MATH 1800 Notes

Kevin L

Winter Term 1 2022

Contents

1 Proofs

1.1 Proof by Induction

Definition 1.1 (The Principle of Mathematical Induction)**.** Let m be an integer, and let $P(n)$ be a statement for each integer $n \geq m$. If

1. $P(m)$ is true.
2. the implication if $P(k)$, then $P(k+1)$ is true. $\forall\, k \in \mathbb{Z} > m$.

$P(m)$ is called the **base case**, and $P(k+1)$ is called the **inductive step**.

Example. Prove $\forall\, n \in \mathbb{N}$, $1+2+3+\ldots+n = \frac{n(n+1)}{2}$. Since $1 = \frac{1(2)}{2}$, the base case holds. Suppose $1+2+3+\ldots+k = \frac{k(k+1)}{2}$ for any $k \in \mathbb{N}$. We must show that $1+2+3+\ldots+k+(k+1) = \frac{(k+1)(k+2)}{2}$.
We have

$$\begin{aligned} 1+2+3+\ldots+k+(k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= (k+1)(\frac{k}{2}+1) \\ &= (k+1)(\frac{k}{2}+\frac{2}{2}) \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Thus by the principle of mathematical induction, it follows the result holds for all n. □

Remark. There is an alternative proof to this problem discovered by Gauss. Let $S = 1+2+\cdots+(n-1)+n$. But $S = n+(n-1)+\cdots+2+1$. Adding these up, $2S = (n+1)+\cdots+(n+1)$. Note that there are n amount of terms. Then $S = \frac{n(n+1)}{2}$.

Example. Prove $\forall\, n \in \mathbb{N}$, $2^n > n$. Since $2^1 > 1$, the base case holds. Suppose $2^k > k \forall k \in \mathbb{N}$. Then we must show that $2^{k+1} > k+1$. We have

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &> 2k \\ &= k+k \\ &\geq k+1 && \text{(k} \geq 1 \text{ from def.)} \end{aligned}$$

□

Remark. Note that the base case does not need to start at 1, as shown below.

Examples. Example 1:
Prove $\forall\, n \geq m \in \mathbb{N}$, $2^n \geq n^2$. Consider

n	2^n	n^2
1	2	1
2	4	4
3	8	9
4	16	16
5	32	25
6	64	36

It appears this holds for $n \geq 5$.

Since $2^5 = 32 \geq 5^2 = 25$, the base case holds. Suppose $2^k > k^2$, for some $k \in \mathbb{Z}$ with $k \geq 5$. We have

$$\begin{aligned}
2^{k+1} &= 2^k \cdot 2^1 \\
&> 2k^2 \\
&= k^2 + k \cdot k \\
&\geq k^2 + 5k && (k \geq 5) \\
&= k^2 + 2k + 3k \\
&\geq k^2 + 2k + 15 && (k \geq 5) \\
&> k^2 + 2k + 1 \\
&= (k+1)^2
\end{aligned}$$

□

Example 2:
Prove $3 \mid (2^{2n} - 1)\ \forall n \geq 0$. We proceed by induction. When $n = 0$, we have $2^{2 \cdot 0} - 1$, which is 0, which is divisible by 3. Suppose $3 \mid (2^{2k} - 1)$ for some $k \in \mathbb{Z}$. Thus, $2^{2k} - 1 = 3c$ for some $c \in \mathbb{Z}$. Looking at $k + 1$, we have

$$\begin{aligned}
2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\
&= 2^2 \cdot 2^{2k} - 1 \\
&= 4(3c + 1) - 1 \\
&= 12c + 4 - 1 \\
&= 12c + 3 \\
&= 3(4c + 1)
\end{aligned}$$

Since $4c + 1 \in \mathbb{Z}$, $3 \mid 2^{2n} - 1$. □

Example 3:
Let $n \in \mathbb{N}$. Then $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$. We proceed by induction. Since $1^2 = 1 = \frac{(1)(2)(3)}{6}$, the base case holds. Suppose $1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$. We have

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\
&= (k+1)\left(\frac{k(2k+1) + 6(k+1)}{6}\right) \\
&= (k+1)\left(\frac{2k^2 + 7k + 6}{6}\right) \\
&= (k+1)\left(\frac{(k+2)(2k+3)}{6}\right) \\
&= \left(\frac{(k+1)(k+1+1)(2(k+1)+1)}{6}\right)
\end{aligned}$$

□

Proposition 1.2. Recall that $n! = 1(2)(3)\ldots(n)$.

Example. Let $n \in \mathbb{N}$. Then, $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$. We proceed by induction. $1 \cdot 1! = 2! - 1 = 1$, so

the base case holds. Suppose $1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! = (k+1)! - 1$. Then,

$$\begin{aligned} 1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! + (k+1) \cdot (k+1)! &= (k+1)! - 1 + (k+1)(k+1)!. \\ &= (k+1)! + (k+1)(k+1)! - 1 \\ &= (k+1)!(1 + (k+1)) - 1 \\ &= (k+1)!(k+2) - 1 \\ &= (k+2)! - 1 \end{aligned}$$

□

1.1.1 Proof by Strong Induction

Definition 1.3 (The Strong Principle of Mathematical Induction)**.** Let m be an integer, and let $P(n)$ be a statement for each integer $n \geq m$. If

1. P(m) is true
2. the implication if $P(i)$ for every i with $m \leq i \leq k$, then $P(k+1)$ is true for every integer $k \geq m$,

Then $P(n)$ is true for every integer $n \geq m$.
In both regular and strong induction, the base case is the same, and in the inductive step we assume an inductive hypothesis and must prove the property holds for $k+1$.
In regular induction, we get to assume the property holds for k. In strong induction, we get to assume the property holds for everything from the base case up to k.

Proposition 1.4. We can define a sequence by **recursion**.

Example. Consider $a_1 = 1$, $a_2 = 4$, and $a_n = 2a_{n-1} - a_{a-2} + 2$ for $n \geq 3$. This is the sequence $(1, 4, 9, 16, 25, \ldots)$. Let us prove the general formula. Then, $a_n = n^2$ for all $n \in \mathbb{N}$. We proceed by strong induction.
Since $a_1 = 1 = 1^2$, the result holds for $n = 1$.
Let $k \in \mathbb{N}$ and suppose a_i is i^2 for all $1 \leq i \leq k$. We must show that $a_{k+1} = (k+1)^2$. For $k \geq 2$, We have

$$\begin{aligned} a_{k+1} &= 2a_k - a_{k-1} + 2 \\ &= 2k^2 - (k-1)^2 + 2 && \text{(By our inductive hypothesis)} \\ &= 2k^2 - (k^2 - 2k + 1) + 2 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

When $k = 1$, $a_{k+1} = a_2 = 4 = 2^2 = (k+1)^2$. □

Proposition 1.5. The **Fibonacci Numbers** satisfy $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. The first few Fibonacci Numbers are $1, 1, 2, 4, 5, 6, 13, 21, 34, 55, 89$. This sequence has many interesting properties.

