \\
. & . & . & . & . & . & . &
\end{array}$$

It is clear that each A_k is countable (why?) and that $\mathbb{Q} = \cup_{n\in\mathbb{N}} A_n$. Therefore $\mathbb{Q}$ is a countable union of countable sets and thus (by Theorem 1.63) $\mathbb{Q}$ is countable.

□

Theorem 1.66. *The set* $\mathbb{R}$ *is uncountable.*

Proof: We will show that the set $(0,1)$ is uncountable. Since $(0,1) \subset \mathbb{R}$ then $\mathbb{R}$ contains an uncountable subset and so by Theorem 1.62 it must be uncountable.

In order to show that $(0,1)$ is uncountable, we will show that it is not possible to have a bijection from $\mathbb{N}$ to $(0,1)$.

Note that if $x \in (0,1)$ then x has decimal representation $x = 0.a_1a_2a_3...$ where each $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$.

Suppose that $f : \mathbb{N} \to (0,1)$ is a bijection (and let's look for a contradiction!). Then for each $m \in \mathbb{N}$ $f(m) \in (0,1)$ and has decimal representation $f(m) = 0.a_{m_1}a_{m_2}a_{m_3}...$ So we can list out all of the images of the natural numbers as follows:

$$f(1) = 0.a_{1_1}a_{1_2}a_{1_3}a_{1_4}...$$

$$f(2) = 0.a_{2_1}a_{2_2}a_{2_3}a_{2_4}...$$

$$f(3) = 0.a_{3_1}a_{3_2}a_{3_3}a_{3_4}...$$

$$f(4) = 0.a_{4_1}a_{4_2}a_{4_3}a_{4_4}...$$

and so on. If f is a bijection then it is onto and so every real number in $(0,1)$ must be on this list. Now consider the number $b = 0.b_1b_2b_3b_4...$ where

$$b_n = \begin{cases} 2 & \text{if } a_{n_n} \neq 2 \\ 3 & \text{if } a_{n_n} = 2 \end{cases}$$

Clearly $b \in (0,1)$ and $b_n \neq a_{n_n}$ for all $n \in \mathbb{N}$. Let's suppose that $b = f(k)$ for some $k \in \mathbb{N}$ then the k^{th} digit after the decimal point in $f(k)$ is a_{k_k} and in b is b_k. Since $b_k \neq a_{k_k}$ we have $f(k) \neq b$. Thus f is not onto and therefore is not a bijection. Thus it is not possible to find a bijection from $\mathbb{N}$ to $(0,1)$, and so we can conclude that $(0,1)$ (and thus $\mathbb{R}$) is uncountable.

[Note: Some numbers do have two different decimal expansions, for example $0.5000000... = 0.4999999....$ However this only happens when the decimal expansions end with infinite strings of 0's or 9's and we have constructed b using only the digits 2 and 3 so b has a unique decimal expansion.]

□

This theorem gives us our first example of an uncountable set. We do not yet know whether all uncountable sets are numerically equivalent to each other or not. We will return to this later.

Remark:

1. We can prove that if $a, b \in \mathbb{R}$ with $a < b$ then (a, b) is numerically equivalent to $(0, 1)$. To do this we observe that the function $f : (0, 1) \to (a, b)$ given by $f(x) = a + (b - a)x$ is a bijection. (Check!) Therefore any open interval $(a, b) \subset \mathbb{R}$ is uncountable.
2. Since $(0, 1)$ is numerically equivalent to $(-1, 1)$ and $(-1, 1)$ is numerically equivalent to $\mathbb{R}$ we see that $(0, 1)$ is numerically equivalent to $\mathbb{R}$. In fact since any interval (a, b) is numerically equivalent to $(0, 1)$ we see that any open interval (a, b) is numerically equivalent to $\mathbb{R}$.
3. We have seen that $\mathbb{Q}$ is not numerically equivalent to $\mathbb{R}$ but 2. tells us that any interval, no matter how tiny, is numerically equivalent to $\mathbb{R}$. Take for example the intervals $I_n = (0, 10^{-n})$ (so $I_1 = (0, 0.1)$, $I_2 = (0, 0.01)$, $I_{10} = (0, 0.0000000001)$ etc.) The lengths of these intervals are extremely small when n is large, but each one contains an uncountable number of elements - and in some sense more elements than $\mathbb{Q}$ does!

