MATH1061 Course Notes

Paddy Maher

September 23, 2021

1 Logic

1.1 Logical Connectives

1.1.1 Basic logical connectives

For a given logical statement come logical connectives. Basic logical connectives include:

- **not** $= \sim$
- **and** $= \wedge$
- **or** $= \vee$
- **exclusive or** $= \oplus$

1.1.2 Logical Equivalence

Given two statement forms, you can show that they are logically equivalent by using a truth table or by using the laws of logical equivalence.
The logical equivalence between two statements is demonstrated by the symbol $\equiv$

[insert truth table]

1.1.3 Conditional logical connectives

Logical connectives and equivalences, for given truth statements 'p' and 'q'

- **if .. then** $= \rightarrow$
- **if and only if** $= \leftrightarrow$
- $p \rightarrow q \equiv \sim p \vee q \equiv \sim q \rightarrow \sim p$

1.1.4 Order of Operations

1. $\sim$
2. $\wedge$ and $\vee$, use parentheses to specify. If no parentheses given, work from left to right.
3. $\rightarrow$ and $\leftrightarrow$, use parentheses to specify. If no parentheses given, work from left to right.

1.2 Necessary and sufficient conditions

For given truth statements 'p' and 'q':

- p is a necessary condition for q means "if $\sim p$ then $\sim q$" or equivalently "if q then p" or "q only if p".
- p is a sufficient condition for q means "if p then q" or equivalently "q if p"

1.3 Definitions

1.3.1 Tautology and contradictions

- A tautology is a statement form which always takes truth values "**true**" for all possible truth values of its variables.
- A contradiction is a statement form which always takes truth values "**false**" for all possible truth values of its variables.

1.3.2 Contrapositive

For given truth statements 'p' and 'q'
The contrapositive of $p \to q$ is $\sim q \to \sim p$

- These are logically equivalent:
  $p \to q \equiv \sim q \to \sim p$

1.3.3 Biconditional

For given truth statements 'p' and 'q'
The biconditional of p and q, denoted $p \leftrightarrow q$, is defined by the following truth table:

[insert truth table]

1.4 Arguments

1.4.1 Premises

Given a collection of statements '$p_1, p_2, ..., p_n$' (called **premises**) and another statement 'q' (called the conclusion), an '*argument*' is the assertion that the conjunction of the premisees implies the conclusion.

$$\begin{gathered} p_1 \\ p_2 \\ \ldots \\ p_n \\ \therefore q \end{gathered}$$

1.4.2 Arguments; validity and invalidity

Definition; valid argument An argument is **valid** if whenever all of the premises are true, the conclusion is also true.

Thus, an argument is valid if $(p_1 \wedge p_2 \wedge ... \wedge p_n \to q)$ is a tautology.

Definition; invalid argument An argument is **invalid** if it is possible to have a situation in which all of the premises are true but the conclusion is false.

We can check whether an argument is valid or invalid using a truth table.

1.4.3 Rules of Inference

Modus Ponens

$p \to q$
p
$\therefore q$

Modus Tollens

$p \to q$
$\sim q$
$\therefore \sim p$

Generalisation

p
$\therefore p \vee q$

q
$\therefore p \vee q$

Specialisation

$p \wedge q$
$\therefore p$

$p \wedge q$
$\therefore q$

Conjunction

p
q
$\therefore p \wedge q$

Elimination

$$\begin{array}{c} p \vee q \\ \sim q \\ \therefore p \end{array}$$

$$\begin{array}{c} p \vee q \\ \sim p \\ \therefore q \end{array}$$

Transitivity

$$\begin{array}{l} p \to q \\ q \to r \\ \therefore p \to r \end{array}$$

Proof by Division into cases

$$\begin{array}{l} p \vee q \\ p \to q \\ q \to r \\ \therefore r \end{array}$$

Contradiction Rule

$$\begin{array}{l} \sim p \to (contradiction) \\ \therefore p \end{array}$$

1.4.4 Alternative method for determining validity

If an argument is *'invalid'* then there is a situation where all the premises are true but the conclusion is false.

Attempt to see whether this is possible. To do this, look for truth values which make all premises true yet the conclusion is false.

If such truth values can be found, then the argument is *invalid*

Summary of this method:

- Try to make all the premises true and the conclusion false
- If this can be done, then the argument is invalid
- On the other hand, if this is **impossible** to do, then the argument is valid

Checks for Validity

- Use a truth table
- Use rules of inference
- Attempt to find turht values that make all premises true but the conclusion false.

1.4.5 Predicates and domains

A predicate is a sentence that contains finitely many variables, and which becomes a statement if the variables are given specific values.

The domain of each variable in a predicate is the set of all possible values that may be assigned to it.

The truth set of a predicate P(x) is the set of all values in the domain that, when assigned to x, make P(x) a true statement.

Common Domains

- Integers: $\mathbb{Z}$ = [..., -3, -2, -1, 0, 1, 2, 3, ..]
- Positive integers: $\mathbb{Z}^{+}$ = [1, 2, 3, ...]
- Non-negative integers: $\mathbb{Z}^{non-neg}$ = [0, 1, 2, 3, ...]
- Natural numbers: $\mathbb{N}$ = [1, 2, 3, ...]
- Rational numbers: $\mathbb{Q}$ = [$\frac{a}{b}$ | a, b $\in \mathbb{Z} \wedge$ b $\neq 0$]
- Real numbers: $\mathbb{R}$ = entire number line

1.5 Quantifiers

1.5.1 Universal and Existental quantifiers

The Universal quantifier

The symbol '$\forall$' denotes *"for all"* and is called the **universal quantifier**

Let Q(x) be a predicate and **D** be the domain of x. The **universal statement**

$\forall$ x $\in$ **D**, Q(x)

is true if and only if Q(x) is true for every x in **D**. It is false if and only if Q(x) is false for at least one x in **D**

The Existental Quantifier

The symbol '∃' denotes "there exists" and is called the **existential quantifier**

Let Q(x) be a predicate and **D** be the domain of x. The **existential statement**

∃ x ∈ **D** such that Q(x)

is true if and only if Q(x) is true for at least one x in **D**. It is false if and only if Q(x) is false for every x in **D**

1.5.2 Negation of Quantified Statements

Universal Statement:

∀ x ∈ **D**, Q(x)

The negation of this statement is logically equivalent to:

∃ x ∈ **D** such that ∼ Q(x)

Existential Statement:

∃ x ∈ **D** such that Q(x)

The negation of this statement is logically equivalent to:

∀ x ∈ **D**, ∼ Q(x)

Universal Conditional Statement

∀ x ∈ **D** if P(x) then Q(x)

The negation of this statment is logically equivalent to:

∃ x ∈ **D** such that ∼ if P(x) then Q(x)

which is;

∃ x ∈ **D** such that P(x) ∧ ∼Q(x)

1.6 Multiple quantifiers

1.6.1 Intro to multiple quantifers

The predicate x ≤ y for real numbers x and y involves more than one variable.

Notation such as P(x,y) is used to denote such predicates.

Such predicates often appear in statments that involve more than one quantifier

In order to establish the truth of a statment of the form:

∀ x ∈ **D**, ∃ y ∈ **D** such that P(x,y)

One must allow another to pick whatever element x ∈ **D** they wish, and then must preceed with finding an element y ∈ **E** which makes P(x,y) true.

In order to establish the truth of a statment of the form:

∃ x ∈ **D** such that ∀ y ∈ **D**, P(x,y)

One must find one particular x ∈ **D** which makes P(x,y) true no matter which y ∈ **D** might be chosen for you.