Example. Let $m, n \geq 2$. Then,

$$F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$$

Setting $m = n$, and then $m = n - 1$ yields the formulas

$$F_{2n} = F_n(F_{n-1} + Fn + 1)$$

and

$$F_{2n-1} = F_{n-1}^2 + F_n^2$$

Let $m, n \in N$ with $n \geq 2$. Then

$$F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$$

.

Fix $m \in \mathbb{N}$. We proceed by induction on n. When $n = 2$,

$$\begin{aligned} F_m F_1 + F_{m+1} F_2 &= F_m + F_{m+1} \\ &= F_{m+2} \end{aligned}$$

and so the base case holds. Let $k \in \mathbb{N}$ with $k \geq 2$ and suppose for i with $2 \leq i \leq k$, we have

$$F_m + i = F_m F_{i-1} + F_{m+1} F_i$$

For $k \geq 3$, we have

$$\begin{aligned} F_{m+k+1} &= F_{m+k} + F_{m+k-1} && \text{(By def. of fib)} \\ &= F_m F_{k-1} + F_{m+1} F_k + F_m F_{k-2} + F_{m+1} F_{k-1} \\ &= F_m (F_{k-1} + F_{k-2}) + F_{m+1} (F_k + F_{k-1}) \\ &= F_m F_k + F_{m+1} F_{k+1} && \text{(By def. of fib)} \end{aligned}$$

When $k = 2$,

$$\begin{aligned} F_m F_k + F_{m+1} F_{k+1} &= F_m F_2 + F_{m+1} F_3 \\ &= F_m + 2F_{m+1} \\ &= F_m + F_{m+1} + F_{m+1} \\ &= F_{m+2} + F_{m+1} \\ &= F_{m+3} \end{aligned}$$

□

Remark. We will cover prove or disprove questions.

Examples. Example 1:

For $n \in \mathbb{N}$, $2^{(2^n)} \geq 4^{n!}$. Let's try some values. This statement is false with $n = 3$ yielding a counterexample.

Example 2:

For every non-negative integer n, 5 divides $2 \cdot 4^n + 3 \cdot 9^n$. Let's try some values. We think this may be true, so let us attempt a proof. We proceed by induction. When $n = 0$, $2 \cdot 4^0 + 3 \cdot 9^0 = 5$, which is divisible by 5. The base case holds. Let $k \in \mathbb{N} \cup \{0\}$ and suppose $5 \mid (2 \cdot 4^k + 3 \cdot 9^k)$. Then $2 \cdot 4^k + 3 \cdot 9^k = 5c$ for some $c \in \mathbb{Z}$. We have

$$\begin{aligned} 2 \cdot 4^{k+1} + 3 \cdot 9^{k+1} &= 2 \cdot 4 \cdot 4^k + 3 \cdot 9 \cdot 9^k \\ &= 2 \cdot 4 \cdot 4^k + 9(5c - 2 \cdot 4^k) \\ &= 8 \cdot 4^k + 45c - 18 \cdot 4^k \\ &= 45c - 10 \cdot 4^k \\ &= 5(9c - 2 \cdot 4^k) \end{aligned}$$

Since $9c - 2 \cdot 4^k \in \mathbb{Z}$, $5 \mid 2 \cdot 4^n + 3 \cdot 9^n$. □

Example 3:

Every even integer $n \geq 4$ can be written as the sum of two primes. This is a famous problem called **Goldbach's**

Conjecture, and this is still an open problem.

2 Relations

Remark. Recall a few theorems: Let $x, y, z \in \mathbb{R}$.

- If $x = y$ and $y = z$, then $x = z$.
- If $x < y$ and $y < z$, then $x < z$.

These different relations share the same property.

Definition 2.1. Let A, B be sets. A **relation** R from A to B is a subset of the set

$$\{(a, b) \mid a \in A \text{ and } b \in B\}$$

which is equivalent to $A \times B$.
Here, (a, b) is an ordered pair. If $(a, b) \in R$, we say that a is related to b by R, and we write $a \ R \ b$. If $(a, b) \notin R$, we say that a is not related to b by R, and we write $a \not R \ b$.
Since $\emptyset$ is a subset of any set, it is always a relation from A to B. For the relation $\emptyset$, no element of A is related to any element of B.
Since a set is always a subset of itself,

$$\{(a, b) \mid a \in A \text{ and } b \in B\}$$

is always a relation from A to B. In this relation, each element of A is related to every element of B.

Definition 2.2. Let R be a relation from A to B. Then the **domain** of R, denoted by dom R is the set

$$\{a \in A \mid (a, b) \in R \text{ for some } b \in B\}$$

The **range** of R, denoted by range(R) is the set

$$\{b \in B \mid (a, b) \in R \text{ for some } a \in A\}$$

Definition 2.3. Let R be a relation from A to B. The **inverse relation** of R, denoted R^{-1}, which is

$$\{(b, a) \mid (a, b) \in R\}$$

It is a relation from B to A.

Example. Let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$. Suppose $R = \{(a, 1), (a, 3), (b, 2), (b, 3)$. Here, $b \ R \ 2$, but $b \not R \ 1$.
The domain of R is $\{a, b\}$, while the range is $\{1, 2, 3\}$.

$$R^{-1} = \{(1, a), (3, a), (2, b), (3, b)\}$$

Definition 2.4. A **relation on a set** A is a relation from A to A.

Examples. We define a relation on $\mathbb{Z}$:

$$R = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } b = a + c \text{ for some } c \in \mathbb{N}\}$$

We have for example, $2R4, 3R4, 4 \not R \ 4, 5 \not R \ 4$.
In fact, this is the $<$ relation on $\mathbb{Z}$.
We define a relation on $\mathbb{Z}$:

$$R = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } 5 \mid (a - b)\}$$

This is congruence modulo 5 relation on $\mathbb{Z}$.

Definition 2.5. We define some properties of relations. Let R be a relation on a set A.

1. R is **reflexive** if $\forall x \in A$, $x \; R \; x$.
2. R is **symmetric** if $\forall x, y \in A$, $x \; R \; y \implies y \; R \; x$.
3. R is **transitive** if $\forall x, y, z \in A$, if $(x \; R \; y \wedge y \; R \; z) \implies x \; R \; z$.

