Discrete Mathematics

MATH1061 · 2026

April Kidd

Contents

Preface

These notes were created as the first input into the UQ Open Source notes repository. Majority of these notes were taken from the 2025 rendition of the course (as it is now), and were constructed from memory, Susanna Epp's book "Discrete Mathematics with Applications", and the UQ Extend pre-reading. Feel free to correct or extend (pun intended) any of the content in this text.

As a personal note, the reason I began with writing this compilation is because Discrete Mathematics, and Dr. Barbara Maenhaut's teaching of it, holds a quite special place in my heart. When I arrived at university, I was beginning a Bachelor of Computer Science / Economics. MATH1061, Discrete Mathematics, was among my first courses in my first semester, and the passion Maenhaut showed for the subject, and her exceptional teaching, invited me to fall back in love with mathematics. Its to her that I owe my eventual change in degree to Pure Mathematics, and the passion I've had reignited in me for the subject. So, truly, thank you, and I hope these notes allow some other students to fall in love with mathematics as I have.

1 Logic

Logic is the foundation of mathematical reasoning. It provides a formal framework for analysing arguments, determining whether statements are true or false, and constructing valid proofs. In this chapter, we study propositional logic, which deals with statements that can be either true or false, and the logical connectives that allow us to build more complex statements from simpler ones.

Understanding logic is essential for:

- Writing and reading mathematical proofs
- Analyzing the correctness of arguments
- Designing algorithms and computer programs
- Reasoning precisely in any mathematical context

We begin by studying the basic building blocks of logic: statements and logical connectives.

1.1 Logical Form

The **logical form** of a statement refers to its structure in terms of logical connectives and statement variables, independent of the specific content. Identifying the logical form allows us to analyse arguments abstractly and determine their validity based on structure alone.

Definition 1

A **statement** (or **proposition**) is a declarative sentence that is either true or false, but not both.

Example 1

The following are statements:

- "$2 + 3 = 5$" (true)
- "Sydney is the capital of Australia" (false)
- "All prime numbers are odd" (false)
- "If $x > 0$, then $x^2 > 0$" (true for real numbers)

The following are **not** statements:

- "Is it raining?" (question, not declarative)
- "Close the door!" (command, not declarative)
- "$x + 1 = 2$" (truth depends on value of x; neither always true nor always false)
- "This statement is false" (paradox, cannot be assigned a truth value)

Definition 2

A **statement variable** (or **propositional variable**) is a letter such as p, q, or r that represents an arbitrary statement.

A **statement form** (or **propositional form**) is an expression involving statement variables and logical connectives that becomes a statement when specific statements are substituted for the variables.

Important
The truth value of a statement form depends on the truth values assigned to its statement variables. Our goal is to understand how the logical connectives combine these truth values.

1.1.1 Statements and Logical Connectives

Logical connectives allow us to combine simple statements to form more complex statements. The truth value of a compound statement is completely determined by the truth values of its components and the connectives used.

Basic Logical Connectives:

Definition 3 (Negation)
The **negation** of a statement p, denoted $\neg p$ and read "not p", is the statement that is true when p is false, and false when p is true.

p	$\neg p$
T	F
F	T

Example 2
- p: "It is raining"
- $\neg p$: "It is not raining"

Definition 4 (Conjunction)
The **conjunction** of statements p and q, denoted $p \wedge q$ and read "p and q", is true when both p and q are true, and false otherwise.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 3
- p: "I have a laptop"

- q: "I have an internet connection"
- $p \wedge q$: "I have a laptop and I have an internet connection"

Definition 5 (Disjunction)
The **disjunction** of statements p and q, denoted $p \vee q$ and read "p or q", is true when at least one of p or q is true, and false when both are false.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Important
In logic, "or" is **inclusive**; it includes the case where both statements are true. This differs from everyday usage where "or" sometimes means "one or the other but not both" (exclusive or).

Example 4
- p: "The dessert comes with ice cream"
- q: "The dessert comes with fruit"
- $p \vee q$: "The dessert comes with ice cream or fruit (or both)"

Note
The **exclusive or** of p and q, sometimes denoted $p \oplus q$, is true when exactly one of p or q is true, but not both. In propositional logic, this can be expressed as $(p \vee q) \wedge \neg(p \wedge q)$.

1.1.2 Truth Tables

A truth table is a systematic way to determine the truth value of a compound statement for all possible combinations of truth values of its component statements.

Definition 6
A **truth table** for a statement form displays:
- All possible combinations of truth values for the statement variables
- The resulting truth value of the compound statement for each combination

Constructing Truth Tables:

1. **Determine the number of rows:** For n statement variables, you need 2^n rows to represent all possible truth value combinations

2. **List all combinations:** Systematically list all T/F combinations for the variables
3. **Evaluate subexpressions:** Work from the inside out, evaluating logical connectives according to their definitions
4. **Compute the final column:** The last column shows the truth value of the entire statement form

Example 5
Construct a truth table for $(p \wedge q) \vee \neg p$.

p	q	$p \wedge q$	$\neg p$	$(p \wedge q) \vee \neg p$
T	T	T	F	T
T	F	F	F	F
F	T	F	T	T
F	F	F	T	T

Since we have 2 variables (p and q), we need $2^2 = 4$ rows.

Steps:
1. List all T/F combinations for p and q
2. Compute $p \wedge q$ using the conjunction definition
3. Compute $\neg p$ using the negation definition
4. Compute $(p \wedge q) \vee \neg p$ using the disjunction definition

Example 6
Construct a truth table for $\neg(p \vee q)$ and compare it to $\neg p \wedge \neg q$.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$
$\neg p \wedge \neg q$	T	T	T	F	F
F	F	T	F	T	F
F	T	F	F	T	T
F	T	F	F	F	F
F	T	T	T	T	

Notice that columns 4 and 7 are identical. This shows that $\neg(p \vee q) \equiv \neg p \wedge \neg q$, which is one of De Morgan's laws.

Important
Number of Rows in Truth Tables:
- 1 variable: $2^1 = 2$ rows
- 2 variables: $2^2 = 4$ rows
- 3 variables: $2^3 = 8$ rows

- n variables: 2^n rows

Truth tables grow exponentially, so for complex statements with many variables, using logical equivalence laws (covered later) is often more efficient.

Remark
When filling in truth value combinations, it's helpful to use a systematic pattern:
- For the first variable: alternate in blocks of 2^{n-1} (half T's, half F's)
- For the second variable: alternate in blocks of 2^{n-2}
- And so on, until the last variable alternates: T, F, T, F, …

This guarantees all combinations are covered exactly once.

1.1.3 Compound Statements

A compound statement is built from simpler statements using logical connectives. Understanding how to parse and evaluate compound statements is essential for working with complex logical expressions.

Definition 7
A **compound statement** is a statement formed by combining one or more statements using logical connectives (negation, conjunction, disjunction, conditional, biconditional).

Order of Operations (Precedence):

When evaluating compound statements, we follow this order of precedence (from highest to lowest):

1. **Negation** ($\neg$) - evaluated first
2. **Conjunction** ($\wedge$) and **Disjunction** ($\vee$) - evaluated second (equal precedence, evaluate left to right)
3. **Conditional** ($\rightarrow$) and **Biconditional** ($\leftrightarrow$) - evaluated last (equal precedence)

Important
When in doubt, use parentheses to clarify the intended meaning. Parentheses override the default precedence.

Example 7
Parse the following statement forms:

- $\neg p \wedge q$ means $(\neg p) \wedge q$, not $\neg(p \wedge q)$
- $p \wedge q \vee r$ means $(p \wedge q) \vee r$ (conjunction before disjunction by left-to-right evaluation)
- $p \vee q \rightarrow r$ means $(p \vee q) \rightarrow r$ (connectives before conditional)

- $p \to q \land r$ means $p \to (q \land r)$ (conjunction before conditional)

Example 8 (Translating English to Logic)
Translate the following English sentences into symbolic logic.

Let:
- p: "It is raining"
- q: "The ground is wet"
- r: "I have an umbrella"

1. "It is raining and the ground is wet" $\to p \land q$
2. "It is not raining but the ground is wet" $\to \neg p \land q$
3. "If it is raining, then the ground is wet" $\to p \to q$
4. "It is raining, or the ground is wet and I have an umbrella" $\to p \lor (q \land r)$
5. "If it is not raining, then I do not have an umbrella" $\to \neg p \to \neg r$

Example 9 (Evaluating Compound Statements)
Evaluate the truth value of $\neg p \lor (q \land r)$ when p is true, q is false, and r is true.

Step by step:
1. $\neg p = \neg T = F$
2. $q \land r = F \land T = F$
3. $\neg p \lor (q \land r) = F \lor F = F$

Therefore, the statement is false under this assignment.

Note
Common English Phrases and Their Logical Forms:

- "both p and q" $\to p \land q$
- "neither p nor q" $\to \neg p \land \neg q$ or equivalently $\neg(p \lor q)$
- "either p or q" $\to p \lor q$
- "p but q" $\to p \land q$ (emphasis on contrast)
- "p unless q" $\to \neg q \to p$ or equivalently $p \lor q$
- "p only if q" $\to p \to q$
- "p if q" $\to q \to p$

Remark
Translating between English and logical notation requires careful attention to context and meaning. Natural language can be ambiguous, while logical notation is

precise. When translating, always verify that the logical form captures the intended meaning of the original statement.

1.2 Logical Equivalence

Two statement forms P and Q are **logically equivalent**, denoted $P \equiv Q$, if they have identical truth values for every possible combination of truth values of their statement variables.

Example 10
Show that $\neg\neg p \equiv p$ using a truth table.

p	$\neg p$	$\neg\neg p$
T	F	T
F	T	F

Since p and $\neg\neg p$ have identical truth values for every row, we conclude $\neg\neg p \equiv p$.

Important
To show two statement forms are **not** logically equivalent, it suffices to find just one row in the truth table where their truth values differ.

1.2.1 Tautologies and Contradictions

Definition 8
A **tautology** is a statement form that always takes truth value "true" for all possible truth values of its variables.

Example 11
The statement form $p \vee \neg p$ is a tautology.

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Since $p \vee \neg p$ is true in every row, it is a tautology.

Definition 9
A **contradiction** is a statement form that always takes truth value "false" for all possible truth values of its variables.

Example 12
The statement form $p \wedge \neg p$ is a contradiction.

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

Since $p \wedge \neg p$ is false in every row, it is a contradiction.

1.2.2 Laws of Logic

The following logical equivalences are fundamental and should be memorised:

Law	**Equivalence**
De Morgan's Laws	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Commutative Laws	$p \wedge q \equiv q \wedge p$
	$p \vee q \equiv q \vee p$
Associative Laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive Laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity Laws	$p \wedge \text{true} \equiv p$
	$p \vee \text{false} \equiv p$
Domination Laws	$p \wedge \text{false} \equiv \text{false}$
	$p \vee \text{true} \equiv \text{true}$
Negation Laws	$p \vee \neg p \equiv \text{true}$
	$p \wedge \neg p \equiv \text{false}$
Double Negative Law	$\neg\neg p \equiv p$
Idempotent Laws	$p \wedge p \equiv p$
	$p \vee p \equiv p$

Remark

When working with three variables, truth tables require $2^3 = 8$ rows. More generally, n variables require 2^n rows, which can become very large. Using logical equivalence laws to simplify expressions is often more efficient than constructing large truth tables.

1.2.3 Simplifying Logical Expressions

We can use the laws of logical equivalence to simplify complex statement forms without constructing truth tables.