1.6.2 Negation of statements with multiple quantifers

The statement:
$\forall$ x $\in$ **D**, $\exists$ y $\in$ **E** such that P(x,y)
Negates to:
$\exists$ x $\in$ **D** such that $\sim$ ($\exists$ y $\in$ **E** such that P(x,y))
Which is:
$\exists$ x $\in$ **D** such that $\forall$ y $\in$ **E** $\sim$ P(x,y)

The statement:
$\exists$ x $\in$ **D** such that $\forall$ y $\in$ **E**, P(x,y)
Negates to:
$\forall$ x $\in$ **D**, $\sim$ ($\forall$ y $\in$ **E**, P(x,y))
Which is:
$\forall$ x $\in$ **D**, $\exists$ y $\in$ **E** such that $\sim$ P(x,y))

2 Proofs and Number Theory

2.1 Proofs

2.1.1 Even and Odd

An integer 'n' is <u>even</u> if and only if 'n' is twice some integer.

- That is: n is even $\leftrightarrow \exists k \in \mathbb{Z}$ such that n = 2k

An integer 'n' is <u>odd</u> if and only if 'n' is twice some integer.

- That is: n is odd $\leftrightarrow \exists k \in \mathbb{Z}$ such that n = 2k + 1

2.1.2 Prime and Composite

An integer 'n' is <u>prime</u> if and only if n > 1 and for all positive integers 'r' and 's', if n = rs, then r = 1 or s = 1.

An integer 'n' is <u>composite</u> if and only if n > 1 and n = rs for some positive integers 'r' and 's' with r $\neq$ 1 and s $\neq$ 1

<u>In symbols:</u>

- n is prime $\leftrightarrow$ n > 1 $\wedge\forall$ r,s $\in \mathbb{Z}^+$, n = rs $\rightarrow$ (r=1 $\wedge$ s=1)
- n is composite $\leftrightarrow$ n > 1 $\wedge\exists$ r, s $\in \mathbb{Z}^+$ such that n = rs $\wedge$ r $\neq$ 1 $\wedge$ s $\neq$ 1
- Note: 1 is neither prime nor composite.

2.1.3 Direct proofs

Proving Existental Statements

To show ∃ x ∈ **D** such that P(x) is true, it is enough to find one example of an element x in **D** for which P(x) is true.

Direct Proof of Universal Statements

One way to show that ∀ x ∈ **D**, P(x) is true is by a direct proof.

1. Suppose x ∈ **D**
2. Show that P(x) is true

Method of direct proof to show that ∀ x ∈ **D** if P(x) then Q(x) is true:

1. Suppose x ∈ **D** and P(x) is true
2. Show that the conclusion Q(x) is true using definitions, previously established results, and the rules for logical inference.

How to write a proof

- Write the theorem to be proved
- Clearly mark the beginning of the proof with the word *"Proof"*
- Use precise definitions for any mathematical terms
- Write the proof in complete sentences
- Give a reason for each assertion in your proof
- Make your proof self-contained
- Display equations and inequalities clearly
- Conclude by stating what it is you have proved

2.1.4 Other forms of proof

Disproof by Counterexample To show that ∀ x ∈ **D** if P(x) then Q(x) is false, find a value of x ∈ **D** for which P(x) is true and Q(x) is false.

Method of Proof by Contradiction

1. Assume that the statement is false
2. Show that this leads logically to a contradiction
    - So it is impossible that the statement is false

3. Conclude that the statement is true

Method of Proof by Contradiction to show that $\forall$ x $\in$ **D**, if P(x) then Q(x) is true:

1. Assume that the statement to be proved is false. Thus, the *negation* of the statement is true: $\exists$ x $\in$ **D** such that P(x) and $\sim$ Q(x)
2. Show that this assumption leads logically to a contradiction
3. Conclude that the statement to be proved is true.

Method of Proof by Contraposition

1. Express the statement to be proved in the form: $\forall$ x $\in$ **D**, if P(x) then Q(x)
2. Rewrite this statement in the contrapositive form: $\forall$ x $\in$ **D**, if $\sim$ Q(x) the $\sim$ P(x)
3. Prove the contrapositive by direct proof:
   - Suppose x $\in$ **D** and Q(x) is false
   - Show that P(x) is false

2.2 Types of numbers

2.2.1 Rational numbers

A real number is rational if and only if it can be expressed as a quotient of two integers with a non-zero denominator.

The set of all rational numbers is denoted by $\mathbb{Q}$

A real number that is not rational is irrational

r is rational $\leftrightarrow \exists$ a, b $\in \mathbb{Z}$ such that r $= \frac{a}{b}$ and b $\neq 0$

Fact: The decimal expansion of a rational number either repeats or terminates

Fact: The decimal expansion of an irrational number does not repeat and does not terminate

Theorem: For all rational numbers r and s where r $<$ s, there exists another rational number q such that r $<$ q $<$ s

2.2.2 Divisibility

If n,d $\in \mathbb{Z}$, d $\neq 0$, then n is divisible by d if and only if there exists some k $\in \mathbb{Z}$ such that n = kd

Alternatively, we say

- n is a multiple of d
- d is a factor of n

- d is a divisor of n
- d divides n

The notation d|n is used to represent the predicate "d divides n"
If n is not divisible by d, we write d∤n
Theorem: Every integer n>1 can be written as a product of primes.
Proof: Suppose the theorem is false. Then there exists an integer n>1 that is not a product of primes.
Choose the smallest number *n*. Either n is prime or n is composite

- If n is prime; then n is trivially a product of primes
- If n is composite: then n = rs for some positive integers r and s, where r ≠ 1 and s ≠ 1. This implies that 1 < r < n and 1 < s < n

Because we chose n to be the smallest integer greater than 1 that is not a product of primes, both r and s (which are smaller than n) must be products of primes.
Therefore, n = rs is a product of primes also.
So, regardless of whether n is prime or composite, we find that n is a product of primes.
This contradicts our choice of n
Therefore, every integer n > 1 can be written as a product of primes.

2.2.3 Prime Factorisation

Given any integer n > 1, there exists

- A positive integer k
- Distinct primes p_1. p_2, ..., p_k
- Distinct primes e_1. e_2, ..., e_k such that
n = $(p_1)^{(e_1)}(p_2)^{(e_2)}(p_3)^{(e_3)}...(p_k)^{(e_k)}$

and any other expression of n as a product of primes is identical to this, except perhaps for the order in which the terms are written

2.2.4 Floor and Ceiling

Given any x ∈ ℝ, the floor of x, denoted ⌊x⌋, is the unique integer n such that n ≤ x < n+1

Given any x ∈ ℝ, the ceilling of x, denoted ⌈x⌉, is the unique integer n such that n - 1 < x ≤ n+1

2.2.5 The quotient-remainder theorem

Given any integer n and a postiive integer d , there exists <u>unique</u> integers q and r such that

- n = dq + r and Q ≤ r < d

For integers *a* and *b*, and a positive integer *d*, we say a is <u>congruent</u> to b modulo d and write

- a ≡ b (mod d)

if and only if d | (a,b)

If a and b are not congruent modulo d, we write a /≡ b (mod d) [don't know how to represent this]

<u>Facts:</u>

- If n = dq + r, then n ≡ r (mod d)
- n ≡ 0 (mod d) if and only if d|n

2.3 Greatest common divisor

For integers *a,b* ∈ ℤ, not both zero, the <u>greatest common divisor</u> of a and b, denoted gcd(a,b), is the integer *d* which satisfies the following two properties:

- d | a and d | b
- for all c ∈ ℤ, if c | a and c | b then c ≤ d

Thus, d is the largest integer for which d | a and d | b

If gcd(a,b) = 1, then a and b have no common factors other than ±1 and we call a and b coprime or relatively prime

What happens if a = b = 0?