Remark. Note for transitivity, x, y, z do not have to be distinct. E.g, if $x \; R \; y$ and $y \; R \; x$, then $x \; R \; x$. Furthermore, when manually checking we can ignore any elements of the form (x, x) since they cannot lead to counterexamples. Also remember if $a \; R \; b$ and $b \; R \; a$, check for transitivity both ways, i.e. $a \; R \; a$ and $b \; R \; b$.

Examples. Let $A = \{1, 2, 3\}$. Consider

$$R_1 = \{(a, b), (b, c), (c, b)\}$$
$$R_2 = \{(a, a), (a, b), (b, a), (b, b), (b, c), (c, b), (c, c)\}$$
$$R_3 = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$$
$$R_4 = \{(b, c)\}$$

R_1 is not reflective since for example, $a \not R \; a$. R_1 is not symmetric since for example, $a \; R \; b \not\implies b \; R \; a$. R_1 is not transitive since for example, $a \; R \; b$ and $b \; R \; c$ but $a \not R \; c$.
R_2 is reflective. R_2 is symmetric. R_2 is not transitive since for example, $a \; R \; b$ and $b \; R \; c$ but $a \not R \; c$.
R_3 is reflective. R_3 is symmetric. R_3 is transitive.
R_4 is not reflective since for example, $a \not R \; a$. R_4 is not symmetric since for example, $b \; R \; c \not\implies c \; R \; b$. R_3 is transitive (vacuously).

Definition 2.6. A relation on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive. The equality relation and R_3 above fulfill this criteria.

Definition 2.7. Let R be an equivalence relation on A. For $a \in A$, the set

$$[a] = \{x \in A \mid x \; R \; a\}$$

is called an **equivalence class**. It consists of all elements of A that are related to A.

Examples. Fix a number $n \in \mathbb{N}$, with $n \geq 2$ and consider the congruence modulo n relation on $\mathbb{Z}$. Since

$$x \equiv x \pmod{n}$$
$$x \equiv y \implies y \equiv x$$
$$x \equiv y \wedge y \equiv z \implies x \equiv z$$

The congruence relation is an equivalence class.
Example 2:
Let $A = \{a, b, c\}$ and $R = \{(a, a), (a, b), (b, a), (b, a), (c, c)\}$ Then

$$[a] = \{a, b\}$$
$$[b] = \{a, b\}$$
$$[c] = \{c\}$$

Example 3:

Let $A = \{1, 2, 3\}$ and $R = \{(a, a), (a, b), (b, a), (b, a), (c, c)\}$ It can be shown R is an equivalence relation. Then,

$$\begin{aligned}
[1] &= \{1, 3, 6\} \\
[2] &= \{2, 4\} \\
[3] &= \{1, 3, 6\} \\
[4] &= \{2, 4\} \\
[5] &= \{5\} \\
[6] &= \{1, 3, 6\}
\end{aligned}$$

Example 4:
Consider the equality relation on $\mathbb{Z}$. Let $a \in \mathbb{Z}$, then

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \mid x \ R \ a\} \\
&= \{x \in \mathbb{Z} \mid x = a\} \\
&= \{a\}
\end{aligned}$$

Example 5:
Define R on Z by $a \ R \ b$ iff $|a| = |b|$. One may show this is a equivalence relation. Then,

$$[a] = \{x \in \mathbb{Z} \mid x \ R \ a\} = \{x \in \mathbb{Z} \mid |x| = |a|\} = \{a, -a\}$$

Example 6:
Define R on Z by $a \ R \ b$ if $5a + b$ is even. Then R is an equivalence relation.
We first show R us reflexive. Let $a \in \mathbb{Z}$, then $5a + a = 6a = 2 \cdot 3a$. Since $3a \in \mathbb{Z}$, $5a + a$ is even and so R is reflexive.
Now we show R is symmetric. Suppose $a \ R \ b$, then $5a + b = 2k$ for some $k \in \mathbb{Z}$. We have

$$\begin{aligned}
5b + a &= 5(2k - 5a) + a \\
&= 10k - 25a + a \\
&= 10k - 24a \\
&= 2(5k - 12a)
\end{aligned}$$

Thus, $b \ R \ a$.
We now show R is transitive. Suppose $a \ R \ b$ and $b \ R \ c$. Then, $5a + b = 2k$ and $5b + c = 2l$ for some $k, l \in \mathbb{Z}$. We have

$$\begin{aligned}
5a + c &= 2k - b + 2l - 5b \\
&= 2k + 2l - 6b \\
&= 2(k + l - 3b)
\end{aligned}$$

Since the above is an integer, $5a + c$ is even and so R is transitive.
Let's look at the equivalence classes. First, we check for 1 specific element.

$$[0] = \{x \in \mathbb{Z} \mid x \ R \ 0\} = \{x \in \mathbb{Z} \mid 5x \text{ is even}\} = \{x \in \mathbb{Z} \mid x \text{ is even}\}$$

Let $a = 2k$. Then,

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \mid x \ R \ a\} \\
&= \{x \in \mathbb{Z} \mid 5x + a \text{ is even}\} \\
&= \{x \in \mathbb{Z} \mid x \text{ is even}\}
\end{aligned}$$

Let $b = 2l + 1$. Then,

$$\begin{aligned} b &= \{x \in \mathbb{Z} \mid 5x + b \text{ is even}\} \\ &= \{x \in \mathbb{Z} \mid x \text{ is odd}\} \end{aligned}$$

Thus, there are 2 distinct classes

$$[0] = [2] = [4] = \dots$$

and

$$[1] = [3] = [5] = \dots$$

Theorem 2.8. Let R be an equivalence relation on a non-empty set A. Let $a, b \in A$. Then

$$[a] = [b] \Leftrightarrow a \; R \; b$$

Proof.
We prove the forwards direction. Suppose $[a] = [b]$. Then as R is reflective we have $a \; R \; a$, and so $a \in [a]$ and since $[a] = [b]$, we have $a \in [B]$. Thus, $a \; R \; b$.
We prove the reverse direction. Suppose $a \; R \; b$. We show $[a] \subseteq [b]$. Let $x \in [a]$, then $x \; R \; a$. Then $x \; R \; a$ and $a \; R \; b$, and as R is transitive, we have $x \; R \; b$ and so $[a] \subseteq [b]$.
Now we show $[b] \subseteq [a]$. Let $x \in [b]$, then $x \; R \; b$. As $a \; R \; b$, and R is symmetric, we have $b \; R \; a$. We have $x \; R \; b$ and $b \; R \; a$, and as R is transitive, we have $x \; R \; a$. Thus, $[b] \subseteq [a]$.
Thus $[a] = [b]$. □

Theorem 2.9. Let R be a equivalence relation on a non-empty set A. Then each element belongs to 1 equivalence class.