Example 13

Show that $(p \wedge (\neg q \vee q)) \wedge q \equiv p \wedge q$ using logical equivalence laws.

$$\begin{aligned}(p \wedge (\neg q \vee q)) \wedge q &\equiv (p \wedge (q \vee \neg q)) \wedge q && \text{(commutative law)}\\ &\equiv (p \wedge \text{true}) \wedge q && \text{(negation law)}\\ &\equiv p \wedge q && \text{(identity law)}\end{aligned}$$

By applying the commutative law, negation law, and identity law in sequence, we have shown that the original expression is logically equivalent to $p \wedge q$.

Remark

This method is particularly useful when dealing with many variables, as the truth table approach would require 2^n rows for n variables. For example, with 5 variables, a truth table would need 32 rows, making algebraic simplification much more practical.

1.3 Conditional Statements

Definition 10

Let p and q be statement variables. The **conditional statement** from p to q, denoted $p \to q$ and read as "p implies q" or "if p then q", is defined by the truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that $p \to q$ is false **only when** p is true and q is false. In the conditional $p \to q$:

- p is called the **hypothesis** (or antecedent)
- q is called the **conclusion** (or consequent)

Example 14

Consider the promise: "If you do your homework, then you get a chocolate."

In which scenario is this promise false?

- **Scenario A:** You do not do your homework, and you get a chocolate. (Promise kept)
- **Scenario B:** You do your homework, and you get a chocolate. (Promise kept)
- **Scenario C:** You do your homework, and you do not get a chocolate. (**Promise broken**)
- **Scenario D:** You do not do your homework, and you do not get a chocolate. (Promise kept)

Only in Scenario C, where the hypothesis is true and conclusion is false, is the promise broken.

Theorem 1
The conditional statement can be expressed using other logical connectives:

$$p \to q \equiv \neg p \lor q$$

Proof
We verify this using a truth table:

p	q	$\neg p \lor q$	$p \to q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Since the columns for $\neg p \lor q$ and $p \to q$ are identical, they are logically equivalent. □

Example 15
The statement "If you do your homework, then you get a chocolate" can be equivalently stated as "Either you do not do your homework, or you get a chocolate."

Negating a Conditional:

Theorem 2
The negation of a conditional statement is:

$$\neg(p \to q) \equiv p \land \neg q$$

Proof

$$\begin{aligned} \neg(p \to q) &\equiv \neg(\neg p \lor q) && \text{(conditional equivalence)} \\ &\equiv \neg\neg p \land \neg q && \text{(De Morgan's law)} \\ &\equiv p \land \neg q && \text{(double negative law)} \end{aligned}$$

□

Example 16
The negation of "If today is Monday, then tomorrow is my birthday" is "Today is Monday, but tomorrow is not my birthday."

(Note: In English, "but" is often used instead of "and" when expressing a surprising or contradictory conjunction.)

1.3.1 Conditional and Biconditional

Definition 11
Let p and q be statement variables. The **biconditional statement** of p and q, denoted $p \leftrightarrow q$ and read as "p if and only if q" (abbreviated "iff"), is defined by the truth table:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Note that $p \leftrightarrow q$ is true when p and q have the **same truth value**, and false otherwise.

Theorem 3
The biconditional can be expressed as a conjunction of two conditionals:

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

Note
The biconditional $p \leftrightarrow q$ can be read as:

- "p if and only if q"
- "p is equivalent to q"
- "p iff q"

1.3.2 Converse, Inverse, and Contrapositive

Given a conditional statement $p \to q$, we can form three related statements:

Definition 12

- The **converse** of $p \to q$ is $q \to p$
- The **inverse** of $p \to q$ is $\neg p \to \neg q$
- The **contrapositive** of $p \to q$ is $\neg q \to \neg p$

Theorem 4
A conditional statement and its contrapositive are logically equivalent:

$$p \to q \equiv \neg q \to \neg p$$

Proof
We verify this using a truth table:

p	q	$\neg p$	$\neg q$	$p \to q$
$\neg q \to \neg p$	T	T	F	F
T	T	T	F	F
T	F	F	F	T
T	F	T	T	F
F	T	T	T	T

Since the columns for $p \to q$ and $\neg q \to \neg p$ are identical, they are logically equivalent. □

Example 17
Consider: "If you do your homework, then you get a chocolate."

The contrapositive is: "If you did not get a chocolate, then you did not do your homework."

These two statements are logically equivalent.

Example 18
The contrapositive of "If Sara passes the final exam, then Sara passes the course" is "If Sara does not pass the course, then Sara does not pass the final exam."

Important
A conditional and its contrapositive are **always** logically equivalent. However, a conditional is **not** necessarily equivalent to its converse or inverse.

1.3.3 Necessary and Sufficient Conditions

The conditional and biconditional can be expressed using the terminology of necessary and sufficient conditions.

Expressing $p \to q$:

The following are equivalent ways of stating $p \to q$:

- "If p then q"
- "p implies q"
- "p is a sufficient condition for q"
- "q is a necessary condition for p"

Example 19
"If it is raining, then the ground is wet" can also be stated as:

- "Rain is a sufficient condition for the ground being wet"

- "The ground being wet is a necessary condition for rain"

Expressing $p \leftrightarrow q$:

The following are equivalent ways of stating $p \leftrightarrow q$:

- "p if and only if q"
- "p iff q"
- "p is a necessary and sufficient condition for q"
- "q is a necessary and sufficient condition for p"

Important
Understanding the language of necessary and sufficient conditions is essential for reading and writing mathematical proofs. When someone says "p is sufficient for q," they mean $p \to q$. When they say "p is necessary for q," they mean $q \to p$ (or equivalently, that q cannot be true without p being true).

Order of Operations:

When parsing logical expressions, the order of operations is:

1. Negation ($\neg$)
2. Conjunction ($\wedge$) and Disjunction ($\vee$)
3. Conditional ($\to$) and Biconditional ($\leftrightarrow$)

Remark
When in doubt, use parentheses to clarify the intended meaning.

1.4 Valid and Invalid Arguments

Definition 13
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 premises implies the conclusion.

Symbolically:

$$\begin{array}{c} P_1 \\ P_2 \\ \vdots \\ P_n \\ \therefore Q \end{array}$$

This means: $(P_1 \wedge P_2 \wedge ... \wedge P_n) \to Q$

Example 20
Consider the argument:

- If it is raining, then there are clouds.
- It is raining.
- Therefore, there are clouds.

This is a valid argument. The form is: $p \to q, p \therefore q$

Example 21
Consider the argument:

- If it is raining, then there are clouds.
- There are clouds.
- Therefore, it is raining.

This is an **invalid** argument. The form is: $p \to q, q \therefore p$

We can see this is invalid by considering a situation where there are clouds but it is not raining. Both premises are true, but the conclusion is false.

Definition 14
An argument is **valid** if whenever all of the premises are true, the conclusion is also true.

Equivalently, an argument is valid if $(P_1 \wedge P_2 \wedge ... \wedge P_n) \to Q$ is a tautology.

Definition 15
An argument is **invalid** if it is possible to have a situation where all of the premises are true but the conclusion is false.

1.4.1 Argument Forms

We can check whether an argument is valid or invalid using a truth table. An argument is valid if every row where all premises are true also has the conclusion true.

Theorem 5 (Modus Ponens)
The argument form $p \to q, p \therefore q$ is valid.

Proof
We verify this using a truth table:

p	q	$p \to q$ (Premise 1)	p (Premise 2)	q (Conclusion)
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	F

The only row where all premises are true is row 1. In that row, the conclusion is also true. Therefore, the argument is valid. □

Important
When checking validity with a truth table, we only need to examine rows where **all** premises are true. Rows where one or more premises are false can be ignored.

Example 22
Show that the argument form $p \to q, q \therefore p$ is invalid.

p	q	$p \to q$ (Premise 1)	q (Premise 2)	p (Conclusion)
T	T	T	T	T
T	F	F	F	F
F	T	T	T	F
F	F	T	F	F

Rows 1 and 3 have all premises true. In row 1, the conclusion is true. However, in row 3 (where p is false and q is true), both premises are true but the conclusion is false. Therefore, the argument is invalid.

1.4.2 Rules of Inference

Rules of inference are argument forms that are well-known to be valid. We can use these to determine the validity of more complicated arguments without constructing truth tables.

Common Rules of Inference:

Name	**Rule**	**Description**
Modus Ponens	$p \to q$ p $\therefore q$	If p implies q and p is true, then q is true
Modus Tollens	$p \to q$ $\neg q$ $\therefore \neg p$	If p implies q and q is false, then p is false
Hypothetical Syllogism	$p \to q$ $q \to r$ $\therefore p \to r$	Chain implications together

Disjunctive Syllogism	$p \vee q$ $\neg p$ $\therefore q$	If one of two alternatives is false, the other is true
Addition	p $\therefore p \vee q$	A true statement remains true when OR'd with anything
Simplification	$p \wedge q$ $\therefore p$	From a conjunction, extract either conjunct
Conjunction	p q $\therefore p \wedge q$	Two true statements can be combined
Resolution	$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	Eliminate common variable between disjunctions

Example 23
Determine if the following argument is valid using rules of inference:

$$p \to \neg r$$
$$r \vee \neg q$$
$$q$$
$$\therefore \neg p$$

We start with the three premises:
1. $p \to \neg r$
2. $r \vee \neg q$
3. q

From (2), by commutativity: $\neg q \vee r$

Rewrite as conditional: $q \to r$ … (5)

From (3) and (5), by modus ponens: r … (6)

From (6), by double negative: $\neg\neg r$ … (7)

From (1) and (7), by modus tollens: $\neg p$

Therefore, the argument is valid. We have shown that the premises imply the conclusion using only valid rules of inference.

Remark
This is how mathematical proofs work: we start with statements known to be true (axioms, previously proven theorems), then combine them using valid arguments to derive new true statements until we reach our desired conclusion.

1.4.3 Methods for Determining Validity

There are three main methods for determining whether an argument is valid or invalid:

1. **Truth Table Method:** Check if every row where all premises are true also has the conclusion true
2. **Rules of Inference:** Combine premises using known valid argument forms
3. **Searching for Counterexamples:** Try to find truth values that make all premises true but the conclusion false

Method 3: Searching for Counterexamples

This method is based on the observation that an argument is invalid if and only if there exists a situation where all premises are true but the conclusion is false.

Important
- If we can find truth values that make all premises true and the conclusion false, then the argument is **invalid**.
- If it is impossible to find such truth values, then the argument is **valid**.

Example 24
Use the counterexample method to show that $p \to q, q \therefore p$ is invalid.

We try to make all premises true and the conclusion false.

- Since p is the conclusion, set $p = \text{false}$
- Since q is a premise, set $q = \text{true}$
- Check premise $p \to q$: With $p = \text{false}$ and $q = \text{true}$, we have $p \to q = \text{true}$ ✓

We found truth values ($p = \text{false}$, $q = \text{true}$) where all premises are true but the conclusion is false. Therefore, the argument is invalid.

Example 25
Use the counterexample method to show that the following argument is valid:

$$p \to \neg r$$
$$r \vee \neg q$$
$$q$$
$$\therefore \neg p$$

Suppose the argument is invalid. Then we can find truth values making all premises true and the conclusion false.

- For the conclusion $\neg p$ to be false, we need $p = \text{true}$
- For premise q to be true, we need $q = \text{true}$
- For premise $p \to \neg r$ to be true (with $p = \text{true}$), we need $\neg r = \text{true}$, so $r = \text{false}$
- For premise $r \vee \neg q$ to be true (with $r = \text{false}$ and $q = \text{true}$), we need $\neg q = \text{true}$

But $q = \text{true}$ means $\neg q = \text{false}$, which contradicts our requirement.