Theorem 1.67. *Any subset of $\mathbb{R}$ which contains an open interval is numerically equivalent to $\mathbb{R}$.*

Proof: Let $X \subset \mathbb{R}$ and suppose there exists an interval $I = (a, b)$ such that $I \subset X \subset \mathbb{R}$. Then X is numerically equivalent to a subset of $\mathbb{R}$ (namely itself) and $\mathbb{R}$ is numerically equivalent to a subset of X (namely I by the remark above). So we can apply the Schroeder-Bernstein theorem and conclude that $\mathbb{R}$ and X are numerically equivalent.

□

Here is another example of an uncountable set:

Theorem 1.68. *Let S be the set of sequences which consist of 0's and 1's. That is*

$$S = \{(a_1, a_2, a_3, ...) | a_i = 0 \text{ or } 1\}.$$

Then S is not a countable set.

Proof: Suppose that $f : \mathbb{N} \to S$ is a function. We will show that f cannot be onto and thus cannot be a bijection. Let us denote $f(n)$ by $f(n) = (x_{n_1}, x_{n_2}, ...)$ where each x_{n_i} is 0 or 1. Define $y = (y_1, y_2, y_3, ...)$ as follows:

$$y_n = \begin{cases} 0 & \text{if } x_{n_n} = 1 \\ 1 & \text{if } x_{n_n} = 0 \end{cases}$$

Clearly $y \in S$ and we can see that $y_n \neq x_{n_n}$ for all $n \in \mathbb{N}$, in other words the n^{th} element in the sequence y is not equal to the n^{th} element in the sequence $f(n)$. This tells us that the sequence $y \neq f(n)$ for all $n \in \mathbb{N}$, i.e. $y \notin f(\mathbb{N})$.

Therefore f is not onto. We can conclude that there are no bijections between $\mathbb{N}$ and S and since S is infinite this means that S is uncountable.

□

Exercise 1.69. Prove the following:

1. The set $\mathbb{N} \times \mathbb{N}$ is countable.
2. The set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is uncountable.
3. The set $\mathbb{R}^2$ is uncountable.

Question: Are all uncountable sets numerically equivalent to each other? It turns out that this is not true. To see this we will need the concept of a *power set*.

Definition 1.70. Given a set A, the *power set* of A (denoted by $P(A)$) is the collection of all subsets of A.

Example 1.71. Let $A = \{a, b, c\}$ then

$$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

So here $P(A)$ has $8 = 2^3$ elements.

Exercise 1.72. Show that if A is a finite set with n elements then $P(A)$ has 2^n elements.

From the exercise above we see that if A is a finite set then there is no onto map from A to $P(A)$ and so they cannot be numerically equivalent. The next theorem tells us that this is true for infinite sets also:

Theorem 1.73 (Cantor's Theorem)**.** *Given a set A there does not exist an onto function from A to $P(A)$.*

Proof: Let $g : A \to P(A)$ be a function. For each $a \in A$ the image $g(a)$ is an element of $P(A)$ and so $g(a)$ is a subset of A. This subset either contains the element a or it does not.

Let B be the subset of A consisting of all elements $a \in A$ such that a is not in the set $g(a)$ that is

$$B = \{a \in A | a \notin g(a)\}.$$

Clearly $B \subset A$ so $B \in P(A)$.

We claim that B is not in the image of g (and thus g is not onto).

Suppose that B is in the image of g, then $B = g(a_0)$ for some $a_0 \in A$. Is $a_0 \in B$ or not?

Case 1 Suppose $a_0 \in B$. Then by the definition of B we have $a_0 \notin g(a_0)$ but $B = g(a_0)$ so $a_0 \notin B$. So $a_0 \in B$ and $a_0 \notin B$ which is impossible.

Case 2 Suppose $a_0 \notin B$. Then since $B = g(a_0)$ we have $a_0 \notin g(a_0)$. So a_0 satisfies the criterion to be an element of B i.e. $a_0 \in B$. So $a_0 \notin B$ and $a_0 \in B$ which is impossible.

Our assumption that $B = g(a_0)$ for some $a_0 \in A$ has led to contradictions so we can conclude that it is not true. Therefore B is not in the image of g and so the function g is not onto.

Since g was arbitrary, we conclude that there is no onto function from A to $P(A)$.