Proof. Let $a \in A$. As R is reflective, we have $a \; R \; a$, so $a \in [A]$. We must now show uniqueness. Suppose $a \; R \; b$. By previous theorem, $[b] = [a]$, and thus a belongs to 1 unique equivalence class. □

Proposition 2.10. Equivalence classes of R form a partition of A.

- They are non-empty.
- They are disjoint.
- They have a union of A.

Example. We know that congruence mod n is an equivalence relation. What are the equivalence classes? We work with mod 3 for now.

$$[0] = \{x \in \mathbb{Z} \mid x \; R \; 0\} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 3\} = \{x \in \mathbb{Z} \mid 3 \mid x\} = \{3k \mid k \in \mathbb{Z}\}$$

$$[1] = \{x \in \mathbb{Z} \mid x \; R \; 1\} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\} = \{x \in \mathbb{Z} \mid 3 \mid (x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\}$$

$$[2] = \{x \in \mathbb{Z} \mid x \; R \; 2\} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\} = \{x \in \mathbb{Z} \mid 3 \mid (x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\}$$

The union of these classes is $\mathbb{Z}$. In general, there are n equivalence classes for the relation congruence mod n.

Proposition 2.11.

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

These are called the integers modulo n, and the elements are called **residue classes**.

Definition 2.12. Let $[a]$ and $[b]$ be two residue classes in $\mathbb{Z}_n$. We define

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

Example. We have (working in $\mathbb{Z}_7$)

$$[6] + [3] = [6 + 3] = [9] = [7]$$

and

$$[6][3] = [6 \times 3] = [18]$$

Remark. There is a potential problem. An equivalence class modulo n has an infinite number of representatives, but our operation seems to depend on which ones are being used.

Theorem 2.13. Let $n \in \mathbb{N}$, $n \geq 2$. Then $+$, $\times$ on $\mathbb{Z}_n$ are well defined. That is, if $[a] = [b]$ and $[c] = [d]$, then $[a + c] = [b + d]$ and $[ac] = [bd]$.

Proof. Suppose $[a] = [b]$ and $[c] = [d]$. Then $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Thus $n \mid (a - b)$ and $n \mid (c - d)$. Thus $a - b = nk$ $(a = nk + b)$ and $c - d = nl$ $(c = nl + d)$ for some $k, l \in \mathbb{Z}$. We have

$$\begin{aligned} a + c - (b + d) &= a - b + c - d \\ &= nk - nl \\ &= n(k - l) \end{aligned}$$

Since $k - l \in \mathbb{Z}$, we have $n \mid ((a + c) - (b + d))$, thus $a + c \equiv b + d \pmod{n}$ and so $[a + b] = [c + d]$.
We also have

$$\begin{aligned} ac - bd &= (b + nk)c - b(c - nl) \\ &= n(kc + bl) \end{aligned}$$

So by the same argument $[ac] = [bd]$. □

Definition 2.14. Let $k \in \mathbb{N}$, $a \in \mathbb{Z}$. Then

$$[a^k] = [a \cdot a \cdot a \ldots] \ (k \text{ times}) \ = [a]^k$$

Example. Show that for $n \in \mathbb{N}$, 5 divides $2 \cdot 4^n + 3 \cdot 9^n$. We have

$$\begin{aligned} [2 \cdot 4^n + 3 \cdot 9^n] &= [2 \cdot 4^n] + [3 \cdot 9^n] \\ &= [2 \cdot 4^n] + [3][9^n] \\ &= [2 \cdot 4^n] + [3][9]^n \\ &= [2 \cdot 4^n] + [3][4]^n \\ &= [2 \cdot 4^n] + [3][4^n] \\ &= [2 \cdot 4^n] + [3 \cdot 4^n] \\ &= [2 \cdot 4^n + 3 \cdot 4^n] \\ &= [5 \cdot 4^n] \\ &= [5][4^n] \\ &= [0][4^n] \\ &= [0 \cdot 4^n] \\ &= [0] \end{aligned}$$

Thus for any $n \in \mathbb{N}$, $2 \cdot 4^n + 3 \cdot 9^n \equiv 0 \pmod 5$.
We can drop the square brackets and just write $\pmod 5$.

$$\begin{aligned} 2 \cdot 4n + 3 \cdot 9n &\equiv 2 \cdot 4n + 3 \cdot 4n \pmod 5 \\ &\equiv 5 \cdot 4n \pmod 5 \\ &\equiv 0 \cdot 4n \pmod 5 \\ &\equiv 0 \pmod 5 \end{aligned}$$

Proposition 2.15. Let $n \in \mathbb{N}$. Then $9 \mid n$ iff 9 divides the digits of n.

Proof. Let $d_k, d_{k-1}, \ldots, d_1, d_0$ be the digits of n.

$$n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10^1 + d_0$$

$$\begin{aligned} n &\equiv d_k 1^k + d_{k-1} 1^{k-1} + \cdots + d_1 + d_0 \pmod 9 \\ &\equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \end{aligned}$$

This is because $10 \equiv 1 \pmod 9$.
Suppose $9 \mid n$, then $n \equiv 0 \pmod 9$, so by the above the digits must be equivalent to 0. Thus $9 \mid (d_k + d_{k-1} + \cdots + d_1 + d_0)$.
Now suppose $9 \mid (d_k + d_{k-1} + \cdots + d_1 + d_0)$. Then by above $n \equiv 0 \pmod 9$, and thus $9 \mid n$. □

2.1 Functions

Definition 2.16. Let A and B be non-empty sets. A **function** f from A to B, written $f : A \to B$ is a relation from A to B where every element of A is the first co-ordinate of exactly one ordered pair in f.

Definition 2.17. Here, dom $f = A$

Definition 2.18. B is called the **co-domain** of f.

Definition 2.19. If $(a, b) \in f$, we write $f(a) = b$.

Definition 2.20. b is called the **image** of a, and we say that f **maps** a to b.

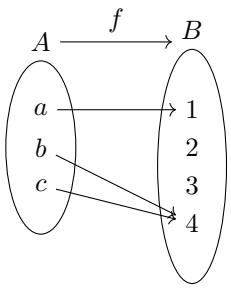
Definition 2.21. The **range** of f is

$$\begin{aligned} \text{range } f &= \{b \in B \mid (a, b) \in f \text{ for some } a \in A\} \\ &= \{f(a) \mid a \in A\} \end{aligned}$$

Example. Let $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$. Which of the following are functions?

$$\begin{aligned} f_1 &= \{(a, 1), (b, 4), (c, 4)\} \\ f_2 &= \{(a, 2), (a, 3), (b, 4), (c, 1)\} \\ f_3 &= \{(a, 1), (b, 2)\} \end{aligned}$$

Of above, only f_1 is a function.