Since it is impossible to make all premises true and the conclusion false simultaneously, the argument is valid.

Remark
When an argument has many statement variables, the truth table method requires 2^n rows for n variables, which can be time-consuming. The rules of inference method and counterexample method are often more efficient for complex arguments.

1.4.4 Fallacies

A **fallacy** is an error in reasoning that results in an invalid argument. Recognising common fallacies helps us avoid making logical mistakes and identify flawed arguments.

Common Logical Fallacies:

Definition 16 (Converse Error (Affirming the Conclusion))
The fallacy of assuming that $p \to q$ and q together imply p.

Form:

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

This is invalid because q could be true for reasons other than p being true.

Example 26
- If I am in Paris, then I am in France.
- I am in France.
- Therefore, I am in Paris. ✗

This is invalid; I could be in Lyon, Marseille, or any other French city.

Definition 17 (Inverse Error (Denying the Hypothesis))
The fallacy of assuming that $p \to q$ and $\neg p$ together imply $\neg q$.

Form:

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

This is invalid because q could be true even when p is false.

Example 27

- If it is raining, then the ground is wet.
- It is not raining.
- Therefore, the ground is not wet. ✗

This is invalid; the ground could be wet from a sprinkler, morning dew, etc.

Important

The converse error and inverse error are the two most common logical fallacies. They arise from confusing:

- A conditional $p \to q$ with its converse $q \to p$
- A conditional $p \to q$ with its inverse $\neg p \to \neg q$

Remember: A conditional is equivalent to its **contrapositive**, not its converse or inverse.

Definition 18 (Begging the Question (Circular Reasoning))

The fallacy of using the conclusion (or a restatement of it) as one of the premises.

This creates a circular argument where you assume what you're trying to prove.

Example 28

"The Bible is true because it is the word of God, and we know it is the word of God because the Bible says so."

This assumes the conclusion (the Bible is true) in the premise.

Definition 19 (False Disjunction (False Dichotomy))

The fallacy of presenting two alternatives as the only possibilities when other alternatives exist.

Form:

$$p \vee q$$
$$\neg p$$
$$\therefore q$$

This is valid **only if** $p \vee q$ truly represents all possibilities. If there are other options, the argument is fallacious.

Example 29

- Either you support the new policy, or you do not care about students.
- You do not support the new policy.
- Therefore, you do not care about students. ✗

This is fallacious because there are other reasons to oppose the policy besides not caring about students.

Definition 20 (Ad Hominem)

The fallacy of attacking the person making an argument rather than addressing the argument itself.

This is a fallacy because the truth of a statement is independent of who states it.

Remark

While ad hominem attacks are fallacious in formal logic, questioning someone's credibility or expertise can be relevant in informal reasoning (e.g., judging the reliability of testimony).

Summary Table of Invalid Argument Forms:

Fallacy	**Invalid Form**	**Confusion**
Converse Error	$p \to q$ q $\therefore p$	Confuses $p \to q$ with $q \to p$
Inverse Error	$p \to q$ $\neg p$ $\therefore \neg q$	Confuses $p \to q$ with $\neg p \to \neg q$
Begging the Question	Premises include conclusion	Circular reasoning
False Dichotomy	$p \vee q$ (incomplete) $\neg p$ $\therefore q$	Assumes only two alternatives

Important

To avoid fallacies:

1. Verify that your argument form is valid (use truth tables or rules of inference)
2. Ensure premises are actually true, not assumed
3. Check that all alternatives have been considered
4. Focus on the argument, not the person making it

1.5 Quantified Statements

Propositional logic deals with statements that are unconditionally true or false. However, many mathematical assertions contain variables: "x is even" has no truth value until x is specified. **Predicate logic** extends propositional logic by introducing **predicates** — sentences whose truth depends on one or more variables — and **quantifiers**, which assert that a predicate holds for all or for some members of a given set. This section follows the treatment in Epp, **Discrete Mathematics with Applications**.

1.5.1 Universal and Existential Quantifiers

Definition 21

A **predicate** (or **propositional function**) $P(x)$ is a sentence containing a variable x that becomes a statement when a specific value is substituted for x. The set of all allowable values for x is called the **domain** (or **universe of discourse**) of x.

Example 30

Let $P(x)$ be the predicate "x is divisible by 3" with domain $\mathbb{Z}^+$ (the positive integers).

- $P(6)$: "6 is divisible by 3" — **true**
- $P(7)$: "7 is divisible by 3" — **false**

The predicate $P(x)$ itself has no truth value; only $P(a)$ for a specific $a \in \mathbb{Z}^+$ does.

Definition 22

Let $P(x)$ be a predicate with domain D. The **universal quantification** of $P(x)$, written

$$\forall x \in D, P(x),$$

is read "for all x in D, $P(x)$." It is **true** when $P(x)$ holds for every $x \in D$, and **false** when there is at least one element $x_0 \in D$ for which $P(x_0)$ is false. Such a value x_0 is called a **counterexample** to the universal statement.

The symbol $\forall$ is the **universal quantifier**.

Definition 23

Let $P(x)$ be a predicate with domain D. The **existential quantification** of $P(x)$, written

$$\exists x \in D, P(x),$$

is read "there exists x in D such that $P(x)$." It is **true** when $P(x)$ holds for at least one element $x \in D$, and **false** when $P(x)$ is false for every $x \in D$.

The symbol $\exists$ is the **existential quantifier**.

Remark
When the domain is clear from context, the restriction $\in D$ is sometimes omitted: $\forall x, P(x)$ or $\exists x, P(x)$. However, the truth value of a quantified statement can change with different domains, so the domain should always be explicitly stated or unambiguously understood.

Example 31
Let the domain be $\mathbb{R}$ (the real numbers). Determine the truth value of each statement.

(a) $\forall x \in \mathbb{R}, x^2 \geq 0$ — **true.** The square of any real number is non-negative.

(b) $\forall x \in \mathbb{R}, x^2 > 0$ — **false.** The value $x = 0$ is a counterexample, since $0^2 = 0$ which is not strictly positive.

(c) $\exists x \in \mathbb{R}, x^2 = 2$ — **true.** The value $x = \sqrt{2}$ satisfies $x^2 = 2$.

(d) $\exists x \in \mathbb{R}, x^2 = -1$ — **false.** No real number has a negative square, so no witness exists.

Example 32
Let the domain be $\mathbb{Z}$ (the integers). Determine the truth value of each statement.

(a) $\forall n \in \mathbb{Z}, n^2 \geq 0$ — **true.** If $n > 0$ then $n^2 > 0$; if $n = 0$ then $n^2 = 0$; if $n < 0$ then $n^2 > 0$. In all cases $n^2 \geq 0$.

(b) $\exists n \in \mathbb{Z}, n^2 = 2$ — **false.** Since $1^2 = 1$ and $2^2 = 4$, and there is no integer strictly between 1 and 2, no integer squared equals 2.

Important
To **disprove** a universal statement $\forall x \in D, P(x)$, it suffices to exhibit a single **counterexample** — one value $x_0 \in D$ for which $P(x_0)$ is false.

To **prove** an existential statement $\exists x \in D, P(x)$, it suffices to exhibit a single **witness** — one value $x_0 \in D$ for which $P(x_0)$ is true.

For a finite domain, a universal statement can be verified by checking every element; for an infinite domain, a general argument is required.

1.5.2 Negation of Quantified Statements

The negation of a quantified statement follows a pattern directly analogous to De Morgan's laws: the quantifier flips and the predicate is negated.

Theorem 6 (Quantifier Negation Laws)
Let $P(x)$ be a predicate with domain D. Then:

$$\neg(\forall x \in D, P(x)) \equiv \exists x \in D, \neg P(x)$$
$$\neg(\exists x \in D, P(x)) \equiv \forall x \in D, \neg P(x)$$

Proof
For the first law: $\neg(\forall x \in D, P(x))$ is true exactly when it is not the case that $P(x)$ holds for every $x \in D$ — that is, when there exists some $x \in D$ for which $P(x)$ is false, i.e., $\exists x \in D, \neg P(x)$.

For the second law: $\neg(\exists x \in D, P(x))$ is true exactly when no element of D satisfies $P(x)$ — that is, $P(x)$ is false for every $x \in D$, i.e., $\forall x \in D, \neg P(x)$. □

In plain language: **the negation of an "all" statement is a "some ... not" statement, and the negation of a "some" statement is an "all ... not" statement.**

Example 33
Write the negation of each statement formally and in words, and determine its truth value. The domain is $\mathbb{Z}$.

(a) Original: $\forall n \in \mathbb{Z}, n + 1 > n$ — "Every integer is less than its successor." **True.**

Negation: $\exists n \in \mathbb{Z}, n + 1 \leq n$ — "There exists an integer that is not less than its successor." **False.**

(b) Original: $\exists n \in \mathbb{Z}, n^2 < 0$ — "There exists an integer with a negative square." **False.**

Negation: $\forall n \in \mathbb{Z}, n^2 \geq 0$ — "Every integer has a non-negative square." **True.**

Example 34
Negate the following English sentences.

(a) "All students passed the exam."

Negation: "There exists at least one student who did not pass the exam."

(b) "Some prime number is even."

Negation: "No prime number is even" (equivalently, "Every prime number is odd").

Note: statement (b) is **true** (since 2 is an even prime), so its negation is **false**.

Important
A common error is to negate "all Ps are Q" as "all Ps are not Q." The correct negation is "some P is not Q." The statement "all Ps are not Q" (i.e., no P is Q) is a stronger claim than the negation requires.

1.5.3 Statements with Multiple Quantifiers

Many important mathematical statements involve predicates of two or more variables and require nested quantifiers. Reading such statements carefully from left to right is essential.

Definition 24
Let $P(x, y)$ be a predicate with variables $x \in D$ and $y \in E$. A **multiply-quantified statement** uses two or more quantifiers in sequence:

- $\forall x \in D, \exists y \in E, P(x, y)$ — "For every x in D, there exists a y in E such that $P(x, y)$." The witness y may depend on x.
- $\exists x \in D, \forall y \in E, P(x, y)$ — "There exists an x in D such that $P(x, y)$ holds for every y in E." A single fixed x must work for all y.

Example 35
Let the domain be $\mathbb{R}$ for both variables, and let $P(x, y)$ be "$x + y = 0$."

(a) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0$

True. For any $x \in \mathbb{R}$, take $y = -x$; then $x + y = x + (-x) = 0$.

(b) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y = 0$

False. This would require a single fixed x satisfying $x + y = 0$ for every real y, which is impossible since y varies freely.

Example 36
Let the domain be $\mathbb{Z}$ for both variables, and let $P(x, y)$ be "$x < y$."

(a) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x < y$ — **true.** For any integer x, take $y = x + 1$.

(b) $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, x < y$ — **false.** This claims the existence of a largest integer, but $\mathbb{Z}$ is unbounded above.

Remark
When evaluating $\forall x \in D, \exists y \in E, P(x, y)$: for each fixed x, a suitable y must exist, but y may be chosen depending on x.

When evaluating $\exists x \in D, \forall y \in E, P(x, y)$: a single x must be found that simultaneously satisfies $P(x, y)$ for every $y \in E$. This is generally a stronger requirement.

1.5.4 Order of Quantifiers

The order in which quantifiers appear matters when they are of **mixed** type (one universal, one existential), but not when they are of the **same** type.