For every d ∈ ℤ, d satisfies d | 0 (d ≠ 0) since 0 = d.0. Thus, there is no greatest common divisor since there is no greatest integer.

However, if b > 0, what is gcd(0,b)?

- d | 0 for all d ∈ ℤ (d ≠ 0)
- the greatest divisor of b is b

Thus, the greatest <u>common</u> divisor is 1

<u>Fact:</u> If b > 0 then gcd(0,b) = b

<u>Fact:</u> If *a* and *b* are integers with b ≠ 0 and if *q* and *r* are integers such that:

$$a = bq + r \tag{1}$$

then gcd(a,b) = gcd(b,r)

<u>Why?</u>

- If d | a and d | b, then d | bq so d | (a - bq). Thus d | r
- If d | r and d | b, then d | bq so d | (bq+ r). Thus d | a

So the common divisors of a and b are the same as the common divisors of b and r.

2.3.1 The Euclidean Algorithm

To find gcd(a,b) where a,b $\in \mathbb{Z}$ and a $\geq$ b > 0:

- Write a = bq + r, as in the quotient-remainder theorem
- If r=0, then terminate gcd(a,b) = b
- Otherwiste, replace (a,b) by (b,r) and repeat

Example: Find gcd(192, 132)

$$a = 192, b = 132, 192 = 132.1 + 60, gcd(192, 132) = gcd(132, 60) \quad (2)$$

$$a = 132, b = 60, 132 = 60.2 + 12, gcd(132, 60) = gcd(60, 12) \quad (3)$$

$$a = 60, b = 12, 60 = 12.5 + 0, gcd(60, 12) = gcd(12, 0) \quad (4)$$

$$Therefore, gcd(192, 132) = 12 \quad (5)$$

Could this process repeat forever? No. By the quotient-remainder theorem; 0 $\leq$ r < b. Since we use the old value of r as the new value of b when we repeat, this means that r becomes strictly smaller on each repetition.

Therefore, we must eventually reach r=0 and terminate.

2.3.2 Lowest common multiple

For nonzero itnegers a,b $\in \mathbb{Z}$, the lowest common multiple of a and b is the smallest postive integer n for which a | n and b | n. We write this as lcm(a,b)

Fact: Suppose a,b $\in \mathbb{Z}$ where a $\leq$ b > 0. Then gcd(a,b).lcm(a,b) = ab

2.4 Sequences

A sequence is an ordered list of elements. It can be finite or infinite.

Each individual element in a sequence is called a term. We often denote the terms of sequences by lower case letters with subscripts.

Note: The subscript of the initial term in a sequence does not need to be 1.

An explicit formula or general formula for a sequence is a rule showing how the value of a general term a_k depends on k.

Different notations are used to denote such a sequence, such as:

- $(2^k)_{k \leq 0}$

- $(2^k)_{k\leq 0}^{\infty}$

ut how to do this brace equivalents

An alternating sequence is a sequence in which the terms alternative between positive and negative

Example: find a general formula for a sequence that has the following initial terms:

$$2, \frac{3}{4}, \frac{4}{9}, \frac{5}{16}, \frac{6}{25}, \frac{7}{36}, ... \tag{6}$$

Let a_n denote the general term and suppose the initial term is a_1.

Observe that the denominator in each term is a perfect and thus we can rewrite the given terms as:

$$\frac{1+1}{1^2}, \frac{2+1}{2^2}, \frac{3+1}{3^2}, \frac{4+1}{4^2}, \frac{5+1}{5^2}, \frac{6+1}{6^2}, ... \tag{7}$$

$a_n = \frac{n+1}{n^2}$

The sequence $(\frac{n+1}{n^2})$ has the given initial terms.

2.4.1 Notation

Summation Notation

We use a Greek capital letter Σ to indicate a sum.

If m, n $\in \mathbb{Z}$ and m $\leq$ n then

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + ... + a_n \tag{8}$$

m is the lower limit of the summation n is the upper limit of the summation

If m=n then the sum only has one term

Dummy Variables The variable i in $\sum_{i=m}^{n} a_i$ is a *dummy variable*
One can use any letter here *(as long as it is not already taken)*

Example:

$$\sum_{i=2}^{n} a_i = a_2 + a_3 + ... + a_n = \sum_{k=2}^{n} a_k = \sum_{j=2}^{n} a_j \tag{9}$$

The dummy variable is only relevant inside the su, which means you can reuse it outside the sum.

You can also perform a *change of variables*

Example:

$$\sum_{i=2}^{6}(i-1)^2 = 1^2+2^2+3^2+4^2+5^2 \tag{10}$$

$$Let k = i-1 \tag{11}$$

$$When i = 2, k = 1 \tag{12}$$

$$When i = 6, k = 5 \tag{13}$$

$$\sum_{k=1}^{6} k^2 = 1^2+2^2+3^2+4^2+5^2 \tag{14}$$

$$\tag{15}$$

Product Notation We use a Greek capital letter Π *(pi)* to indicate a product.

If m,n $\in \mathbb{Z}$ and m $\leq$ n then

$$\prod_{i=m}^{n} a_i = a_m.a_{m+1}.....a_n \tag{16}$$

If m=n then the product only has one term

2.4.2 Factorials

For each positive integer n, we define n! *(read n factorial)* to be

$$n! = n(n-1)(n-2)...3.2.1 = \prod_{i=1}^{n} i \tag{17}$$

Also, we define 0! = 1
So,

$$0! = 1 \tag{18}$$

$$1! = 1 \tag{19}$$

$$2! = 2.1 = 2 \tag{20}$$

$$3! = 3.2.1 = 6 \tag{21}$$

$$4! = 4.3.2.1 = 24 \tag{22}$$

2.4.3 Properties of Summation and Product

If a_m, a_{m+1}, ... and b_m, b_{m+1}, ... are sequences of real numbers, and c is any real number, then for any integer n ≥ m, the following hold:

1. $\sum_{i=m}^{n} a_i \pm \sum_{i=m}^{n} b_i = \sum_{i=m}^{n}(a_i \pm b_i)$
   (adding/subtracting over the same range)
2. $\sum_{i=m}^{n} ca_i = c\sum_{i=m}^{n} a_i$
   (taking out a common factor)
3. $(\prod_{i=m}^{n} a_i)(\prod_{i=m}^{n} b_i) = \prod_{i=m}^{n} a_i.b_i$

Suppose P(n) is a predicate and we know:

- P(1)
- P(1) → P(2)
- P(2) → P(3)
- P(3) → P(4)

Can we conclude that P(4) is true? Yes. By repeated use of modus ponens.

2.5 Mathematical Induction

2.5.1 The principle of mathematical induction

Let P(n) be a predicat that is defined for every integer n ≥ a, where a is some fixed integer.

Suppose

1. P(a) is true
2. For every integer k ≥ a, P(k) → P(k+1)

How to use the principle of mathematical induction:

To prove that: For every integer n ≥ a, P(a).