The range of f is $\{1, 4\}$.

Definition 2.22. We say two functions $f : A \to B$ and $g : A \to B$ are **equal**, written $f = g$ if for all $a \in A$, $f(a) = g(a)$. This implies that f and g are equal as relations.

Example. Let $f = \{(x, x^2 \mid x \in \mathbb{R}\}$ is a function from $\mathbb{R}$ to $\mathbb{R}$. Here, for any $x \in \mathbb{R}$, we have $f(x) = x^2$.
Note that the function f is the set of ordered pairs, while $f(x) = x^2$ is the rule that describes the image of an arbitrary $x \in \mathbb{R}$.

Definition 2.23. Let $f : A \to B$ be a function, and let $C \subseteq A$. The image of C is the set

$$f(C) = \{f(x) \mid x \in C\}$$

We have $f(C) \subseteq B$. Note that $f(A) = \operatorname{range} f$.

Definition 2.24. Let $D \subseteq B$. The **inverse image** or **preimage** of D is the set

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}$$

Example. Let $A = \{a, b, c, d, e\}$ and $B = \{1, \ldots, 6\}$. Let $f = \{(a, 5), (b, 2), (c, 3), (d, 5), (e, 6)\}$.
Let $c_1 = \{c, d, e\}, c_2 = \{a, d\}$, and $c_3 = \{b\}$.

$$\begin{aligned} f(c_1) &= \{3, 5, 6\} \\ f(c_2) &= \{5\} \\ f(c_3) &= \{2\} \\ f(A) &= \{2, 3, 5, 6\} \end{aligned}$$

$$\begin{aligned} f^{-1}(\{3, 5, 6\}) &= \{a, c, d, e\} \\ f^{-1}(\{5\}) &= \{a, d\} \\ f^{-1}(\{1\}) &= \emptyset \\ f^{-1}(B) &= A \end{aligned}$$

Example. Let $f : \mathbb{Q} \to \mathbb{Q}$ be defined by $f(r) = \frac{3r}{2}$. Let E be the set of even integers.

$$
\begin{aligned}
f(\mathbb{Z}) &= \{f(n) \mid n \in \mathbb{Z}\} \\
&= \{\frac{3n}{2} \mid n \in \mathbb{Z}\}
\end{aligned}
$$

$$
\begin{aligned}
f(E) &= \{f(n) \mid n \in E\} \\
&= \{f(2k) \mid k \in \mathbb{Z}\} \\
&= \{3k \mid k \in \mathbb{Z}\}
\end{aligned}
$$

$$
\begin{aligned}
f^{-1}(\mathbb{Z}) &= \{r \in \mathbb{Q} \mid f(r) \in \mathbb{Z}\} \\
&= \{r \in \mathbb{Q} \mid \frac{3r}{2} \in \mathbb{Z}\} \\
&= \{\frac{2n}{3} \mid n \in \mathbb{Z}\}
\end{aligned}
$$

$$
\begin{aligned}
f^{-1}(E) &= \{r \in \mathbb{Q} \mid f(r) \in E\} \\
&= \{r \in \mathbb{Q} \mid \frac{3r}{2} \in E\} \\
&= \{\frac{4k}{3} \mid k \in \mathbb{Z}\}
\end{aligned}
$$

Definition 2.25. Let A and B be non-empty sets. Then B^A is the set of all functions from A to B.
In general, if A, B are finite, then $|B^A| = |B|^{|A|}$.

Example. Let $A = \{a, b, c\}$ and $B = \{x, y\}$.

$$
\begin{aligned}
f_1 &= \{(a, x), (b, x), (c, x)\} \\
f_2 &= \{(a, x), (b, x), (c, y)\} \\
f_3 &= \{(a, x), (b, y), (c, x)\} \\
f_4 &= \{(a, y), (b, x), (c, x)\} \\
f_5 &= \{(a, x), (b, y), (c, y)\} \\
f_6 &= \{(a, y), (b, y), (c, x)\} \\
f_7 &= \{(a, y), (b, x), (c, y)\} \\
f_8 &= \{(a, y), (b, y), (c, y)\}
\end{aligned}
$$

$$
B^A = \{f_1, \ldots, f_8\}
$$

2.1.1 Properties of Functions

Definition 2.26. A function $f : A \to B$ is **injective** or **one-to-one** if $\forall x, y \in A$,

$$
x \neq y \implies f(x) \neq f(y)
$$

and

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

If A and B are finite, and f is injective, then $|A| \leq |B|$.

Example. Prove that $f(x) = x^2 + x + 1$ is not injective.
Let $x, y \in \mathbb{R}$ and suppose $f(x) = f(y)$. Then

$$\begin{aligned} x^2 + x + 1 &= y^2 + y + 1 \\ 0 &= x^2 - y^2 + x - y \\ &= (x - y)(x + y) + (x - y) \\ &= (x - y)(x + y + 1) \end{aligned}$$

This is satisfied when $x = y$ or when $x + y + 1 = 0$. Thus $f(x) = f(y)$ does not imply $x = 0$ as there is another possibility.

Definition 2.27. A function $f : A \to B$ is **surjective** or **onto** if for each $y \in B$, there exists $x \in A$ with $f(x) = y$.
Equivalently, f is surjective if range $f = B$. That is $f(A) = B$.
If A and B are finite sets and f is surjective, then $|A| \geq |B|$.

Example. Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 7x + 5$ is surjective.
Rough: Given $y \in \mathbb{R}$, show that $\exists x \in \mathbb{R}$ s.t. $f(x) = y$. That is, $7x + 5 = y \Leftrightarrow x = \frac{y-5}{7}$.
Proof: Let $y \in \mathbb{R}$, and let $x = \frac{y-5}{7}$. Then $f(x) = y$.

Example. Show that $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 7x + 5$ is not surjective.
Since $0 \in \mathbb{Z}$, but $\nexists x \in \mathbb{Z}$ s.t. $f(x) = 0$, f is not surjective. (We need $x = \frac{-5}{7}$)

Definition 2.28. A function $f : A \to B$ is **bijective** if it is injective and surjective.
If A and B are finite sets and f is bijective, then $|A| = |B|$.

Remark. Injective means everything gets "hit" at most once.
Surjective means everything gets "hit" at least once.
Bijective means everything gets "hit" exactly once.
A bijective function from A to B is a perfect pairing of the elements of A with the elements of B.