Theorem 7

For any predicate $P(x, y)$ with $x \in D$ and $y \in E$:

$$(\forall x \in D, \forall y \in E, P(x, y)) \equiv (\forall y \in E, \forall x \in D, P(x, y))$$
$$(\exists x \in D, \exists y \in E, P(x, y)) \equiv (\exists y \in E, \exists x \in D, P(x, y))$$

In general, $(\forall x \in D, \exists y \in E, P(x, y))$ is **not** equivalent to $(\exists y \in E, \forall x \in D, P(x, y))$.

Proof

The first equivalence holds because $\forall x \in D, \forall y \in E, P(x, y)$ is true exactly when $P(x, y)$ holds for every pair $(x, y) \in D \times E$, a condition symmetric in x and y. The second equivalence is analogous. The non-equivalence of the mixed case is shown by the examples above: in the domain $\mathbb{R}$ with $P(x, y)$ being "$x + y = 0$," the statement $\forall x, \exists y, x + y = 0$ is true while $\exists y, \forall x, x + y = 0$ is false. □

Example 37

Let the domain be $\mathbb{Z}$ for both variables, and let $P(x, y)$ be "$x \cdot y = x$."

- $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, xy = x$ — **false** (take $x = 1, y = 2$: $1 \cdot 2 = 2 \neq 1$).
- $\forall y \in \mathbb{Z}, \forall x \in \mathbb{Z}, xy = x$ — **false** (same counterexample; order of $\forall\forall$ does not matter).
- $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, xy = x$ — **true** (take $y = 1$ for any x).
- $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, xy = x$ — **true** ($y = 1$ works for every x).

Here the mixed statements happen to have the same truth value, but this is not the case in general.

Important

The statement $\exists y \in E, \forall x \in D, P(x, y)$ is logically **stronger** than $\forall x \in D, \exists y \in E, P(x, y)$:

- If a single y works for all x, it certainly provides a witness for each individual x.
- However, the converse fails: having a (possibly different) witness y for each x does not guarantee a single universal witness.

In symbols:

$$(\exists y \in E, \forall x \in D, P(x, y)) \to (\forall x \in D, \exists y \in E, P(x, y))$$

but the reverse implication does not hold in general.

2 Proof Techniques

Mathematical proof is the cornerstone of mathematical reasoning. A proof is a logically rigorous argument that establishes the truth of a mathematical statement beyond any doubt. Unlike empirical evidence or examples, which can suggest truth, a proof provides absolute certainty.

In this chapter, we study various techniques for constructing proofs:

- **Direct proof**: Start with the hypothesis and deduce the conclusion
- **Proof by contraposition**: Prove the logically equivalent contrapositive
- **Proof by contradiction**: Assume the negation and derive a contradiction
- **Proof by cases**: Break the problem into exhaustive cases
- **Counterexamples**: Disprove universal statements by finding exceptions

Understanding when and how to apply each technique is essential for reading and writing mathematical proofs. We begin with the most fundamental approach: direct proof.

2.1 Direct Proofs

A direct proof is the most straightforward method of proving a statement. To prove a conditional statement "if P then Q" directly, we assume P is true and show that Q must follow logically.

Definition 1

A **direct proof** of a conditional statement $P \to Q$ proceeds as follows:

1. Assume P is true (the hypothesis)
2. Use definitions, axioms, and previously proven theorems to deduce that Q is true (the conclusion)
3. Conclude that $P \to Q$ is true

Direct proofs typically follow this pattern:

- **Assumption:** "Suppose P is true…"
- **Body:** Chain of logical deductions using definitions, algebra, and known results
- **Conclusion:** "Therefore, Q is true."

Example 1

Theorem: For all integers n, if n is even, then n^2 is even.

Proof: Suppose n is an even integer. By definition of even, there exists an integer k such that $n = 2k$.

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since k is an integer, $2k^2$ is also an integer. Let $m = 2k^2$. Then $n^2 = 2m$ where m is an integer.

Therefore, by definition, n^2 is even.

Important
Key elements of a good direct proof:

- Clearly state what you're assuming (the hypothesis)
- Use precise definitions (e.g., "even means $n = 2k$ for some integer k")
- Show each logical step explicitly
- Conclude by explicitly stating what you've proven

2.1.1 Structure of a Direct Proof

Direct proofs follow a standard structure that helps organise the logical flow from hypothesis to conclusion.

Standard Template for Direct Proof:

Theorem: For all $x \in D$, if $P(x)$ then $Q(x)$.

Proof:

1. Suppose $x \in D$ and $P(x)$ is true. [Assume the hypothesis]
2. … [Chain of logical deductions]
3. … [Using definitions, axioms, previously proven results]
4. Therefore, $Q(x)$ is true. [State the conclusion]

Example 2 (Sum of Even Integers)
Theorem: The sum of any two even integers is even.

Proof: Suppose m and n are even integers. [Assume hypothesis]

By definition of even, there exist integers r and s such that $m = 2r$ and $n = 2s$. [Apply definition]

Then $m + n = 2r + 2s = 2(r + s)$. [Algebraic manipulation]

Since r and s are integers, $r + s$ is also an integer. [Closure of integers under addition]

Let $t = r + s$. Then $m + n = 2t$ where t is an integer. [Define witness]

Therefore, by definition, $m + n$ is even. [Conclude]

Example 3 (Product of Odd Integers)
Theorem: The product of any two odd integers is odd.

Proof: Suppose m and n are odd integers.

By definition of odd, there exist integers r and s such that $m = 2r + 1$ and $n = 2s + 1$.

Then

$$mn = (2r + 1)(2s + 1) = 4rs + 2r + 2s + 1 = 2(2rs + r + s) + 1$$

Since r and s are integers, $2rs + r + s$ is also an integer. Let $t = 2rs + r + s$.

Then $mn = 2t + 1$ where t is an integer.

Therefore, by definition, mn is odd.

Note

Using Definitions: Most direct proofs rely heavily on definitions. When proving something is even, odd, divisible, rational, etc., you must:

1. State the relevant definition precisely
2. Apply the definition to expand the given information
3. Manipulate to show the conclusion matches the definition

2.1.2 Proving Universal Statements

A universal statement has the form "for all $x \in D$, $P(x)$" or equivalently "$\forall x \in D, P(x)$". To prove such a statement directly, we use the **method of generalising from the generic particular**.

Definition 2

To prove $\forall x \in D, P(x)$:

1. Let x be an arbitrary element of D (not a specific example!)
2. Show that $P(x)$ is true for this arbitrary x
3. Conclude that $P(x)$ is true for all $x \in D$

Important

The key word is **arbitrary**. You cannot prove a universal statement by checking specific examples. You must prove it works for a generic, unspecified element of the domain.

Example 4

Theorem: For all integers n, $n^2 - n$ is even.

Proof: Let n be an arbitrary integer. [Choose generic element]

We consider two cases:

Case 1: n is even. Then $n = 2k$ for some integer k.

$$n^2 - n = (2k)^2 - 2k = 4k^2 - 2k = 2(2k^2 - k)$$

Since $2k^2 - k$ is an integer, $n^2 - n$ is even.

Case 2: n is odd. Then $n = 2k + 1$ for some integer k.

$$n^2 - n = (2k+1)^2 - (2k+1) = 4k^2 + 4k + 1 - 2k - 1 = 4k^2 + 2k = 2(2k^2 + k)$$

Since $2k^2 + k$ is an integer, $n^2 - n$ is even.

In both cases, $n^2 - n$ is even. Since n was arbitrary, the statement holds for all integers n.

Remark
When the domain has natural subcases (like integers being even or odd), **proof by cases** is often the clearest approach for universal statements.

2.1.3 Proving Existential Statements

An existential statement has the form "there exists $x \in D$ such that $P(x)$", denoted $\exists x \in D, P(x)$. To prove such a statement, it suffices to find one specific element of D for which $P(x)$ holds; this is called a **constructive proof of existence**.

Definition 3
To prove $\exists x \in D, P(x)$, it suffices to:
1. Find (or construct) a specific value $x_0 \in D$
2. Verify that $P(x_0)$ is true

Example 5
Theorem: There exists an integer that can be expressed as the sum of two perfect squares in two different ways.

Proof: Take $x_0 = 50$. Then $50 = 1^2 + 7^2 = 5^2 + 5^2$.

Since 50 is an integer expressible as the sum of two perfect squares in two different ways, the statement is proved.

Example 6
Theorem: There exist irrational numbers a and b such that a^b is rational.

Proof: Consider $a = b = \sqrt{2}$. We know $\sqrt{2}$ is irrational.

Let $c = \left(\sqrt{2}\right)^{\sqrt{2}}$.

- **Case 1:** If c is rational, then we have found irrational $a = b = \sqrt{2}$ with a^b rational.
- **Case 2:** If c is irrational, let $a = c = \left(\sqrt{2}\right)^{\sqrt{2}}$ and $b = \sqrt{2}$. Then $a^b = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$, which is rational.

In either case, irrational numbers a and b exist such that a^b is rational.

Remark
Not all existence proofs are constructive. A **non-constructive** proof of existence establishes that a solution must exist (e.g., by contradiction), without explicitly identifying one. The example above is non-constructive since we do not know which case holds.

Note
Disproving an Existential Statement: To disprove $\exists x \in D, P(x)$, you must show $\forall x \in D, \neg P(x)$; that is, that no element of D satisfies P. This is typically harder than proving existence, as you must rule out all possible candidates.

2.2 Counterexamples

A universal statement claims something holds for **all** elements of a domain. A single element for which the statement fails is called a **counterexample** and is sufficient to disprove the statement entirely.

Definition 4
A **counterexample** to the universal statement $\forall x \in D, P(x)$ is a specific value $x_0 \in D$ for which $P(x_0)$ is false.

Important
To **prove** a universal statement, you must show it holds for all elements; no finite list of examples suffices.

To **disprove** a universal statement, a single counterexample is enough.

2.2.1 Disproving Universal Statements

To disprove $\forall x \in D, P(x)$, find one $x_0 \in D$ such that $P(x_0)$ is false. The negation of a universal statement is existential:

$$\neg(\forall x \in D, P(x)) \equiv \exists x \in D, \neg P(x)$$

Example 7
Claim: For all integers n, $n^2 > n$.

Disproof: Let $n = 0$. Then $n^2 = 0$ and $n = 0$, so $n^2 = n$, not $n^2 > n$.

Therefore, the claim is false. (Also false for $n = 1$ and all negative integers.)

Example 8
Claim: For all real numbers x, $\sqrt{x^2} = x$.

Disproof: Let $x = -3$. Then $\sqrt{x^2} = \sqrt{9} = 3$, but $x = -3 \neq 3$.

The correct statement is $\sqrt{x^2} = |x|$ for all real x.

Example 9
Claim: For all integers $n \geq 2$, $n^2 - n + 11$ is prime.

Disproof: Let $n = 11$. Then $n^2 - n + 11 = 121 - 11 + 11 = 121 = 11^2$, which is not prime.

2.2.2 Constructing Counterexamples

Finding a counterexample requires understanding why a statement might fail. Useful strategies:

1. **Test boundary cases:** Try $n = 0$, $n = 1$, negative values, or extreme values
2. **Test special structures:** For statements about integers, try even vs. odd; for divisibility, try primes
3. **Work backwards:** Identify what would make the conclusion false, then check if the hypothesis can still hold

Example 10
Claim: For all integers a, b, c, if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Strategy: We need $a \mid bc$ but $a \nmid b$ and $a \nmid c$. Try $a = 4$, $b = 2$, $c = 6$: then $bc = 12$ and $4 \mid 12$, but $4 \nmid 2$ and $4 \nmid 6$.