1. Basis Step: Prove P(a)
2. Inductive Step: Prove that: For every integer k ≥ a, P(k) → P(k+1)
   - Suppose k is an integer, where k ≥ a, and P(k) is true. *(this is called the* ***Inductive Hypothesis***
   - Using this, show that P(k+1) is true

2.5.2 The principle of strong mathematical induction

Let P(n) be a predicate that is defined for every integer n ≥ a, where a is some fixed integer, and let b be an integer where b ≥ a

Suppose

1. Basis Step: P(a), P(a+1), ..., P(b) are all true
2. Inductive Step: For every integer k ≥ b, if P(a), P(a+1), ..., P(k) are all true, then P(k+1) is true

Then P(n) is true for every integer n ≥ a

It can be shown that this is **equivalent** to the ordinary principle of mathematical induction

Example: Prove that For every integer n ≥ 8, we can form n cent postage using 3 cent and/or 5 cent stamps

Before starting a proof, observe that:

$$\begin{aligned} 8 = 5 + 3 \rightarrow 11 = 5 + 3 + 3 \qquad (23) \\ 9 = 3 + 3 + 3 \rightarrow 12 = 3 + 3 + 3 + 3 \qquad (24) \\ 10 = 5 + 5 \rightarrow 13 = 5 + 5 + 3 \qquad (25) \\ \qquad (26) \end{aligned}$$

We now use this idea in a formal proof.

Proof: Let P(n) be the predicate ”n cent postage can be formed using only 3 cent and/or 5 cent stamps”

Basis Step: We can prove P(8), P(9) and P(10) directly, since:

$$\begin{aligned} 8 = 5 + 3 \qquad (27) \\ 9 = 3 + 3 + 3 \qquad (28) \\ 10 = 5 + 5 \qquad (29) \end{aligned}$$

Inductive Hypothesis: Suppose that for some integer k ≥ 10, P(8), ..., P(k) are all true. We will use this to prove P(k+1)

Since k ≥ 10, we have k-2 ≥ 8. Thus, by the Inductive Hypothesis, we can form (k-2) cents using 3 cent and/or 5 cent stamps.

Now we can add one more 3 cent stamp to make (k+1) postage and so P(k+1) is true.

Therefore, by strong induction, it follows that P(n) is true for every integer n ≥ 8

2.5.3 The Well-Ordering principle for the integers:

If S is a non-empty set of integers all of which are greater than some fixed integer, then S has a least element

It can be shown that the well-ordering principle is equivalent to the principle of mathematical induction, or even strong mathematical induction. All three are equivalent.

For each of the following sets, do they have a least element?

- The set of all integers greater than 2? Yes
- The set of all natural numbers $\mathbb{N}$? Yes
- The set of all odd integers? No
- The set of all primes? Yes
- The set of positive real numbers? No

2.5.4 Recurrence

A recurrence relation for a sequence $a_0, a_1, a_2, ...$ is a formula that relates each term a_k to some of its predecessors $a_{k-1}, ..., a_{k-i}$ where i $\in \mathbb{Z}$ and k - i $\geq$ 0

The initial conditions for such a recurrence relation specify the values of some of the initial terms

Example: The fibonacci sequence is defined recursively by

$$F_0 = 1, F_1 = 1 (initial conditions) and F_n = F_{n-1} + F_{n-2} (recurrence relation) for n \geq 2 \tag{30}$$

2.5.5 Forms of defining a sequence

Ways to define sequences

A sequence can be defined

- Informally, by listing the first few terms of the sequence until the pattern becomes obvious
  - Ex: 1, 1, 2, 6, 24, 120, 720, ...
- With a general formula, by stating how a term a_n depends on n and stating where it starts
  - Ex: $(n!)_{n \geq 0}$
- Recursively, by giving a recurrence relation relating later terms in the sequence to earlier ones and also some initial conditions
  - Ex: a_0 = 1, a_n = n.a_{n-1} For n $\geq$ 1

Example: Let c_0, c_1, c_2, ... be a sequence defined by

$$c_0 = 1, c_1 = 2, c_2 = 3 \tag{31}$$
$$c_n = 3c_{n-1} - c_{n-2} - c_{n-3} for n \geq 3 \tag{32}$$

Write out the first 6 terms for the sequence

$$c_0 = 1 \tag{33}$$
$$c_1 = 2 \tag{34}$$
$$c_2 = 3 \tag{35}$$
$$c_3 = 3c_2 - c_1 - c_0 = 3.3 - 2 - 1 = 6 \tag{36}$$
$$c_4 = 3c_3 - c_2 - c_1 = 3.6 - 3 - 2 = 13 \tag{37}$$
$$c_5 = 3c_4 - c_3 - c_2 = 3.13 - 6 - 3 = 30 \tag{38}$$
$$\tag{39}$$

Example: Show that the sequence $a_k = 3 - 2^k$, for k $\geq$ 0, satisfies the recurrence relation $a_n = 2a_{n-1}$ for n $\geq$ 1

The sequence is $(3.2^k)_{k \geq 0}$ = 3, 6, 12, 24, 48, ...
For every integer n $\geq$ 1 we have $a_n = 3 - 2^n$ and $a_{n-1} = 3 - 2^{n-1}$
Hence

$$a_n = 3 - 2^n \tag{40}$$
$$= 3.2.2^{n-1} \tag{41}$$
$$= 2.(3.2^{n-1}) \tag{42}$$
$$= 2.a_{n-1} \tag{43}$$

Therefore, the sequence $(3.2^k)_{k \geq 0}$ satisfies the recurrence relation $a_n = 2a_{n-1}$ for n $\geq$ 1

We have seen that sequences of numbers can be defined recursively. Many other objects can be defined recursively as well, such as: sets, sums, products and functions ...
A recursive definition for a set of objects requires three things:

1. **BASE:** A statement that a certain object belongs in a set
2. **RECURSION:** A collection of rules showing how to form new objects for the set from existing ones in the set
3. **RESTRICTION:** A statement that no objects belong to the set other than those arising from steps **1** and **2**

Given a sequence that is defined recursively, one may wish to find an explicit formula for the sequence

Method of Iteration

1. Use iteration to write down several terms of the sequence and **guess** an explicit formula
2. Use induction to prove that the guess is correct

Example: Find an explicit formula for the sequence defined by

$$\begin{align} b_0 &= 2 \tag{44} \\ b_n &= b_{n-1} + 5 for n \geq 1 \tag{45} \end{align}$$

We have $b_0 = 2$

$$\begin{align} b_1 &= b_0 + 5 = 2 + 5 = 7 \tag{46} \\ b_2 &= b_1 + 5 = 7 + 5 = 12 \tag{47} \\ b_3 &= b_2 + 5 = 12 + 5 = 17 \tag{48} \\ b_4 &= b_3 + 5 = 17 + 5 = 22 \tag{49} \\ & \tag{50} \end{align}$$

Each term is 5 more than the previous term. Note that repeated addition can be written as multiplication

Guess: b_n = 5n + 2 for n $\geq$ 0

Next, we prove that for n $\geq$ 0, b_n = 5n + 2

Proof

Basis Step: When n = 0 $\rightarrow$ b_0 = 2 and 5(0) + 2

Inductive Hypothesis: Suppose from some integer k $\geq$ 0, b_k = 5k + 2

Now b_{k+1} = b_k + 5 by definition (since k + 1 $\geq$ 1)
= 5k + 2 + 5 by the Inductive Hypothesis
= 5(k+1) + 2

Therefore, by the principle of mathematical induction, for every integer n $\geq$ 0, b_n = 5n + 2

2.5.6 Arthimetic Sequences

A sequence a_0, a_1, a_2, ... is an arthimetic sequence if and only if there is a constant d such that a_k - a_{k-1} + d for every k $\geq$ 1