Example. Show that $f : \mathbb{R} - \{-1\} \to \mathbb{R} - \{1\}$ is bijective.
We show f is injective. Suppose $f(x) = f(y)$, for $x, y \in \text{dom } f$.
Then

$$\begin{aligned} \frac{x-1}{x+1} &= \frac{y-1}{y+1} \\ \implies (x-1)(y+1) &= (y-1)(x+1) \\ \implies xy + x - y - 1 &= xy + y - x - 1 \\ \implies x - y &= y - x \\ \implies 2x &= 2y \\ \implies x &= y \end{aligned}$$

Rough Work: Given $y \in \mathbb{R} - \{1\}$, we find $x \in \text{dom } f$ with $f(x) = y$.

$$\begin{aligned} \frac{x-1}{x+1} &= y \\ \Leftrightarrow x - 1 &= y(x+1) \\ \Leftrightarrow x - 1 &= yx + y \\ \Leftrightarrow x - yx &= y + 1 \\ \Leftrightarrow x(1-y) &= y + 1 \\ \Leftrightarrow x &= \frac{y+1}{1-y} \end{aligned}$$

Proof: We show f is surjective. Let $y \in \mathbb{R} - \{1\}$. Then take $x = \frac{y+1}{1-y}$. $f(x) = y$.

Definition 2.29. Let A be nonempty set. The function $i_A : A \to A$ defined by $i_A(a) = a$ for all $a \in A$ is called the **identity function** on A.

Definition 2.30. Let A, B, C be non-empty sets, and let $f : A \to B$ and $g : B \to C$ be functions. The composition $g \circ f$ is the function from $A \to C$ defined by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$.

Example. Let

$$A = \{1, 2, 3, 4\}$$
$$B = \{a, b, c, d\}$$
$$C = \{x, y, z\}$$

We define $f : A \to B$ and $g : B \to C$ as

$$f = \{(1, c), (2, b), (3, a), (4, a)\}$$
$$g = \{(a, x), (b, z), (c, x), (d, y)\}$$

Then $g \circ f = \{(1, x), (2, z), (3, x), (4, x)\}$.

Example. Let $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = 2n + 1$ and $g(n) = n^2 - 1$.
Then $g \circ f = (2n + 1)^2 - 1$ and $f \circ g = 2(n^2 - 1) + 1$.

Theorem 2.31. Let $f : A \to B$ and $g : B \to C$. Then

- If f, g are injective, then $f \circ g$ is injective.
- If f, g are surjective, then $f \circ g$ is surjective.

Proof. Let f, g be injective. Suppose $(g \circ f)(x) = (g \circ f)(y)$. Then

$$\begin{aligned} (g \circ f)(x) &= (g \circ f)(y) \\ \implies g(f(x)) &= g(f(y)) \\ \implies f(x) &= f(y) \\ \implies x &= y \end{aligned}$$

Thus $f \circ g$ is injective.
Let f, g be surjective. Let $c \in C$. Since g is surjective, we have $b \in B$ with $g(b) = C$. Since f is surjective, we have $a \in A$ where $f(a) = b$. We have

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) \\ &= f(b) \\ &= c \end{aligned}$$

□

Theorem 2.32. Let $f : A \to B$ be a function. The inverse relation $f^{-1} : B \to A$ is a function iff f is bijective. Furthermore, if f is bijective, so is f^{-1}.

Proof. We prove the forwards direction. Suppose f^{-1} is a function from B to A. We show that f is bijective.
Suppose $f(x_1) = f(x_2) = y$ where $x_1, x_2 \in A$ and $y \in B$. Then, $(x_1, y), (x_2, y) \in f$ and so $(y, x_1), (y, x_2) \in f^{-1}$. Since f^{-1} is a function, $x_1 = x_2$. Thus f is injective.
Now let $y \in B$. Since f^{-1} is a function from B to A, there is some $x \in A$ with $f^{-1}(y) = x$. That is, $(y, x) \in f^{-1}$, and so $(x, y) \in f$. Hence $f(x) = y$. Thus f is surjective,
As f is injective and surjective, it is bijective.
Now we prove the reverse direction.
Suppose f is bijective. We will show f^{-1} is a function.
Let $b \in B$. Since f is surjective, there is an $a \in A$ such that $f(a) = b$. Then $(a, b) \in f$ and so $(b, a) \in f^{-1}$. We must show that (b, a) is the unique element with first element b. Suppose $(b, a), (b, a') \in f^{-1}$. Then $(a, b) \in f$ and $(a', b) \in f$. Since f is injective, $a' = a$. Thus $\forall b \in B, \exists! a$ with $(b, a) \in f^{-1}$. Thus f^{-1} is a function.
Finally, we show that if f is bijective, so is f^{-1}.
Suppose $f^{-1}(x_1) = f^{-1}(x_2) = y$ for $x_1, x_2 \in B$ and $y \in A$. The ordered pairs

$$\begin{aligned}(x_1, y), (x_2, y) \in f^{-1} &\implies (y, x_1), (y, x_2) \in f \\ &\implies x_1 = x_2\end{aligned}$$

since f is a function. Thus f^{-1} is injective.
Let $a \in A$ and let $f(a) = b$. Then $(a, b) \in f \implies (b, a) \in f^{-1}$. Since f^{-1} is a function, $f^{-1}(b) = a$. Thus f^{-1} is surjective. As f^{-1} is injective and surjective, it is bijective. □

Theorem 2.33. If $f : A \to B$ and $g : B \to A$ are functions satisfying $g \circ f = i_A$ and $f \circ g = i_B$, then f, g are bijective with $g = f^{-1}$.

Proof. Let $f : A \to B$ and $g : B \to A$. Let $a \in A$ and suppose $f(a) = b$. Then $(a, b) \in f$, and so $(b, a) \in f^{-1}$. Thus $f^{-1}(b) = a$.
We have

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$$

and

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$$

□

Example. We saw $f : \mathbb{R} - \{-1\} \to \mathbb{R} - \{1\}$ defined by $f(x) = \frac{x-1}{x+1}$ is bijective. Let's find a formula for f^{-1}.
We use the fact that $(f \circ f^{-1})(x) = x$.
Thus,

$$\begin{aligned} x &= f(f^{-1}(x)) \\ &= \frac{ff^{-1}(x) - 1}{f^{-1}(x) + 1} \\ \implies x f^{-1}(x) + x &= f^{-1}(x) - 1 \\ \implies x f^{-1}(x) - f^{-1}(x) &= -1 - x \\ \implies f^{-1}(x)(x - 1) &= -1 - x \\ \implies f^{-1}(x) &= \frac{1 + x}{1 - x} \end{aligned}$$

Remark. In general, $f^{-1}(x) \neq \frac{1}{f(x)}$.