Counterexample: $a = 4$, $b = 2$, $c = 6$.

Then $a \mid bc$ (since $4 \mid 12$), but $a \nmid b$ (since $4 \nmid 2$) and $a \nmid c$ (since $4 \nmid 6$).

Therefore, the claim is false. (However, it becomes true when a is prime; this is a key property of prime numbers.)

Example 11
Claim: For all real numbers x and y, $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$.

Counterexample: Let $x = 4$ and $y = 9$. Then $\sqrt{x+y} = \sqrt{13}$, but $\sqrt{x} + \sqrt{y} = 2 + 3 = 5$. Since $\sqrt{13} \approx 3.6 \neq 5$, the claim is false.

2.3 Proof by Contradiction

A proof by contradiction is an indirect argument that is often a useful alternative to direct proof. Instead of proving a statement is true directly, we assume it is false and show this leads to a logical impossibility.

Definition 5
A **proof by contradiction** follows these steps:

1. Assume that the statement to be proved is false
2. Show that this assumption leads logically to a contradiction
3. Conclude that the statement must be true (since it cannot be false)

Proof by contradiction is particularly useful when:

- Showing that no object exists with a certain property
- Showing that an object does not have a particular property
- Proving conditional statements that are difficult to prove directly

Example 12 (No Greatest Integer)
Lemma: There is no greatest integer.

Proof: Suppose, for the sake of contradiction, that the lemma is false. Then there exists a greatest integer N. That is, for all integers n, we have $N \geq n$.

Let $M = N + 1$. Since N is an integer, M is also an integer. But clearly $M > N$, so M is an integer greater than N. This means N is not the greatest integer, which is a contradiction.

Therefore, there is no greatest integer.

Example 13 (Even and Odd are Disjoint)
Lemma: For all integers n, n is not simultaneously both even and odd.

Proof: Suppose, for the sake of contradiction, that the lemma is false. Then there exists an integer n that is both even and odd.

Since n is even, we have $n = 2k$ for some integer k (by definition of even).

Since n is odd, we have $n = 2l + 1$ for some integer l (by definition of odd).

Therefore, $2k = 2l + 1$, which gives us $1 = 2(k - l)$, or equivalently, $k - l = \frac{1}{2}$.

But this is impossible, because k and l are integers, so $k - l$ must be an integer, not $\frac{1}{2}$. This is a contradiction.

Therefore, an integer cannot be simultaneously even and odd.

2.3.1 Structure of a Proof by Contradiction

When proving a universal conditional statement of the form "for all $x \in D$, if $P(x)$ then $Q(x)$" by contradiction:

1. **Assume the statement is false.** The negation is: "there exists $x \in D$ such that $P(x)$ and $\neg Q(x)$"
2. **Show this leads to a contradiction.** Derive a logical impossibility from this assumption.
3. **Conclude the original statement is true.** Since the negation leads to a contradiction, the original statement must be true.

Important
The negation of $\forall x \in D, P(x) \to Q(x)$ is $\exists x \in D, P(x) \wedge \neg Q(x)$.This is because $\neg(P \to Q) \equiv P \wedge \neg Q$.

Example 14 (Using Contradiction for Conditional Statements)
Lemma: For all integers n, if n^2 is odd, then n is odd.

Attempted Direct Proof: Suppose n is an integer and n^2 is odd. Then $n^2 = 2k + 1$ for some integer k, so $n = \sqrt{2k + 1}$. But now what? It's unclear how to proceed.

Proof by Contradiction: Suppose the lemma is false. Then there exists an integer n such that n^2 is odd and n is even.

Since n is even, we have $n = 2k$ for some integer k.

Therefore, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Let $l = 2k^2$. Since k is an integer, l is also an integer. Thus $n^2 = 2l$, which means n^2 is even (by definition).

But we assumed n^2 is odd. Therefore, n^2 is both odd and even, which is impossible by our previous lemma. This is a contradiction.

Therefore, the original statement is true: if n^2 is odd, then n is odd.

Remark
Notice how the contradiction proof was much more straightforward than trying to prove the statement directly. This is a common situation; the contrapositive or contradiction approach often provides clearer paths to the conclusion.

2.3.2 Proving Irrationality

Proving that a number is irrational; that it cannot be written as a ratio of two integers; is a classic application of proof by contradiction. The standard approach assumes the number is rational, writes it in lowest terms, and derives a contradiction.

Theorem 1
$\sqrt{2}$ is irrational.

Proof
Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. We may assume the fraction is in lowest terms, so a and b share no common factors (in particular, they are not both even).

Squaring both sides: $2 = \frac{a^2}{b^2}$, so $a^2 = 2b^2$.

This means a^2 is even. By a previously proven lemma (if n^2 is even, then n is even), a must be even. So $a = 2k$ for some integer k.

Substituting: $(2k)^2 = 2b^2$, which gives $4k^2 = 2b^2$, so $b^2 = 2k^2$.

This means b^2 is even, so b is also even.

But now both a and b are even, contradicting our assumption that $\frac{a}{b}$ is in lowest terms.

Therefore, $\sqrt{2}$ is irrational. □

Remark
This proof can be adapted to show $\sqrt{p}$ is irrational for any prime p.

Theorem 2
$\log_2 3$ is irrational.

Proof
Suppose, for the sake of contradiction, that $\log_2 3$ is rational. Then $\log_2 3 = \frac{a}{b}$ for some integers a and b with $b > 0$.

By definition of logarithm, $2^{\frac{a}{b}} = 3$, so $2^a = 3^b$.

But 2^a is even for all $a \geq 1$, while 3^b is odd for all $b \geq 1$. An even number cannot equal an odd number; a contradiction.

(The case $a \leq 0$ is also impossible since $3^b \geq 3 > 1 \geq 2^0 \geq 2^a$ for $b \geq 1$, $a \leq 0$.)

Therefore, $\log_2 3$ is irrational. □

2.3.3 Other Applications

Proof by contradiction is widely applicable whenever a direct approach is unclear. A common pattern is to assume the opposite of what you want to show and derive something visibly impossible.

Theorem 3
There are infinitely many prime numbers.

Proof
Suppose, for the sake of contradiction, that there are only finitely many primes. List them all as $p_1, p_2, ..., p_n$.

Let $N = p_1 p_2 \cdots p_n + 1$.

When N is divided by any p_i, the remainder is 1, so no p_i divides N. Therefore N has no prime factor in our list.

But every integer greater than 1 has at least one prime factor. Since $N > 1$, N must have a prime factor not in our list; a contradiction.

Therefore, there are infinitely many primes. □

Theorem 4
If n^2 is odd, then n is odd (for any integer n).

Proof
Suppose, for the sake of contradiction, that n^2 is odd but n is even. Then $n = 2k$ for some integer k, so $n^2 = 4k^2 = 2(2k^2)$, which is even. But n^2 was assumed odd; a contradiction. Therefore n must be odd. □

Remark
Choosing Between Contradiction and Contraposition:

Both methods handle statements of the form "if P then Q" indirectly. A useful heuristic:

- Use **contraposition** when $\neg Q$ gives clean, concrete information to work with
- Use **contradiction** when the negation of the entire statement (assuming both P and $\neg Q$) leads more naturally to an impossibility
- When in doubt, try both and see which leads to a cleaner proof

2.4 Proof by Contraposition

A proof by contraposition is based on the logical equivalence between a conditional statement and its contrapositive. Since $p \to q \equiv \neg q \to \neg p$, proving the contrapositive proves the original statement.

Definition 6
The method of **proof by contraposition** follows these steps:

1. Express the statement in the form: "for all $x \in D$, if $P(x)$ then $Q(x)$"
2. Rewrite in contrapositive form: "for all $x \in D$, if $\neg Q(x)$ then $\neg P(x)$"
3. Prove the contrapositive by direct proof

Example 15 (Square Even Implies Even)
Lemma: For all integers n, if n^2 is even, then n is even.

Attempted Direct Proof: Suppose n is an integer where n^2 is even. Then $n^2 = 2k$ for some integer k, so $n = \sqrt{2k}$. It's unclear how to show n is even from here.

Proof by Contraposition: The contrapositive is: "For all integers n, if n is not even, then n^2 is not even."

Equivalently: "For all integers n, if n is odd, then n^2 is odd."

We prove this directly. Suppose n is an odd integer. Then $n = 2k + 1$ for some integer k (by definition of odd).

Therefore,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Since k is an integer, $2k^2 + 2k$ is also an integer. Let $l = 2k^2 + 2k$. Then $n^2 = 2l + 1$, which means n^2 is odd (by definition).

Since the contrapositive is true, the original statement is true.

2.4.1 Relation to the Contrapositive

The method of proof by contraposition works because of the logical equivalence:

$$p \to q \equiv \neg q \to \neg p$$

This means:

- If we prove the contrapositive $\neg q \to \neg p$ is true, then the original statement $p \to q$ is also true
- The proof of the contrapositive is typically a **direct proof**

Important

When forming the contrapositive:

- Negate both the hypothesis and conclusion
- Reverse their order
- Be careful when negating compound statements (use De Morgan's laws)

Example 16 (Same Parity Lemma)

Lemma: For all integers n and m, if $n + m$ is even, then n and m have the same parity.

(Recall: Two integers have the **same parity** if they are both even or both odd. They have **opposite parity** if one is even and the other is odd.)

Contrapositive: For all integers n and m, if n and m have opposite parity, then $n + m$ is odd.

Proof: Suppose n and m are integers with opposite parity. Without loss of generality, suppose n is even and m is odd.

Then $n = 2k$ for some integer k, and $m = 2l + 1$ for some integer l.

Therefore,

$$n + m = 2k + (2l + 1) = 2(k + l) + 1$$

Since k and l are integers, $k + l$ is an integer. Thus $n + m$ is odd (by definition).

Since the contrapositive is true, the original statement is true.

Example 17 (Product Greater Than 25)
Lemma: If the product of two positive real numbers is greater than 25, then at least one of the numbers is greater than 5.

Symbolically: For all $x, y \in \mathbb{R}^+$, if $xy > 25$, then $x > 5$ or $y > 5$.

Contrapositive: For all $x, y \in \mathbb{R}^+$, if $x \leq 5$ and $y \leq 5$, then $xy \leq 25$.

Note: $\neg(x > 5 \vee y > 5) \equiv (x \leq 5 \wedge y \leq 5)$ by De Morgan's law.

Proof: Suppose x and y are positive real numbers with $x \leq 5$ and $y \leq 5$.

Since $x \leq 5$, multiplying both sides by $y > 0$ gives $xy \leq 5y$.

Since $y \leq 5$, multiplying both sides by $5 > 0$ gives $5y \leq 25$.

Therefore, $xy \leq 5y \leq 25$, which means $xy \leq 25$.

Since the contrapositive is true, the original statement is true.

2.4.2 When to Use Contraposition

Proof by contraposition is particularly useful when:

1. **The conclusion is difficult to work with directly** - The conclusion might be a negation or disjunction that's hard to prove directly, but easier to negate
2. **The negated hypothesis gives more information** - The negation of the hypothesis might provide a concrete property to work with (e.g., "not even" becomes "odd")
3. **You get stuck with a direct proof** - If a direct proof attempt leads nowhere, try contraposition

Remark
Comparing Proof Methods:

- **Direct Proof:** Assume $P(x)$, deduce $Q(x)$
- **Contraposition:** Assume $\neg Q(x)$, deduce $\neg P(x)$ (still a direct proof, but of the contrapositive)
- **Contradiction:** Assume $P(x) \wedge \neg Q(x)$, deduce a contradiction

All three methods are valid, but one may be easier than the others depending on the statement.