□

Example 1.74. This theorem tell us that $\mathbb{R}$ and its power set $P(\mathbb{R})$ are not numerically equivalent. We can conclude that it is not true that all uncountable sets are numerically equivalent to each other.

Cardinal Numbers

Cardinal numbers are used to denote the cardinality of a set. If a set is empty it has cardinal number 0. If a set is finite then its cardinal number is a natural number (eg the set $A = \{a, b, c\}$ has cardinal number 3). We denote the cardinality of the Natural numbers by the symbol $\aleph_0$ (read as 'aleph nought'). Thus the cardinal number of $\mathbb{Z}$ and $\mathbb{Q}$ is $\aleph_0$. The cardinal number of $\mathbb{R}$ is denoted by c (for continuum).

We have $0 < 1 < 2 < 3 < .... < \aleph_0 < c$.

We might ask whether there are cardinal numbers between $\aleph_0$ and c? The statement that there are no cardinal numbers between $\aleph_0$ and c is the Continuum Hypothesis. It has been shown by Gödel and Cohen that the Continuum Hypothesis is independent of our axioms of set theory - that is proving it or disproving it are impossible using our set theory axioms (more accurately using the axioms of Zermelo-Fraenkel Set Theory).

We might also ask if there are cardinal numbers greater than c? The answer to this is clear from Cantor's Theorem since the cardinal number of $P(\mathbb{R})$ must be greater than c. We denote the cardinal number of $P(\mathbb{R})$ by 2^c (and in general if a set A has cardinal number b we denote the cardinal number of the power set $P(A)$ by 2^b. Thus we can see that we have infinitely many equivalence classes of infinite sets:

$$0 < 1 < 2 < 3 < .... < \aleph_0 < c < 2^c < 2^{2^c} < 2^{2^{2^c}} < ....$$

We can show that $2^{\aleph_0} = c$ - try it!

1.5 Properties of $\mathbb{R}$

Definition 1.75. A relation $<$ on a set A is called an *order relation* (or a simple order or a linear order) if it has the following properties:

1. For every $x, y \in A$ for which $x \neq y$ either $x < y$ or $y < x$. (Comparability)
2. For no $x \in A$ does the relation $x < x$ hold. (Non-reflexivity)
3. If $x < y$ and $y < x$ then $x < z$. (Transitivity)

A relation which satisfies 2. and 3. is called a strict partial order on A.

Example 1.76. The usual meaning of $<$ on $\mathbb{R}$ is an order relation. What about $\leq$?

Example 1.77. if we return to our relations B, D and S from Example 1.44, we can see that B satisfies none of the three criteria for an order. The relation S satisfies 3. only. The relation D satisfies 2. and 3. and so is a strict partial order.

Suppose A and B are sets with orders $<_A$ and $<_B$, can we find an order on $A \times B$? Well we could say that $(a, b) < (a', b')$ if $a <_A a'$ and $B <_B b'$. This is called the *dictionary order* on $A \times B$.

We will consider the usual order $<$ on $\mathbb{R}$. Let $A \subset \mathbb{R}$. We say that b is the *largest element* of A if $b \in A$ and $x < b$ for all $x \in A - \{b\}$. We say that a is the *smallest element* of A if $a \in A$ and $a < x$ for all $x \in A - \{a\}$. Clearly A has at most one largest and one smallest element. Note that it does not have to have either; for example $(-1, 1) \subset \mathbb{R}$ has neither a largest nor a smallest element.

Definition 1.78. We say that A is *bounded above* if there exists $b \in \mathbb{R}$ such that $x \leq b$ for all $x \in A$. We call b an *upper bound* for A.

Example 1.79. If $A = (-1, 1)$ then 2 is an upper bound for A, as is 1. If $B = (-1, \infty)$ then B does not have any upper bounds.

The example above shows that upper bounds do not have to be unique. However there seems to be something special about the upper bound 1 in that example in that it is the smallest possible upper bound. We will look at that idea next:

Definition 1.80. If the set of all upper bounds for A has a smallest element it is called the *least upper bound* (or supremum) of A. We write $lub(A)$ or $sup(A)$.

Example 1.81. Clearly if $A = (-1, 1)$ then $lub(A) = 1$. Note that in this case $lub(A)$ does not belong to A. Let $B = [-1, 2]$, we can see that $lub(B) = 2$ and in this case the $lub(B)$ does belong to B.