It follows that an explicit for the sequence is

$$a_n = a_0 + dn \tag{51}$$

for every integer n $\geq$ 0

2.5.7 Geometric Sequences

A sequence a_0, a_1, a_2, ... is a geometric sequence if and only if there is a constant r such that a_k = ra_{k-1} for every integer k $\geq$ 1

It follows that an explicit formula for the sequence is $a_n = a_0.r^n$ for every n $\geq$ 0

Note: It is not always possible to guess an explicit formula, and, in fact, some recursively defined sequences do not have an explicit formula

Example: $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for n $\geq$ 2

The explicit formula is

$$F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{n+1} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{n+1} \tag{52}$$

3 Set theory

A set S is a collection of objects, which are called the elements of S

If x is in S, one writes x $\in$ S

If not, one writes x $\notin$ S

We can sometimes list the elements of S with curly braces: S = $\{x_1, x_2, ...\}$

Example: S = {2, 3, 4}

2 $\in$ S but 1 $\notin$ S and $\pi \notin$ S

Example: Let E be the set of positive even integers, so E = {2, 4, 6, 8, ...}, which is an infinite set. 20 $\in$ E but 21 $\notin$ E and -4 $\notin$ E

Order does not matter. {2, 3, 5, 8} = {3, 8, 5, 2}

Repetitions are ignored {1, 3, 4} = {1, 1, 3, 4}
= {4, 3, 1, 3, 4, 1, 1}

One can define a set by a property that its elements must satisfy:

$$A = \{x \in S | P(x)\} \tag{53}$$

means that the elements of A are precisely those elements of S for which the predicate P(x) is true.

Example: The set of all even integer is

$$\{n \in \mathbb{Z}|n = 2kforsomek \in \mathbb{Z}\} \tag{54}$$

Example:

$$\{x \in \mathbb{Z}|3 < x < 7\} = \{4, 5, 6\} \tag{55}$$

The elements of a set can be sets themselves
Example:

$$A = \{1, 2, \{3\}, \{5, 6\}\} \tag{56}$$

Here 2 ∈ A and {3} ∈ A
but {2} ∉ A and 5 ∉ A

3.1 Subsets

If A and B are sets, A is called a subset of B, written A ⊆ B, if and only if every element of A is also an element of B

A ⊆ B ↔ ∀ x, x ∈ A → x ∈ B

Example: x = {1, 2, 3, 4}, y = {1, 3, 4}, z = {1, 2}

We have y ⊆ x and z ⊆ x but z ⊈ y

Note: Every set is a subset of itself. So if S is any set, we have S ⊆ S.

For sets A and B, A is a proper subset of B, denoted A ⊂ B, if and only if A ⊆ B and A ≠ B

Venn diagrams are a convenient way of visualising the relationships between different sets.

Two sets are **equal** if they contain the same elements.

$$A = B \leftrightarrow \forall x, x \in A \leftrightarrow x \in B \tag{57}$$

$$\leftrightarrow A \subseteq BandB \subseteq A \tag{58}$$

The empty set is the set containing no elements and is denoted by ∅
∅ = {}

Note: The empty set is a subset of every set. So if S is any set, we have $\emptyset \subseteq$ S

For a finite set A, the cardinality of A is the number of elements in the set A, which is denoted by |A|

Example: |{1, 2, 7, 13}| = 4
$|\emptyset| = 0$

3.1.1 Russel's Paradox

S = {A| A is a set and A $\notin$ A}

Is S $\in$ S?

- If S $\in$ S, then *(by definition)* S $\notin$ S, which is a contradiction
- If S $\notin$ S, then *(by definition)* S = S, which is a contradiction

To avoid problems such as Russel's Paradox, one can attempt to define all sets recursively:

Base: $\emptyset$ is a set
Recursion: We define several operations that build new sets from old sets

3.1.2 Operations on sets

Let A and B be any sets

- The union of sets A and B, denoted A $\cup$ B, is the set of all elements x such that x $\in$ A or x $\in$ B *(or both)*. A $\cup$ B = {x| x $\in$ A or x $\in$ B}
- The intersection of sets A and B, denoted A $\cap$ B, is the set of all elements x usch that x $\in$ A and x $\in$ B. A $\cap$ B = {x| x $\in$ A and x $\in$ B}
- The set difference of B minus A, denoted B - A, is the set of all elements x such taht x $\in$ B and x $\notin$ A. B - A = {x| x $\in$ A and x $\notin$ B}
- If the sets one is consdering are all subsets of some set U, called the universal set, the U - A is called the complement of A and is denoted A', or sometimes $\bar{A}$. A' = {x$\in$ U | x $\notin$ A}

Given sets A_0, A_1, A_2, ... and an integer n $\geq$ 0,

$$\begin{align}
\cup_{i=0}^{n} A_i &= \{x|x \in A_i foratleastonei = 0, 1, ..., n\} \tag{59}\\
\cup_{i=0}^{\infty} A_i &= \{x|x \in A_i foratleastoneintegeri \geq 0\} \tag{60}\\
\cap_{i=0}^{n} A_i &= \{x|x \in A_i foralli = 0, 1, ..., n\} \tag{61}\\
\cap_{i=0}^{\infty} A_i &= \{x|x \in A_i foreveryintegeri \geq 0\} \tag{62}\\
& \tag{63}
\end{align}$$

Definition: For any set S, the power set of S, denoted by P(S), is the set of all subsets of S

$$P(S) = \{x|x \leq S\} \tag{64}$$

Example: S = {1,3}
P(S) = {∅, {1}, {3}, {1,3}}

Note: For any set S, ∅ ∈ P(S) and S ∈ P(S)

Fact: If |S| = n, then the |P(S)| = 2^n

Definition: Two sets A and B are disjoint if and only if A ∩ B = ∅

Definition: Sets A_1, A_2, A_3, ... are mutually disjoint (or pairwise disjoint or nonoverlapping) if and only if $A_i \cap A_j = \emptyset$ whenever i ≠ j

Definition: A finite or infinite collection of nonempty sets {A_1, A_2, A_3, ...} is a partition of a set A if and only if A is the union of all A_i and A_1, A_2, A_3, .. are mutually disjoint.

Example: A partition of S = {2, 3, 5, 7, 17} is given by {{2}, {3,5}, {7,17}}

Example: Consider ℤ and division by 3. Thus, by the quotient remainder theorem every integer n can be written uniquely as n = 3q + r, where 0 < r < 3

$$A_0 = \{n \in \mathbb{Z}|n \equiv 0(mod3)\} \tag{65}$$
$$A_1 = \{n \in \mathbb{Z}|n \equiv 1(mod3)\} \tag{66}$$
$$A_2 = \{n \in \mathbb{Z}|n \equiv 2(mod3)\} \tag{67}$$
$$\tag{68}$$

{A_0, A_1, A_2} is a partition of ℤ

Definition: Let n ∈ $\mathbb{Z}^+$ and let x_1, x_2, ..., x_n, be n not necessarily distinct elements. The ordered n-tuple, denoted (x_1, x_2, ..., x_n), consists of the n elements with their ordering:

First x_1, then x_2, and so on up to x_n.