Important
The contrapositive is logically equivalent to the original statement, so proving the contrapositive **is** proving the original statement. This is different from the converse or inverse, which are equiv.notalent to the original.

3 Number Theory

Number theory is the study of the integers and their properties. Despite the apparent simplicity of the integers, they exhibit rich and complex behaviour that has fascinated mathematicians for millennia.

In this chapter we study:

- **Rational and irrational numbers:** which real numbers can be expressed as fractions?
- **Divisibility:** when does one integer divide evenly into another?
- **Modular arithmetic:** the arithmetic of remainders, essential in cryptography and computing
- **The Euclidean Algorithm:** an efficient method for computing greatest common divisors

Throughout, we apply the proof techniques from the previous chapter to establish rigorous results.

3.1 Rational Numbers

Definition 1

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

Symbolically: $r \in \mathbb{Q}$ if and only if there exist integers a and b such that $r = \frac{a}{b}$ and $b \neq 0$.

The set of all rational numbers is denoted $\mathbb{Q}$ (from the German word "Quotient").

Definition 2

A real number that is not rational is **irrational**.

Theorem 1

The decimal expansion of a rational number either repeats or terminates.

Conversely, the decimal expansion of an irrational number does not repeat and does not terminate.

Example 1

- $\frac{1}{4} = 0.25$ is rational (terminating decimal)
- $\frac{1}{3} = 0.333...$ is rational (repeating decimal)
- $\pi = 3.14159...$ is irrational (non-repeating, non-terminating decimal)
- $\sqrt{2} = 1.41421...$ is irrational (non-repeating, non-terminating decimal)

3.1.1 Definitions and Properties

The rational numbers have many important algebraic properties. We prove several of these properties below.

Theorem 2 (Sum of Rationals)
The sum of any two rational numbers is rational.

Formally: For all $r, s \in \mathbb{Q}$, we have $r + s \in \mathbb{Q}$.

Proof
Suppose r and s are rational numbers. Then by definition, $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers a, b, c, d where $b \neq 0$ and $d \neq 0$.

Therefore,

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Since a, b, c, d are integers:
- The numerator $ad + bc$ is an integer
- The denominator bd is an integer
- Since $b \neq 0$ and $d \neq 0$, we have $bd \neq 0$

Thus, by definition, $r + s$ is a rational number. □

Theorem 3 (Quotient of Rationals)
For any rational number r and any non-zero rational number s, the quotient $\frac{r}{s}$ is rational.

Formally: For all $r, s \in \mathbb{Q}$, if $s \neq 0$, then $\frac{r}{s} \in \mathbb{Q}$.

Proof
Suppose r and s are rational numbers with $s \neq 0$. Then by definition, $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers a, b, c, d where $b \neq 0$, $d \neq 0$, and $c \neq 0$ (since $s \neq 0$).

Therefore,

$$\frac{r}{s} = \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}$$

Since a, b, c, d are integers:
- The numerator ad is an integer
- The denominator bc is an integer
- Since $b \neq 0$ and $c \neq 0$, we have $bc \neq 0$

Thus, by definition, $\frac{r}{s}$ is a rational number. □

Theorem 4 (Density of Rationals)
For all rational numbers r and s where $r < s$, there exists another rational number q such that $r < q < s$.

That is, between any two rational numbers, there is always another rational number. (The rationals are **dense** in the real numbers.)

Proof
Suppose r and s are rational numbers with $r < s$. By definition, $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers a, b, c, d where $b \neq 0$ and $d \neq 0$.

Let $q = \frac{r+s}{2}$ (the midpoint of r and s).

Since r and s are rational, $r + s$ is rational by the previous theorem. Since $2 \in \mathbb{Q}$ and $2 \neq 0$, we have $\frac{r+s}{2}$ is rational by the quotient theorem. Thus $q \in \mathbb{Q}$.

Now we show $r < q < s$:
- Since $r < s$, we have $q = \frac{r+s}{2} < \frac{s+s}{2} = s$
- Similarly, $q = \frac{r+s}{2} > \frac{r+r}{2} = r$

Therefore, $r < q < s$, and q is rational. □

Theorem 5 (Multiplicative Inverse)
For every non-zero rational number r, there exists a non-zero rational number s such that $rs = 1$.

(That is, every non-zero rational has a multiplicative inverse.)

Proof
Suppose r is a non-zero rational number. By definition, $r = \frac{a}{b}$ for some integers a and b where $b \neq 0$ and $a \neq 0$ (since $r \neq 0$).

Let $s = \frac{b}{a}$. Since a and b are both non-zero integers, s is a non-zero rational number.

Moreover,

$$rs = \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1$$

Therefore, for every non-zero rational r, there exists a non-zero rational s (namely, $s = \frac{1}{r}$) such that $rs = 1$. □

Theorem 6 (Sum of Rational and Irrational)
For any rational number q and any irrational number x, the sum $q + x$ is irrational.

Proof
We use proof by contradiction. Suppose the theorem is false. Then there exist a rational number q and an irrational number x such that $q + x$ is rational.

By definition, $q = \frac{a}{b}$ for some integers a, b with $b \neq 0$.

Also, $q + x = \frac{c}{d}$ for some integers c, d with $d \neq 0$ (since $q + x$ is rational).

Therefore,

$$x = (q + x) - q = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$$

Since a, b, c, d are integers and $b \neq 0$, $d \neq 0$:

- The numerator $bc - ad$ is an integer
- The denominator bd is an integer
- Since $b \neq 0$ and $d \neq 0$, we have $bd \neq 0$

Thus, by definition, x is a rational number.

But x was assumed to be irrational, which by definition means x is not rational. This is a contradiction.

Therefore, for any rational q and irrational x, the sum $q + x$ is irrational. □

3.1.2 Representations of Rational Numbers

Every rational number has multiple equivalent representations as a fraction. The most useful is the fully reduced form.

Definition 3

A fraction $\frac{a}{b}$ is in **lowest terms** (or **fully reduced**) if $\gcd(a, b) = 1$, i.e., a and b share no common factor other than 1.

Theorem 7

Every rational number can be written as a fraction in lowest terms. This representation is unique up to sign.

Example 2

- $\frac{12}{18} = \frac{2}{3}$ (dividing numerator and denominator by $\gcd(12, 18) = 6$)
- $-\frac{15}{25} = -\frac{3}{5}$ (dividing by $\gcd(15, 25) = 5$)
- $\frac{7}{1} = 7$ (integers are rational numbers with denominator 1)

Remark

When using the definition of rational number in a proof, we often write $r = \frac{a}{b}$ with $b > 0$ and $\gcd(a, b) = 1$ to obtain a canonical representation. This is standard practice when proving irrationality results.

3.2 Divisibility

Divisibility is a fundamental concept in number theory. It describes when one integer can be divided by another leaving no remainder.

Definition 4
Let a and b be integers with $a \neq 0$. We say a **divides** b, written $a \mid b$, if there exists an integer k such that $b = ak$.

Equivalently, $a \mid b$ means "b is divisible by a", "a is a factor of b", or "b is a multiple of a".

If a does not divide b, we write $a \nmid b$.

Example 3
- $3 \mid 12$ since $12 = 3 \times 4$
- $7 \mid 0$ since $0 = 7 \times 0$
- $5 \nmid 13$ since $13 = 5 \times 2 + 3$, which is not a multiple of 5
- $a \mid 0$ for every non-zero integer a
- $1 \mid b$ for every integer b

3.2.1 Definition and Basic Properties

Theorem 8 (Properties of Divisibility)
Let a, b, c be integers with $a \neq 0$. Then:

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
2. If $a \mid b$, then $a \mid bc$ for any integer c
3. If $a \mid b$ and $b \mid c$, then $a \mid c$ (transitivity)

Proof
We prove each part directly.

(1) Suppose $a \mid b$ and $a \mid c$. Then $b = as$ and $c = at$ for some integers s, t. Therefore $b + c = as + at = a(s + t)$. Since $s + t$ is an integer, $a \mid (b + c)$.

(2) Suppose $a \mid b$. Then $b = ak$ for some integer k. Therefore $bc = (ak)c = a(kc)$. Since kc is an integer, $a \mid bc$.

(3) Suppose $a \mid b$ and $b \mid c$. Then $b = as$ and $c = bt$ for some integers s, t. Therefore $c = bt = (as)t = a(st)$. Since st is an integer, $a \mid c$. □

Theorem 9
More generally, if $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n. Any such expression $mb + nc$ is called an **integer linear combination** of b and c.

Proof
Since $a \mid b$ and $a \mid c$, there exist integers s and t such that $b = as$ and $c = at$. Then $mb + nc = m(as) + n(at) = a(ms + nt)$. Since $ms + nt$ is an integer, $a \mid (mb + nc)$. □

3.2.2 The Division Algorithm

Theorem 10 (Division Algorithm)
For any integer a and positive integer d, there exist unique integers q (the **quotient**) and r (the **remainder**) such that:

$$a = dq + r \quad \text{and} \quad 0 \leq r < d$$

Example 4
- $17 = 5 \times 3 + 2$, so dividing 17 by 5 gives quotient 3 and remainder 2
- $-7 = 3 \times (-3) + 2$, so dividing -7 by 3 gives quotient -3 and remainder 2
- $21 = 7 \times 3 + 0$, so dividing 21 by 7 gives quotient 3 and remainder 0

Note
The remainder r satisfies $0 \leq r < d$, so it is always non-negative. For negative dividends, this means the quotient is not simply the truncated value; for example, $-7 \div 3 = -3$ with remainder 2, not $-7 \div 3 = -2$ with remainder -1.

3.2.3 Common Divisors

Definition 5
An integer d is a **common divisor** of integers a and b if $d \mid a$ and $d \mid b$.

The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b.

Two integers a and b are **relatively prime** (or **coprime**) if $\gcd(a, b) = 1$.

Example 5
- $\gcd(12, 18) = 6$, since the common divisors of 12 and 18 are $1, 2, 3, 6$
- $\gcd(15, 28) = 1$, since 15 and 28 share no common factor other than 1
- $\gcd(0, n) = n$ for all positive integers n

Definition 6
The **least common multiple** of positive integers a and b, denoted $\text{lcm}(a, b)$, is the smallest positive integer divisible by both a and b.

Theorem 11
For any positive integers a and b:

$$\gcd(a, b) \times \text{lcm}(a, b) = ab$$

3.3 Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers that considers only their remainders upon division by a fixed positive integer n, called the **modulus**. It is some-

times called "clock arithmetic" since hours on a 12-hour clock wrap around cyclically. It underpins much of modern cryptography, computer science, and algebra.

3.3.1 Congruence Modulo n

Definition 7

Let n be a positive integer. Two integers a and b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n \mid (a-b)$.

Equivalently, $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.