Definition 1.82. We say that A is *bounded below* if there exists $a \in \mathbb{R}$ such that $a \leq x$ for all $x \in A$. We call a a *lower bound* for A. If the set of all lower bounds for A has a largest element it is called the *greatest lower bound* (or infimum) of A. We write $glb(A)$ or $inf(A)$.

Example 1.83. Clearly if $A = (-1, 1)$ then $-1, -2, -1.5$ etc. are all lower bounds for A and $glb(A) = -1$.

Consider the set $S = \{r \in \mathbb{Q} | r^2 < 2\}$ as a subset of $\mathbb{Q}$. S has lots of upper bounds in $\mathbb{Q}$ e.g. $b = 2, 3/2, ...$ However S does not have a least upper bound in $\mathbb{Q}$ (Intuitively the *lub* should be $\sqrt{2}$ but this is not in $\mathbb{Q}$). It seems natural that a set which is bounded above in $\mathbb{R}$ should have a least upper bound in $\mathbb{R}$. We will take this as an axiom:

The Axiom of Completeness: Every subset of $\mathbb{R}$ which is bounded above has a least upper bound in $\mathbb{R}$.

One consequence of this axiom is:

Theorem 1.84 (The Archimedian Property)**.** *If $x \in \mathbb{R}$, then there exists $n \in \mathbb{N}$ such that $x < n$.*

Proof: If the property does not hold then x is an upper bound for $\mathbb{N}$ so by the Axiom of Completeness $\mathbb{N}$ has a least upper bound $u \in \mathbb{R}$. Now $u - 1 < u$ and so $u - 1$ is not an upper bound for $\mathbb{N}$. Thus there exists $m \in \mathbb{N}$ such that $u - 1 < m$ but then $u < m + 1$. Since $m + 1 \in \mathbb{N}$ this means that u is not an upper bound for $\mathbb{N}$ and so we get a contradiction.

□

Theorem 1.85 (The density of $\mathbb{Q}$ in $\mathbb{R}$)**.** *Let $a, b \in \mathbb{R}$ with $a < b$. Then there exists $r \in \mathbb{Q}$ such that $a < r < b$.*

Proof: Without loss of generality, assume $0 \leq a < b$. We must find $m, n \in \mathbb{N}$ such that $a < \frac{m}{n} < b$.
Consider the number $\frac{1}{b-a}$. Since this number is a real number there exists $n \in \mathbb{N}$ such that $\frac{1}{b-a} < n$ (by The Archimedian Property). So $\frac{1}{n} < b - a$ or $a < b - \frac{1}{n}$.
Now choose m to be the smallest natural number greater than na (this is possible by The Archimedian Property). That is $m - 1 \leq na < m$. Therefore $a < m/n$.
Since $m - 1 \leq na$ we have $m \leq na + 1 < n(b - 1/n) + 1 = nb$ so $m/n < b$.
We have found $m, n \in \mathbb{N}$ such that $a < \frac{m}{n} < b$ as required.

□

Exercise 1.86. How would you prove this theorem if $a < 0$?

We need one more result:

Theorem 1.87 (The Nested Intervals Theorem)**.** *For each $n \in \mathbb{N}$, assume we have a closed interval $I_n = [a_n, b_n] = \{x \in \mathbb{R} | a_n \leq x \leq b_n\}$. Assume that each I_n contains I_{n+1}. Then $\cap_{n \in \mathbb{N}} I_n \neq \emptyset$.*

Proof: Let A be the set of left-hand endpoints of the intervals I_n so

$$A = \{a_n | n \in \mathbb{N}\}.$$

Then $A \subset \mathbb{R}$ and A is bounded above by each b_n so A as a least upper bound. Let $x = lub(A)$. We will show that $x \in I_n$ for all $n \in \mathbb{N}$.
Since x is a least upper bound for A we have that $a_n \leq x$ for all $n \in \mathbb{N}$.
Since each b_n is an upper bound for A and x is the least upper bound of A we have $x \leq b_n$ for all $n \in \mathbb{N}$.
Thus $a_n \leq x \leq b_n$ for all $n \in \mathbb{N}$, or $x \in I_N$ for all $n \in \mathbb{N}$. This means that $x \in \cap_{n \in \mathbb{N}} I_n$ and so $\cap_{n \in \mathbb{N}} I_n \neq \emptyset$.

□