When n = 2, we call (x_1, x_2) an ordered pair

When n = 3, we call (x_1, x_2, x_3) an ordered triple

$(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n) \rightarrow x_i = y_i$ for all i with 1 ≥ i ≥ n

Example: (1, 2, 3) ≠ (1, 2, 4)
(1,3) ≠ (3,1)

Definition: The Cartesian product of sets A and B, denoted AxB is:

- AxB = {(a,b) | a ∈ A, b ∈ B }

Example: If A = {a,b} and B = {2,3} then

- AxB = {(a,2), (a,3), (b,2), (b,3)}

Example: The familar x-y plane is

- ℝxℝ = {(x,y)| x,y ∈ ℝ}

In general, A_1 x A_2 x ... A_n = {(a_1,a_2, ...,a_n | $a_i \in A_i$, 1 ≥ i ≥ n }

3.2 Intervals:

Given a,b ∈ ℝ with a ≥ b,

- (a,b) = { x ∈ ℝ| a < x < b } open interval
- .[a,b] = { x ∈ ℝ| a ≤ x ≤ b } closed interval
- (a,b] = { x ∈ ℝ| a < x ≤ b }
- .[a,b) = { x ∈ ℝ| a < x ≤ b }

The symbols ∞ and -∞ are used to indicate intervals that are unbounded either on the left or on the right.

- (a,∞) = { x ∈ ℝ| x > a }
- .[a,∞) = { x ∈ ℝ| x ≥ a }
- (∞,b) = { x ∈ ℝ| x < b }
- (-∞,b] = { x ∈ ℝ| x ≤ b }

Method to prove A ⊆ B

1. Suppose x ∈ A
2. Show that x ∈ B

Example:

Let A = { n $\in \mathbb{Z}$, n = 4k + 2 for some k $\in \mathbb{Z}$ } and E = { n $\in \mathbb{Z}$, n = 2m for some m $\in \mathbb{Z}$ }

Prove that A $\subseteq$ E.

Proof:

Suppose n $\in$ A. THen n = 4k + 2 for some k $\in \mathbb{Z}$

Hence n = 2(2k+1), and 2k + 1 $\in \mathbb{Z}$

Thus n is one of the form 2m for some m $\in \mathbb{Z}$, so n $\in$ E, therefore A $\subseteq$ E

Note: 4 $\in$ E but 4 $\notin$ A, so A $\subset$ E

Theorem:

For all sets A, B and C, if A $\subseteq$ B and B $\subseteq$ C, then A $\subseteq$ C *(Transitive Property of Subsets)*

Proof:

Suppose A, B and C, are sets and A $\subseteq$ B and B $\subseteq$ C.

Suppose x $\in$ A. Then, since A $\subseteq$ B, we have x $\in$ B. Hence, since B $\subseteq$ C, we have x $\in$ C.

Therefore, A $\subseteq$ C

Theorem:

For all sets A and B,

A $\cap$ B $\subseteq$ A and A $\cap$ B $\subseteq$ B *(Inclusion of Intersection)*

A $\subseteq$ A $\cup$ B and B $\subseteq$ A $\cup$ B *(Inclusion in Union)*

Method to Prove A = B

1. Prove A $\subseteq$ B *(Suppose $x \in A$ and then show $x \in B$)*
2. Prove B $\subseteq$ A *(Suppose $x \in B$ and then show $x \in A$)*

Example:

Let A = { x $\in \mathbb{Z}$| x $\equiv$ 1 (mod 6) } and B = { x $\in \mathbb{Z}$| x $\equiv$ 1 (mod 2) and x $\equiv$ (mod 3) }

Prove that A = B

Proof:

- First, prove that A ⊆ B:
  Let x ∈ A. Then x ∈ ℤ and x = 6k + 1 for some k ∈ ℤ

  Hence x = 2(3k) + 1 so x ≡ 1 *(mod 2)*

  Also x = 3(2k) + 1 so x ≡ 1 *(mod 3)*

  Thus x ∈ B, ∴ A ⊆ B
- Next, prove that B ⊆ A:
  Let x ∈ B. Then x ∈ ℤ and x = 2k + 1 for some k ∈ ℤ and x = 3l + 1 for some l ∈ ℤ. Either l is even or l is odd. If l is odd, then x = 3l + 1 is even, which contradicts the fact that x = 2k + 1. Hence l is even.

  Now l = 2m for some m ∈ ℤ and so x = 3(2m) + 1 = 6m + 1. Thus x ∈ A. ∴ B ⊆ A.
- ∴ A = B

Let A and B be any subsets of the universal set U. Prove that (A∩B)' = A' ∪ B'.

Proof:

Let x ∈ U.

$$x \in (A \cap B)' \leftrightarrow x \notin A \cap B \tag{69}$$
$$\leftrightarrow \sim (x \in A \cap B) \tag{70}$$
$$\leftrightarrow \sim (x \in A \wedge x \in B) \tag{71}$$
$$\leftrightarrow \sim (x \in A) \vee \sim (x \in B) \tag{72}$$
$$\leftrightarrow x \in A' \wedge x \in B' \tag{73}$$
$$\leftrightarrow x \in A' \cup B' \tag{74}$$

∴ (A ∩ B)' = A' ∪ B'

3.3 Set Identities

Let A, B and C be any sets

Commutative Laws
A ∪ B = B ∪ A

$A \cap B = B \cap A$

Associative Laws

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

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

Distributive Laws

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

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

Absorption Laws

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

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

Idempotent Laws

$A \cup A = A$

$A \cap A = A$

3.3.1 More Set Identities

Let A and B be subsets of a universal set U.

De Morgan's Laws

$(A \cup B)' - A' \cap B'$

$(A \cap B)' - A' \cup B'$

Set Difference Law

$A - B = A \cap B'$

Double Complement Law

$(A')' = A$

Complements of U and ϕ

$U' = \phi$

$\phi' = U$

Complement Laws

$A \cup A' = U$

$A \cap A' = \phi$

Identity Laws

$A \cup \phi = A$

$A \cap U = A$

Universal Bound Laws

A ∪ U = U

A ∩ ϕ = ϕ

3.3.2 Lemma for sets

Lemma

For any sets A, B and C that are subsets of a universal set U,

$$(A \cup B) - C = (A - C) \cup (B - C) \tag{75}$$

Proof:

Let A, B and C be any subsets of U. Then,

$$\begin{aligned} (A \cup B) - C &= (A \cup B) \cap C' && (76)\\ &= C' \cap (A \cup B) && (77)\\ &= (C' \cap A) \cup (C' \cap B) && (78)\\ &= (A \cap C') \cup (B \cap C') && (79)\\ &= (A - C) \cup (B - C) && (80) \end{aligned}$$

3.4 Functions

Definition:

A function f from a set X to a set Y, denoted f : X ⟶ Y is a subset of the Cartesian product X x Y such that for every element x ∈ X, there exists a unique element y ∈ Y for which (x,y) ∈ f.

We call X the **domain** of f and Y the **co-domain** of f.

If f: X ⟶ Y is a function and (x,y) ∈ f

- write f(x) = y
- write f: x ⟼ y
- call f(x) the value of f at x
- call f(x) the image of x under f

Note:

f denotes a function, f(x) denotes an element of Y

Note:

Distinct elements of the domain may share the same image

Image and Range

Given a function f: X ⟶ Y and an element x ∈ X, we call f(x) the **image** of

x. If A ⊆ X, then the **image** of A is f(A) = { f(x) | x ∈ A }
= { y | f(x) = y for some x ∈ A }

Note that f(A) ⊆ Y.