Example 6

- $17 \equiv 5 \pmod{6}$ since $6 \mid (17-5) = 12$
- $-1 \equiv 11 \pmod{4}$ since $4 \mid (-1-11) = -12$
- $100 \equiv 0 \pmod{10}$ since $10 \mid 100$
- $29 \not\equiv 2 \pmod{9}$ since $9 \nmid (29-2) = 27$… actually $9 \mid 27$, so $29 \equiv 2 \pmod{9}$

Theorem 12

Congruence modulo n is an **equivalence relation** on the integers. That is, for all integers a, b, c:

1. **Reflexivity:** $a \equiv a \pmod{n}$
2. **Symmetry:** If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
3. **Transitivity:** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

Proof

(1) $n \mid (a-a) = 0$. ✓

(2) If $n \mid (a-b)$, then $n \mid (-(a-b)) = (b-a)$. ✓

(3) If $n \mid (a-b)$ and $n \mid (b-c)$, then $n \mid ((a-b)+(b-c)) = (a-c)$. ✓ □

3.3.2 Properties of Modular Arithmetic

Theorem 13

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

1. $a + c \equiv b + d \pmod{n}$
2. $a - c \equiv b - d \pmod{n}$
3. $ac \equiv bd \pmod{n}$

Proof

Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, there exist integers s and t such that $a = b + ns$ and $c = d + nt$.

(1) $a + c = (b + ns) + (d + nt) = (b + d) + n(s + t)$, so $n \mid ((a + c) - (b + d))$.

(2) $a - c = (b + ns) - (d + nt) = (b - d) + n(s - t)$, so $n \mid ((a - c) - (b - d))$.

(3) $ac = (b + ns)(d + nt) = bd + n(bt + ds + nst) = bd + n(bt + ds + nst)$, so $n \mid (ac - bd)$. □

Important
These three properties mean we can reduce intermediate results modulo n at any point in a computation. This is essential for efficiency when working with large numbers.

Example 7
Compute $7^{\{100\}} \pmod{10}$ (i.e., find the last digit of $7^{\{100\}}$).

Observe the pattern of powers of 7 modulo 10:
- $7^1 \equiv 7$
- $7^2 \equiv 49 \equiv 9$
- $7^3 \equiv 7 \times 9 = 63 \equiv 3$
- $7^4 \equiv 7 \times 3 = 21 \equiv 1$
- $7^5 \equiv 7 \times 1 = 7$ (cycle repeats with period 4)

Since $100 = 4 \times 25$, we have $7^{\{100\}} = \left(7^4\right)^{\{25\}} \equiv 1^{\{25\}} = 1 \pmod{10}$.

Therefore, the last digit of $7^{\{100\}}$ is **1**.

3.3.3 Applications
Modular arithmetic has many important applications:

Checksums and Error Detection:

Example 8
ISBN-10 numbers use a checksum based on modular arithmetic. For a 10-digit ISBN $d_1 d_2 ... d_{\{10\}}$, the check digit satisfies:

$$d_1 + 2d_2 + 3d_3 + ... + 10d_{\{10\}} \equiv 0 \pmod{11}$$

This detects any single-digit error and any transposition of adjacent digits.

Day of the Week Calculations:

Example 9
To find the day of the week n days from today: if today is day d (where 0 = Sunday, 1 = Monday, ..., 6 = Saturday), then the day in n days is $(d + n) \pmod{7}$.

If today is Wednesday (day 3), then in 100 days it will be day $(3 + 100) \pmod{7} = 103 \pmod{7} = 5$, which is Friday.

Cryptography:

Remark
Many modern encryption systems, including RSA, are built on modular arithmetic with very large moduli. The security relies on the computational difficulty of certain problems in modular arithmetic, such as finding discrete logarithms.

3.4 The Euclidean Algorithm

The Euclidean Algorithm is one of the oldest algorithms in mathematics, dating back to Euclid's **Elements** (c. 300 BCE). It efficiently computes the greatest common divisor of two integers by repeatedly applying the Division Algorithm.

The key observation is:

Theorem 14
For integers a and b with $b \neq 0$, if $a = bq + r$ (with $0 \leq r < |b|$), then:

$$\gcd(a, b) = \gcd(b, r)$$

Proof
Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$.

Since $d \mid a$ and $d \mid b$, we have $d \mid (a - bq) = r$. So d is a common divisor of b and r, meaning $d \leq e$.

Since $e \mid b$ and $e \mid r$, we have $e \mid (bq + r) = a$. So e is a common divisor of a and b, meaning $e \leq d$.

Therefore $d = e$, i.e., $\gcd(a, b) = \gcd(b, r)$. □

3.4.1 Computing the GCD

The Euclidean Algorithm applies the division algorithm repeatedly, reducing the problem at each step until the remainder is 0.

Algorithm — Euclidean Algorithm
To compute $\gcd(a, b)$ where $a \geq b > 0$:

Apply the division algorithm repeatedly:

$$\begin{aligned} a &= bq_1 + r_1 && (0 \leq r_1 < b) \\ b &= r_1 q_2 + r_2 && (0 \leq r_2 < r_1) \\ r_1 &= r_2 q_3 + r_3 && (0 \leq r_3 < r_2) \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + 0 \end{aligned}$$

The last non-zero remainder is $\gcd(a, b) = r_{n-1}$.

Example 10
Compute $\gcd(252, 198)$.

$$\begin{aligned} 252 &= 198 \times 1 + 54 \\ 198 &= 54 \times 3 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 + 0 \end{aligned}$$

The last non-zero remainder is 18, so $\gcd(252, 198) = 18$.

Example 11
Compute $\gcd(414, 662)$.

$$\begin{aligned} 662 &= 414 \times 1 + 248 \\ 414 &= 248 \times 1 + 166 \\ 248 &= 166 \times 1 + 82 \\ 166 &= 82 \times 2 + 2 \\ 82 &= 2 \times 41 + 0 \end{aligned}$$

Therefore $\gcd(414, 662) = 2$.

4 Induction and Recursion

Mathematical induction is a powerful proof technique for establishing statements that hold for all positive integers (or all integers from some starting point). It is especially natural for statements about sequences, sums, divisibility, and inequalities indexed by n.

Closely related is the idea of **recursive definition**, where an object is defined in terms of smaller instances of itself. Together, induction and recursion form the foundation for reasoning about computation and combinatorics.

4.1 Sequences

A sequence is an ordered list of numbers. Many mathematical patterns and formulas involve sequences, and understanding them precisely is essential before working with induction.

4.1.1 Definitions and Notation

Definition 1
A **sequence** is a function whose domain is a set of consecutive integers. If the domain is $\{m, m+1, m+2, l...\}$ for some integer m, the sequence is written:

$$a_m, a_{m+1}, a_{m+2}, \ldots$$

and is denoted $\{a_n\}_{n \geq m}$ or simply $\{a_n\}$.

Each value a_n is called a **term** of the sequence; a_m is the **initial term**.

Example 1

- The sequence defined by $a_n = 2n$ for $n \geq 1$ gives: $2, 4, 6, 8, \ldots$
- The sequence defined by $b_n = n^2$ for $n \geq 0$ gives: $0, 1, 4, 9, 16, \ldots$
- The sequence defined by $c_n = (-1)^n$ for $n \geq 1$ gives: $-1, 1, -1, 1, \ldots$

Definition 2

A **summation** (or **series**) is the sum of terms of a sequence. The notation:

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \ldots + a_n$$

is called **sigma notation**. Here k is the **index**, m is the **lower limit**, and n is the **upper limit**.

Definition 3

A **product** of sequence terms uses **pi notation**:

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \cdots \cdot a_n$$

In particular, the **factorial** of a non-negative integer n is:

$$n! = \prod_{k=1}^{n} k = 1 \times 2 \times 3 \times \cdots \times n, \quad 0! = 1$$

4.1.2 Common Sequences

Example 2

Arithmetic sequences: $a_n = a + (n-1)d$ for constants a (first term) and d (common difference).

$$3, 7, 11, 15, \ldots \quad (a = 3, d = 4)$$

Sum of first n terms: $\displaystyle\sum_{k=1}^{n} (a + (k-1)d) = \frac{n}{2}(2a + (n-1)d)$

Example 3

Geometric sequences: $a_n = ar^{n-1}$ for constants a (first term) and r (common ratio).

$$2, 6, 18, 54, \ldots \quad (a = 2, r = 3)$$

Sum of first n terms: $\displaystyle\sum_{k=1}^{n} ar^{k-1} = a\frac{r^n - 1}{r - 1}$ for $r \neq 1$

Example 4
The Fibonacci sequence: Defined by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

Each term is the sum of the two preceding terms. The Fibonacci sequence arises throughout mathematics and nature.

Note
Useful summation formulas:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

$$\sum_{k=1}^{n} k^2 = n(n+1)\frac{2n+1}{6}$$

$$\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2$$

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1}-1}{r-1} \quad (r \neq 1)$$

4.2 Mathematical Induction

Mathematical induction is a proof technique for statements of the form "for all integers $n \geq a$, $P(n)$". It works by establishing a base case and then showing each case implies the next.

4.2.1 The Principle of Mathematical Induction

Definition 4 (Principle of Mathematical Induction)
Let $P(n)$ be a property defined for integers $n \geq a$. If:

1. **Base case:** $P(a)$ is true, and
2. **Inductive step:** For every integer $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true,

then $P(n)$ is true for all integers $n \geq a$.

The inductive step assumes $P(k)$ (the **inductive hypothesis**) and derives $P(k+1)$. The most common base case is $a = 0$ or $a = 1$.

Remark
Think of induction like an infinite row of dominoes. The base case knocks over the first domino. The inductive step guarantees that whenever domino k falls, domino $k+1$ falls too. Together, all dominoes fall.

4.2.2 Writing Induction Proofs

Every induction proof has a standard structure:

Claim: For all integers $n \geq a$, $P(n)$.

Proof (by mathematical induction):

Base case ($n = a$): [Verify $P(a)$ directly.]

Inductive step: Let $k \geq a$ be an arbitrary integer and suppose $P(k)$ is true. [This is the inductive hypothesis.]

[Use $P(k)$ to derive $P(k+1)$.]

Therefore, $P(k+1)$ is true.

By the principle of mathematical induction, $P(n)$ is true for all integers $n \geq a$.

4.2.3 Summation and Inequality Proofs

Example 5

Theorem: For all integers $n \geq 1$, $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof (by mathematical induction):

Base case ($n = 1$): The left side is $\sum_{k=1}^{1} k = 1$. The right side is $1\frac{1+1}{2} = 1$. These are equal. ✓

Inductive step: Suppose $k \geq 1$ and $\displaystyle\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. We must show $\displaystyle\sum_{i=1}^{k+1} i = (k+1)\frac{k+2}{2}$.

$$\sum_{i=1}^{k+1} i = \underbrace{\sum_{i=1}^{k} i}_{=\frac{k(k+1)}{2} \text{ by I.H.}} + (k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1)\left[\frac{k}{2} + 1\right] = (k+1)\frac{k+2}{2}$$

Therefore, the formula holds for $k+1$. By induction, it holds for all $n \geq 1$.

Example 6

Theorem: For all integers $n \geq 1$, $2^n > n$.

Proof (by mathematical induction):

Base case ($n = 1$): $2^1 = 2 > 1$. ✓

Inductive step: Suppose $k \geq 1$ and $2^k > k$. Then:

$$2^{k+1} = 2 \cdot 2^k > 2k = k + k \geq k + 1$$

where the last step uses $k \geq 1$.

Therefore $2^{k+1} > k + 1$. By induction, $2^n > n$ for all $n \geq 1$.

Example 7

Theorem: For all integers $n \geq 0$, $3 \mid (n^3 - n)$.

Proof (by mathematical induction):

Base case ($n = 0$): $0^3 - 0 = 0 = 3 \times 0$. ✓

Inductive step: Suppose $3 \mid (k^3 - k)$. Then:

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

Since $3 \mid (k^3 - k)$ and $3 \mid 3k(k+1)$, we have $3 \mid ((k+1)^3 - (k+1))$. ✓

By induction, $3 \mid (n^3 - n)$ for all $n \geq 0$.