Remark. It's not always possible to solve for the formula of an inverse function algebraically. For example,
One may show that the function e^x is bijective. We call the inverse $\ln x$.
One may show that the function $\sin x$ is bijective (on an interval). We call the inverse $\arcsin x$.
One may show that the function $f(x) = 3x^7 + 5x^3 + 4x - 1$ is bijective. There is no way to write a formula for the inverse. As a set, it is

$$f^{-1} = \{(3x^7 + 5x^3 + 4x - 1, x) \mid x \in \mathbb{R}\}$$

3 Counting Arguments

Definition 3.1. The **Principle of Inclusion/Exclusion** states, if A_1, A_2, A_3 are finite sets, then:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Note that if $A_1, A_2, \ldots, A_n$ are mutually disjoint, then

$$|A_1 \cup A_2 \cup dots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

This is called **sum rule**

Definition 3.2. Suppose a procedure can be broken down into a sequence of 2 tasks, and for each of the n_1 ways to do the first task, there are n_2 ways to do the second. Then there are $n_1 n_2$ ways to do the procedure. This is the **product rule**.

Example. How many 2 letter initials are there?
26 choices for first, 26 for second. Total is 26×26.
How many non-repeating? Total is 26×25.

Example. If $A = \{x_1, \ldots, x_m\}$ and B are finite sets with $|A| = m$ and $|B| = n$, how many functions are there that map from A to B?
Assign values to $f(x)$ for each of the elements of A.
For x_1, there are n choices. For x_2, there are n choices and so on.
Thus we have $n \cdot n \cdot n \cdot \cdots = n^m = |B|^|A|$
How many injective functions? For x_1, there are n choices. For x_2, there are $n-1$ choices and so on.
Thus we have $n(n-1)\ldots(n-(m-1)) = \frac{n!}{(n-m)!}$

The Pigeonhole Principle. Let $k \in \mathbb{N}$. If $k+1$ or more objects are placed into k boxes, then at least one box contains two or more objects.

Proof. Suppose not. Then each of the k boxes contains at most one object, giving at most k objects. A contradiction. □

Example. Let $f : A \to B$ be a function with $|A| \geq k+1$ and $|B| = k$. Then f is not injective.
For each $y \in B$, we can form the box or set of all $x \in A$ with $f(x) = y$.
We have k boxes and at least $k+1$ objects, so there must exist $y \in B$ such that $f(x) = y$ for 2 values of x or more.

Definition 3.3. Given a collection of distinct objects, a **permutation** is an ordering of the objects. An **r-permutation** is an ordering of r of the objects. $P(n, r)$ is the number of r-permutations of a set of n distinct objects.
If $r \leq n$, then $P(n, r) = \frac{n!}{(n-r)!}$

Example. How many ways a deck of cards can be shuffled?
$P(52, 52) = \frac{52!}{0!} = 52!$

Example. A raffle is held with 40 names. There are distinct 1st, 2nd, 3rd place prizes. No one can win more than once. Then there are

$$P(40, 3) = \frac{40!}{37!} = 40 \cdot 39 \cdot 38$$

winning combinations

Definition 3.4. The number of **combinations** $C(n,r)$ is the number of unordered selections of r elements from a set of n distinct elements.

$$C(n,r) = \frac{n!}{(n-r)!r!}$$

Example. How many 5 card hands can be dealt from a deck?

$$C(52,5) = \frac{52!}{5!(52-5)!} = 259,960$$

Definition 3.5. We can sometimes prove identities by giving 2 different ways to count the same thing. This is called a **combinatoral proof**.

Example. Show $C(n,0) + C(n,1) + \dots C(n,n) = 2^n$.
We count the number of subsets of an n element set in 2 ways. For each element, we can either include it in the subset or not. By the product rule, there are 2^n subsets.
On the other hand, there are $C(n,0)$ 0-element subsets, $C(n,1)$ 1-element subsets, and so on. These are disjoint, by the sum rule there are $C(n,0) + C(n,1) + \dots C(n,n)$ subsets.

Definition 3.6. 2 sets A and B have the **same cardinality** written $|A| = |B|$, if A, B are both empty or there's a bijective function $f : A \to B$.

Theorem 3.7. Let S be a non-empty collection of non-empty sets. Then a relation R is defined on S by $A\ R\ B$ if there is a bijective function $f : A \to B$ and R is an equivalence relation.

Proof. We show R is reflexive.
Let $a \in S$, then i_A is a bijective function mapping from A to A. Thus R is reflexive.
Let $a, b \in S$. Suppose $a\ R\ b$, then $\exists$ a bijective function $f : A \to B$, so f^{-1} is also bijective. Then $f^{-1}(b) = a$. Thus $b\ R\ a$.
Let $a, b, c \in S$. Suppose $a\ R\ b$ and $b\ R\ c$, then $\exists f$ s.t. $f(a) = b$, and $\exists g$ s.t. $g(b) = c$. Then the bijective function $(g \circ f)(a) = c$. Thus $a\ R\ b$.
$\therefore R$ is an equivalence relation. □

Definition 3.8. Set A is **denumerable** if $|A| = |\mathbb{N}|$.

Example. Let $E = \{2k \mid k \in \mathbb{Z}\}$.
Show that E is denumerable.
We must find a bijective function $f : \mathbb{N} \to E$. We define f by $f(n) = 2n$.
Suppose $f(n) = f(m)$ for some $n, m \in \mathbb{N}$. Then, $2m = 2n \implies m = n$.
Let $2k \in E$ for $k \in \mathbb{N}$. Then $f(k) = 2k$. Thus f is surjective.

Definition 3.9. A is **countable** if either A is finite or denumerable.

Definition 3.10. A **countably infinite set** is a denumerable set.

Definition 3.11. An **uncountable** set is a set that's not countable.

Proposition 3.12. There is a convenient method for showing a set is denumerable. Let A be a denumerable set. Then there is a bijective function $f : \mathbb{N} \to A$. We have

$$A = \{f(1), f(2), f(3), \dots\}$$

That is, we can enumerate the elements of A.

Conversely, suppose we can give an enumeration of all the elements of an infinite set A:

$$a_1, a_2, a_3, \ldots$$

where $a_i \neq a_j$ for $i \neq j$. Then $g : \mathbb{N} \to A$ defined by $g(n) = a_n$ is bijective, and so A is denumerable.
If we can list the elements of an infinite set, then it is denumerable.
Our listing must start with a first element and it must be clear every number is hit exactly once.

Example. For the proof above, we can list E as

$$2, 4, 6, 8, \ldots$$

Theorem 3.13. Every infinite subset of a denumerable set is denumerable.