The set f(x) is called the **range** of f. f(X) = { y ∈ Y | y = f(x) for some x ∈ X }

[insert image of domain and co-domain, and range]

Inverse Image:
Given a function f: X ⟶ Y, if B ⊆ Y, the **inverse image** or **preimage** of B is

$$f^{-1}(B) = \{x \in X | f(x) \in B\} \tag{81}$$

Observation: Suppose f and g are functions from X to Y. Then f and g are equal, written f = g, if and only if

- f(x) = g(x), ∀ x ∈ X

Example:
Define f: ℤ ⟶ ℤ by f(x) = x
and g: ℤ ⟶ ℤ by g(x) = $\sqrt{x^2}$

Hence f ≠ g since f(-1) = -1 but g(-1) = $\sqrt{(-1)^2}$ = 1

Note that the range of f is ℤ and the range of g is $\mathbb{Z}^{\geq 0}$

The Identity Function
Given a set X, the function ι_X: X ⟶ X defined by

- ι_X(x) = x for every x ∈ X

is called the **identity function** on X

Here ι is the Greek letter **iota**

Sequences:
An infinite sequence is a function defined on the set of integers greater than or equal to some fixed integer.

Example:
A sequence { a_n }$_{k \geq 1}$, is a function f with domain $\mathbb{Z}^+$

- f(n) = an for every n ∈ $\mathbb{Z}^+$

One-to-one functions

Let f be a function from a set X to a set Y. The function f is one-to-one (or **injective**) if and only if for all elements x_1 and x_2 in X, if f(x_1) = f(x_2), then $x_1 = x_2$

Or, equivalently, for all elements x_1 and x_2 in X,

- if $x_1 \neq x_2$, then f(x_1) $\neq$ f(x_2)

A function f: X $\longrightarrow$ Y is not not one-to-one if and only if there exists some x_1 and x_2 in X such that f(x_1) = f(x_2) and $x_1 \neq x_2$

3.4.1 Proving one-to-one

To prove a function f: X $\longrightarrow$ Y is one-to-one, usually use the direct method of proof:

- Suppose x_1 and x_2 are elements of X and f(x_1) = f(x_2)
- Show that $x_1 = x_2$
- To prove that a function f: X $\longrightarrow$ Y is not one-to-one, usually find elements x_1 and x_2 in X such that f(x_1) = f(x_2) but $x_1 \neq x_2$

Example: Let f: $\mathbb{R} \longrightarrow \mathbb{R}$ be defined by f(x) = x^2. Is f one-to-one (injective)?

Proof that f is **not** one-to-one:
Take x_1 = 2 and x_2 = -2. Since f(2) = 4 and f(-2) = 4, **different** elements with the same image. Thus, f is not one-to-one.

Example: Let f: $\mathbb{R} \longrightarrow \mathbb{R}$ be defined by f(x) = $\frac{x}{2}$. Is f one-to-one?

Proof that f is one-to-one:
Suppose x_1,$x_2 \in \mathbb{R}$ and f(x_1) = f(x_2). Hence $\frac{x_1}{2} = \frac{x_2}{2}$, so multiplying both sides by 2 we have $x_1 = x_2$

Thus, $\forall x_1$, $x_2 \in \mathbb{R}$, f(x_1) = f(x_2) $\rightarrow x_1 = x_2$. $\therefore$ f is one-to-one

3.5 Onto functions

Let f be a function from a set X to a set Y. The function f is **onto** (or **surjective**) if and monly if given any element y $\in$ Y, it is possible to find an element x $\in$ X with the property that y = f(x)

Equivalently, f : X $\longrightarrow$ Y is onto if and only if

- $\forall$ y $\in$ Y, $\exists$ x $\in$ X such that f(x) = y

A function f: X $\longrightarrow$ Y is not onto if and only if there exists some y $\in$ Y such that for all x $\in$ X, f(x) $\neq$ y

3.5.1 Proving if a function is onto

- To prove a function f: X $\longrightarrow$ Y is onto:
  - Suppose that y $\in$ Y
  - Consturct an element x of X with f(x) = y
- To prove that a function f: X $\longrightarrow$ Y is not onto:
  - Find an element y $\in$ Y such that y $\neq$ f(x) for any x $\in$ X

Example:
Let f: $\mathbb{R} \longrightarrow \mathbb{R}$ be defined by f(x) = 2x - 3. Is f onto?

Proof that f is onto:
Suppose y $\in \mathbb{R}$. Take x = $\frac{y+3}{2} \in \mathbb{R}$. Then f(x) = f($\frac{y+3}{2}$) = 2($\frac{y+3}{2}$)-3 = y+3-3 = y

Hence $\forall$ y $\in \mathbb{R}$, $\exists$ x $\in \mathbb{R}$ such that f(x) = y. Thus, f is onto.

Example:
Let g: $\mathbb{Z} \longrightarrow \mathbb{Z}$ be denoted by g(x) = x^2. Is g onto?

Proof that g is not onto:
Take y = -1 $\in \mathbb{Z}$. Since $x^2 \geq 0$ for every x $\in \mathbb{Z}$, there does not exist an element in the domain with image -1. Hence, g is not onto.

3.6 Bijections

A function f is a one-to-one correspondence or a **bijection** (or **bijective**) if and only if f is both one-to-one and onto.

Theorem:

Suppose that the function f: X $\longrightarrow$ Y is a bijection. Then there exists a function f^{-1}: Y $\longrightarrow$ X that is defined as follows:

Given any element y $\in$ Y,

- f^{-1}(y) = the unique element x $\in$ X such that f(x) = y

In other words,

- f^{-1}(y) = x if and only if y = f(x)

The function f^{-1} is called the **inverse function** of f.

Example:
Let f: $\mathbb{R} \longrightarrow \mathbb{R}$ be defined by f(x) = 2x + 1

f is a bijection

$$f(x) = y \leftrightarrow 2x + 1 = y \tag{82}$$

$$\leftrightarrow x = \frac{y-1}{2} \tag{83}$$

Therefore, the function

- f^{-1}(y) = $\frac{y-1}{2}$ is the inverse function of f

3.6.1 Composition of functions

Let f: X $\longrightarrow$ Y and g: Y $\longrightarrow$ Z be functions.

The composition of f and g is the function

- g ∘ f: X $\longrightarrow$ Z defined by
  - (g ∘ f)(x) = g(f(x)) ∀ x ∈ X

[insert picture of g∘f]

The domain of g ∘ f is X and the co-domain of g ∘ f is Z.

The range of g ∘ f is the image (under g) of the range of f.

Example:
Let f: $\mathbb{R} \longrightarrow \mathbb{R}$ and g: $\mathbb{R} \longrightarrow \mathbb{R}$ be defined by

- f(x) = x^2 for all x ∈ $\mathbb{R}$
- g(x) = x^3 - 2x for all x ∈ $\mathbb{R}$

Find (g ∘ f)(x) and (f ∘ g)(x)

$$(g \circ f)(x) = g(f(x)) = g(x^2) = (x^2)^3 - 2(x^2) = x^6 - 2x^2 \tag{84}$$

$$(f \circ g)(x) = f(g(x)) = f(x^3 - 2x) = (x^3 - 2x)^2 = x^6 - 4x^4 + 4x^2 \tag{85}$$

Warning: Note that g ∘ f and f ∘ g mean different things

Theorem:
If f: X $\longrightarrow$ Y is a function and ι_x is the identity function on X and ι_y is the identity function on Y, then

- f ∘ ι_x = f and ι_y ∘ f = f

Proof:

Suppose f: X $\longrightarrow$ Y is a function and ι_x and ι_y are the identity functions on X and y respectively. Then, by definition

- ι_x(x) = x $\forall$ x $\in$ X
- ι_y(y) = y $\forall$ y $\in$ Y

Now for all x $\in$ X (f $\circ$ ι_x)(x) = f(ι_x(x)) = f(x)
Hence f $\circ$ ι_x = f.