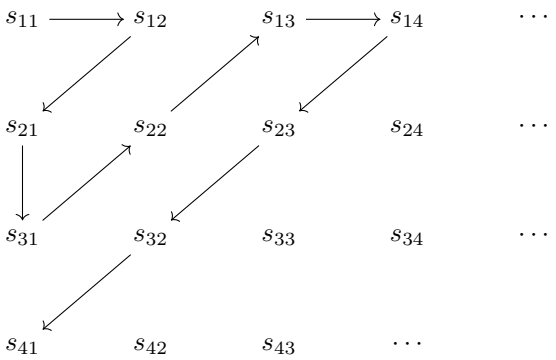
Example. $\mathbb{Z}$ is denumerable. We can list the elements:

$$0, 1, -1, 2, -2, \ldots$$

Proof. The basis idea is as follows. The denumerable set can be listed. The subset will contain infinitely many of the elements in this listing. We can list these remaining elements in the same order as the original list. Since we can give a listing of the elements in the infinite subset, it is denumerable. □

Example. For the proof above, note that $E \subseteq \mathbb{N}$.

Example. We show that the rationals are denumerable.



To list $\mathbb{Q}+$, traverse diagonal lines and skip encountered numbers, i.e.

$$1, 2, \frac{1}{2}, 3, \frac{1}{3}, 4, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, 5, \frac{1}{5}, \ldots$$

Then to show $\mathbb{Q}$ is denumerable, simply list again but add the negative versions after their counterpart.

3.1 Uncountable Sets

Theorem 3.14. Let $A = \{x \in \mathbb{R} \mid 0 < x < 1\}$. Then A is uncountable.

Proof. Suppose A is countable, then it must be denumerable as A is of infinite size. Then there exists a bijective function $f : \mathbb{N} \to A$. Let $f(n) = a_n$. Since $a_n \in A$, it has a decimal expansion. Let

$$a_n = 0.d_{n1}d_{n2}\ldots$$

We have

$$\begin{aligned} f(1) &= a_1 = 0.d_{11}d_{12}\ldots \\ f(2) &= a_2 = 0.d_{21}d_{22}\ldots \\ f(3) &= a_3 = 0.d_{31}d_{32}\ldots \\ &\vdots \end{aligned}$$

we produce an element of A that differs from each number in this list. We define $b = 0.b_1b_2b_3\ldots$ by

$$b_i = \begin{cases} 5 & \text{if } d_{ii} \neq 5 \\ 6 & \text{if } d_{ii} = 5 \end{cases}$$

For any $i \in \mathbb{N} b_i \neq d_{ii}$, so $b_n \neq a_n$ for any $n \in \mathbb{N}$. Thus $b \neq \text{range}(f)$ and so f is not surjective. However, f is bijective, so there is a contradiction. □

Theorem 3.15. Let A, B be sets with $A \subseteq B$. If A is uncountable, then B is uncountable.

Proof. Suppose $A \subseteq B$ with A being uncountable. Then A, B are of infinite size. Suppose B is countable. Then B must be denumerable. However, since A is a subset of a denumerable set, by Theorem it is also denumerable. This is a contradiction. □

Theorem 3.16. $\mathbb{R}$ is uncountable.

Proof. Let $A = \{x \in \mathbb{R} \mid 0 < x < 1\}$. $A \subseteq \mathbb{R}$ and since A is uncountable, then B is uncountable. □

Remark. If A is a non-empty set, then $\{0,1\}^A$ is the set of all functions $f : A \to \{0,1\}$. If A is finite, then $|\{0,1\}| = 2^{|A|}$. Also, $|\mathcal{P}(A) = 2^{|A|}$. Thus

$$|\{0,1\}| = |\mathcal{P}(A)|$$

Is this true when A is infinite?
Let $S \subseteq A$. How can we use S to define a function $f : A \to \{0,1\}$?
Suppose $S = \{a, b\}$. Then $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
All functions from A to $\{0,1\}$:

$$f_1 = \{(a,0),(b,0)\}$$
$$f_2 = \{(a,0),(b,1)\}$$
$$f_3 = \{(a,1),(b,0)\}$$
$$f_4 = \{(a,1),(b,1)\}$$

The idea is to send S to the function that maps elements of S to 1.
We construct a bijective function Ψ from $\mathcal{P}(\mathcal{A})$ to $\{0,1\}^A$. If $S \subseteq A$, we define $\Psi(S) = f_s$ where for any $a \in A$,

$$f_s(a) = \begin{cases} 1 & \text{if } a \in S \\ 0 & \text{if } a \notin S \end{cases}$$

We show f is injective. Suppose $\Psi(S) = \Psi(T)$ for $S, T \subseteq A$. Then $f_S = f_T \implies f_s(a) = f_T(a) \forall a \in A$. Thus $f_S(a) = 1 \Leftrightarrow f_T(a) = 1$. Thus $S = T$.
We show f is surjective. Let $f : A \to \{0,1\}$ and $S = \{a \in A \mid f(a) = 1\} = f^{-1}(\{1\})$, then $\Psi_S = f_s = f$ and so Ψ is surjective.

Theorem 3.17. Let A be a non-empty set. Then $|\mathcal{P}(A)| = |\{0,1\}^A|$

Definition 3.18. If there exists an injective function $f : A \to B$ then we write $|A| \leq |B|$. We say that A has **smaller cardinality** than B, written $|A| < |B|$, if there exists an injective function $f : A \to B$ but no bijective function $f : A \to B$.

Theorem 3.19. Let A be a set. Then $|A| < |\mathcal{P}(A)|$

Proof. If $A = \emptyset$, then $|A| = 0$ and $|\mathcal{P}(A)| = |\{\emptyset\}| = 1$.
Assume $A \neq \emptyset$. We define $f : A \to \mathcal{P}(A)$ by $f(a) = \{a\}$. Suppose $f(a) = f(b)$. Then $\{a\} = \{b\} \implies a = b$ and so f is injective. Thus $|A| \leq |\mathcal{P}(A)|$.

Now we show that there is no bijective function.
Suppose $g : A \to \mathcal{P}(A)$ is bijective. For each $x \in A$, let $g(x) = A_x$ where $A_x \subseteq A$.
We describe a set $B \in \mathcal{P}(A)$ (a subset of A) but not equal to any A_x. Let $B = \{x \in A \mid x \notin A_x\}$. Thus g is surjective, for some $y \in A$ we have $B = g(y) = A_y$.
Suppose $y \in A_y$, then $y \in B$. By definition of $B, y \notin A_y$. Contradiction.
Suppose $y \notin A_y$, then $y \notin B$. By definition of $B, y \in B$. Contradiction.
Thus there is no bijective function from A to $\mathcal{P}(A)$. □