Theorem:

Let f: X $\longrightarrow$ Y be a bijection with inverse function f^{-1}: Y $\longrightarrow$ X. Then

- $f^{-1}\circ$ f = ι_x and f $\circ$ f^{-1} = ι_y
- $\forall$ x $\in$ X, y $\in$ Y
- f^{-1}(y) = x $\leftrightarrow$ f(x) = y

Example:

The function f: $\mathbb{R} \longrightarrow \mathbb{R}$ defined by f(x) = 2x + 1 for all x $\in \mathbb{R}$ is a bijective function with inverse function f^{-1}(y) = $\frac{y-1}{2}$ for all y $\in \mathbb{R}$

Thus, for all x $\in \mathbb{R}$,

$$(f^{-1} \circ f)(x) \tag{86}$$
$$= f^{-1}(f(x)) \tag{87}$$
$$= f^{-1}(2x+1) \tag{88}$$
$$= \frac{(2x+1)-1}{2} \tag{89}$$
$$= x \tag{90}$$
$$\therefore f^{-1} \circ f = \iota_{\mathbb{R}} \tag{91}$$

Also, for all y $\in \mathbb{R}$,

$$(f^{-1} \circ f)(y) \tag{92}$$
$$= f^{-1}(f(y)) \tag{93}$$
$$= f\frac{y-1}{2} \tag{94}$$
$$= 2\frac{y-1}{2} + 1 \tag{95}$$
$$= y \tag{96}$$
$$\therefore f^{-1} \circ f = \iota_{\mathbb{R}} \tag{97}$$

3.6.2 Injective and surjective composite functions

Theorem:

If f: X $\longrightarrow$ Y and g: Y $\longrightarrow$ Z are both one-to-one, then g $\circ$ f is one-to-one.

Proof:

Suppose f: X $\longrightarrow$ Y and g: Y $\longrightarrow$ Z are both one-to-one functions. Suppose x_1, x_2 $\in$ X and

- (g $\circ$ f)(x_1) = (g $\circ$ f)(x_2)

Then,

- g(f(x_1)) = g(f(x_2))

Since g is one-to-one, we have f(x_1) = f(x_2)

Now, since f is one-to-one, we have $x_1 = x_2$

Therefore, g $\circ$ f is one-to-one

Theorem:

If f: X $\longrightarrow$ Y and g: Y $\longrightarrow$ Z are both onto functions, then g $\circ$ f is onto.

Proof:

Suppose f: X $\longrightarrow$ Y and g: Y $\longrightarrow$ Z are both onto functions

Suppose z $\in$ Z

Since g is onto, $\exists$ y $\in$ Y such that g(y) = z

Since f is onto, $\exists$ x $\in$ X such that f(x) = y

Hence $\exists$ x $\in$ X such that

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) && (98)\\ &= g(y) && (99)\\ &= 3 && (100)\end{aligned}$$

Therefore, g $\circ$ f is onto.

3.6.3 Cardinality

The **cardinality** of a set is a measure of how large it is

One says that two sets X and Y have the *same cardinality* if and only if there is a bijection between them.
We write this as |X| = |Y|

Fact:
If |X| = |Y| and |Y| = |Z|, then |X| = |Z|

3.7 Infinite and Finite sets

A finite set is either one which has no elements at all, or one for which there exists a bijection with a set of the form { 1, 2, ..., n } for some fixed positive integer n.

An infinite set is a nonempty set for which there does **not** exist any bijection with a set of the form { 1, 2, ..., n } for any positive integer n.

3.7.1 Finite Sets

Theorem:

Suppose X and Y are finite sets.

1. If |X| ¿ |Y|, then there is no injective function f: X ⟶ Y
2. If |X| ¡ |Y|, then there is no surjective function f: X ⟶ Y
3. There is a bijective function f: X ⟶ Y if and only if |X| = |Y|

Corollary:

For finite sets X and Y with |X| = |Y|, the following statements are equivalent:

- f: X ⟶ Y is injective
- f: X ⟶ Y is surjective
- f: X ⟶ Y is bijective

Note these results do **NOT** apply to infinite sets.

For example, if X = $\mathbb{Z}$ and Y = $\mathbb{Z}$ then f: X ⟶ Y given by f(x) = 2x, $\forall$ x $\in$ X is one-to-one but not onto, even though |X| = |Y|

3.7.2 Infinite Sets

Let $2\mathbb{Z} = \{$ n | n = 2k for some k $\in \mathbb{Z}$ $\}$. Prove that $|\mathbb{Z}| = |2\mathbb{Z}|$

Proof:

Define a function f: $\mathbb{Z} \longrightarrow 2\mathbb{Z}$ as follows:

- f(k) = 2k for every k $\in \mathbb{Z}$

To show f is injective:
Suppose k_1, $k_2 \in \mathbb{Z}$ and f(k_1) = f(k_2). Then $2k_1 = 2k_2$, so, by dividing both sides by 2, we have

- $k_1 = k_2$

Hence f is injective.

To show f is surjective: Suppose n $\in 2\mathbb{Z}$. Then n = 2k for some k $\in \mathbb{Z}$. Hence f(k) = 2k = n, so f is surjective.

Thus, f is a bijection from $\mathbb{Z}$ to $2\mathbb{Z}$
$\therefore$ $|\mathbb{Z}| = |2\mathbb{Z}|$

Fact:

$|\mathbb{Z}^+| = |\mathbb{Z}|$

The function f: $\mathbb{Z}^+ \longrightarrow \mathbb{Z}$ defined by;

$$\begin{cases} \frac{n}{2} & ifn \in \mathbb{Z}^+ iseven \\ -\frac{(n-1)}{2} & ifn \in \mathbb{Z}^+ isodd \end{cases}$$

4 Logical Equivalences

Given any statement variables 'p', 'q' and 'r', a tautology '**t**' and contradiction '**c**', the following logical equivalences hold.

4.1 Commutative laws

- $p \wedge q \equiv q \wedge p$
- $p \vee q \equiv q \vee p$

4.2 Associative laws

- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- $(p \vee q) \vee r \equiv p \vee (q \vee r)$

4.3 Distributive laws

- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

4.4 Identity laws

- $p \wedge \mathbf{t} \equiv p$
- $p \vee \mathbf{c} \equiv p$

4.5 Negation laws

- $p \vee {\sim}p \equiv \mathbf{t}$
- $p \wedge {\sim}p \equiv \mathbf{c}$

4.6 Double negative laws

- ${\sim}({\sim}p) \equiv p$

4.7 Idempotent laws

- $p \vee p \equiv p$
- $p \wedge p \equiv p$

4.8 Universal bound laws

- $p \vee \mathbf{t} \equiv \mathbf{t}$
- $p \wedge \mathbf{c} \equiv \mathbf{c}$

4.9 De Morgan's laws

- ${\sim}(p \wedge q) \equiv {\sim}p \vee {\sim}q$
- ${\sim}(p \vee q) \equiv {\sim}p \wedge {\sim}q$

4.10 Absorption laws

- $p \vee (p \wedge q) \equiv p$
- $p \wedge (p \vee q) \equiv p$

4.11 Negations of t and c

- ${\sim}\mathbf{t} \equiv \mathbf{c}$
- ${\sim}\mathbf{c} \equiv \mathbf{t}$