4.3 Strong Mathematical Induction

Sometimes the inductive step needs not just $P(k)$, but P at all values up to k. This calls for **strong induction**.

4.3.1 The Principle of Strong Induction

Definition 5 (Principle of Strong Mathematical Induction)
Let $P(n)$ be a property defined for integers $n \geq a$. If:

1. **Base case(s):** $P(a)$ is true (or $P(a), P(a+1), ..., P(b)$ are true for some $b \geq a$), and
2. **Inductive step:** For every integer $k \geq a$ (or $k > b$), if $P(j)$ is true for all integers j with $a \leq j \leq k$, then $P(k+1)$ is true,

then $P(n)$ is true for all integers $n \geq a$.

Remark
Strong induction is logically equivalent to ordinary induction; they can prove the same statements. Strong induction is more convenient when $P(k+1)$ depends on earlier terms besides just $P(k)$.

4.3.2 Comparing Ordinary and Strong Induction

Ordinary Induction	Strong Induction
Assumes only $P(k)$ in inductive step	Assumes $P(a), P(a+1), ..., P(k)$ in inductive step
Use when $P(k+1)$ follows from $P(k)$ alone	Use when $P(k+1)$ depends on multiple earlier cases
Common for sums, products, inequalities	Common for divisibility, prime factorisation, Fibonacci

Example 8
Theorem: Every integer $n \geq 2$ can be written as a product of primes.

Proof (by strong induction):

Base case ($n = 2$): 2 is itself prime. ✓

Inductive step: Let $k \geq 2$ and suppose every integer j with $2 \leq j \leq k$ is a product of primes. Consider $k + 1$:

- If $k + 1$ is prime, we are done.
- If $k + 1$ is not prime, then $k + 1 = ab$ for integers a, b with $2 \leq a, b \leq k$. By the inductive hypothesis, both a and b are products of primes, so $k + 1 = ab$ is also a product of primes.

By strong induction, every integer $n \geq 2$ is a product of primes.

Example 9
Theorem: Every amount of postage ≥ 12 cents can be formed using 4-cent and 5-cent stamps.

Proof (by strong induction):

Base cases:
- $n = 12$: $12 = 4 + 4 + 4$ ✓
- $n = 13$: $13 = 4 + 4 + 5$ ✓
- $n = 14$: $14 = 4 + 5 + 5$ ✓
- $n = 15$: $15 = 5 + 5 + 5$ ✓

Inductive step: Let $k \geq 15$ and suppose all amounts from 12 to k can be formed. Then $k + 1 \geq 16$, so $(k + 1) - 4 \geq 12$. By the inductive hypothesis, $(k + 1) - 4$ can be formed using 4- and 5-cent stamps. Adding one 4-cent stamp gives $k + 1$. ✓

By strong induction, all amounts ≥ 12 can be formed.

4.4 Recursive Definitions

A recursive definition defines an object using previously defined instances of the same object. It has two parts: a **base case** (one or more explicitly defined starting values) and a **recursive step** (defining subsequent values in terms of earlier ones).

4.4.1 Recursively Defined Sequences

Definition 6
A **recurrence relation** for a sequence $\{a_n\}$ is a formula that expresses a_n in terms of one or more preceding terms $a_{n-1}, a_{n-2}, l...$, together with **initial conditions** that provide enough starting values to determine the sequence completely.

Example 10
The **Fibonacci sequence** is defined by:

$$F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad \text{for } n \geq 3$$

This gives: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$

Example 11
The **factorial function** can be defined recursively:

$$0! = 1, \quad n! = n \cdot (n-1)! \quad \text{for } n \geq 1$$

Example 12
The sequence defined by $a_1 = 2$, $a_n = 3a_{n-1} + 1$ gives:

$$a_1 = 2, \quad a_2 = 7, \quad a_3 = 22, \quad a_4 = 67, \ldots$$

4.4.2 Recursively Defined Sets and Functions

Definition 7
A set S can be defined recursively by:

1. **Base clause:** Specifying initial elements of S
2. **Recursive clause:** Providing rules for constructing new elements of S from existing ones
3. **Extremal clause:** Stating that nothing else is in S

Example 13
The set of natural numbers $\mathbb{N}$ can be defined recursively:

1. $0 \in \mathbb{N}$
2. If $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$
3. Nothing else is in $\mathbb{N}$

Example 14
The set of all strings over an alphabet Σ can be defined recursively:

1. The empty string $\varepsilon \in \Sigma^*$
2. If $w \in \Sigma^*$ and $a \in \Sigma$, then $wa \in \Sigma^*$

Remark
Recursive definitions are the natural home of induction proofs. When an object is defined recursively, induction on its structure typically gives the cleanest proof of properties about it.

4.5 Solving Recurrence Relations

A recurrence relation defines a sequence implicitly. Solving it means finding an explicit (closed-form) formula for the n-th term.

4.5.1 First-Order Recurrences

A **first-order linear recurrence** has the form $a_n = ra_{n-1} + f(n)$.

Example 15

Homogeneous case: $a_n = ra_{n-1}$, $a_0 = C$.

The solution is $a_n = Cr^n$ (geometric sequence).

Example 16

Solve $a_n = 2a_{n-1}$ with $a_0 = 3$.

This is a geometric recurrence with ratio $r = 2$, so $a_n = 3 \cdot 2^n$.

Verification by induction: $a_0 = 3 \cdot 2^0 = 3$ ✓, and $2a_{n-1} = 2 \cdot 3 \cdot 2^{n-1} = 3 \cdot 2^n = a_n$ ✓.

Example 17

Non-homogeneous case: Solve $a_n = 2a_{n-1} + 3$ with $a_1 = 1$.

Compute a few terms: $a_1 = 1$, $a_2 = 5$, $a_3 = 13$, $a_4 = 29$.

These suggest $a_n = 2^{n+1} - 3$. Verify: $2a_{n-1} + 3 = 2(2^n - 3) + 3 = 2^{n+1} - 3$ ✓.

5 Sets and Functions

Set theory provides the language in which virtually all of mathematics is expressed. A set is simply a collection of objects, and the operations on sets mirror the logical connectives we studied in Chapter 1. Functions formalise the idea of a rule that assigns each input exactly one output. Together, sets and functions are foundational to every branch of mathematics.

5.1 Set Theory Definitions

5.1.1 Sets and Elements

Definition 1

A **set** is an unordered collection of distinct objects called **elements** (or **members**).

We write $x \in A$ to mean "x is an element of A", and $x \notin A$ to mean "x is not an element of A".

Sets are typically denoted by capital letters $A, B, C, l...$ and elements by lowercase letters $a, b, c, l...$

Definition 2
Two sets A and B are **equal**, written $A = B$, if and only if they have exactly the same elements:

$$A = B \leftrightarrow \forall x, (x \in A \leftrightarrow x \in B)$$

Example 1
- $A = \{1, 2, 3\}$ and $B = \{3, 1, 2\}$ are equal (order does not matter)
- $C = \{1, 2, 2, 3\}$ and A are equal (repetition does not matter)
- The **empty set** $\emptyset = \{\}$ contains no elements

5.1.2 Set-Builder Notation

Definition 3
Set-builder notation defines a set by a property its elements must satisfy:

$$\{x \in D \mid P(x)\}$$

read as "the set of all x in D such that $P(x)$".

Example 2
- $\{x \in \mathbb{Z} \mid x > 0\} = \{1, 2, 3, 4, l...\}$; positive integers
- $\{x \in \mathbb{R} \mid x^2 < 4\} = (-2, 2)$; real numbers between -2 and 2
- $\{n \in \mathbb{Z} \mid 2 \mid n\} = \{l..., -4, -2, 0, 2, 4, l...\}$; even integers

5.1.3 Common Sets of Numbers

The following sets of numbers are standard throughout mathematics:

Symbol	Name	Description
$\mathbb{N}$	Natural numbers	$\{0, 1, 2, 3, l...\}$ (sometimes $\{1, 2, 3, l...\}$)
$\mathbb{Z}$	Integers	$\{l..., -2, -1, 0, 1, 2, l...\}$
$\mathbb{Q}$	Rational numbers	$\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
$\mathbb{R}$	Real numbers	All points on the number line
$\mathbb{C}$	Complex numbers	$\{a + bi \mid a, b \in \mathbb{R}\}$

Note the containment chain: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

5.1.4 Subsets and Power Sets

Definition 4
A is a **subset** of B, written $A \subseteq B$, if every element of A is also an element of B:

$$A \subseteq B \leftrightarrow \forall x, (x \in A \rightarrow x \in B)$$

A is a **proper subset** of B, written $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Example 3
- $\{1,3\} \subseteq \{1,2,3\}$ (subset)
- $\{1,3\} \subset \{1,2,3\}$ (proper subset)
- $\emptyset \subseteq A$ for every set A
- $A \subseteq A$ for every set A (a set is a subset of itself)

Important
To prove $A \subseteq B$: let x be an arbitrary element of A and show $x \in B$.

To prove $A = B$: prove $A \subseteq B$ and $B \subseteq A$.

Definition 5
The **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A:

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}$$

Example 4
If $A = \{1,2,3\}$, then:

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Theorem 1
If $|A| = n$ (i.e., A has n elements), then $|\mathcal{P}(A)| = 2^n$.

5.2 Properties of Sets

5.2.1 Set Operations

Definition 6
Let A and B be subsets of a **universal set** U.

- **Union:** $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$
- **Intersection:** $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$
- **Difference:** $A \setminus B = \{x \in U \mid x \in A \text{ and } x \notin B\}$
- **Complement:** $A^c = \{x \in U \mid x \notin A\}$

Example 5
Let $U = \{1,2,3,4,5,6,7,8\}$, $A = \{1,2,3,4\}$, $B = \{3,4,5,6\}$.
- $A \cup B = \{1,2,3,4,5,6\}$

- $A \cap B = \{3, 4\}$
- $A \setminus B = \{1, 2\}$
- $A^c = \{5, 6, 7, 8\}$

Definition 7
Sets A and B are **disjoint** if $A \cap B = \emptyset$.

5.2.2 Venn Diagrams

Venn diagrams represent sets as overlapping regions within a rectangle (the universal set). They are useful for visualising set relationships and verifying set identities.

Note
For two sets A and B, a Venn diagram has four regions:

- Inside A only: $A \setminus B$
- Inside B only: $B \setminus A$
- Inside both: $A \cap B$
- Outside both: $(A \cup B)^c$

5.2.3 Laws of Set Algebra

The laws of set algebra closely parallel the laws of logical equivalence from Chapter 1. This is not a coincidence; the correspondence is:

Logic	**Set Theory**
$\vee$ (disjunction)	$\cup$ (union)
$\wedge$ (conjunction)	$\cap$ (intersection)
$\neg$ (negation)	complement
T (tautology)	U (universal set)
F (contradiction)	$\emptyset$ (empty set)

Law	**Identity**
De Morgan's Laws	$(A \cup B)^c = A^c \cap B^c$
	$(A \cap B)^c = A^c \cup B^c$
Commutative Laws	$A \cup B = B \cup A$ and $A \cap B = B \cap A$
Associative Laws	$A \cup (B \cup C) = (A \cup B) \cup C$

	$A \cap (B \cap C) = (A \cap B) \cap C$
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity Laws	$A \cup \emptyset = A$ and $A \cap U = A$
Complement Laws	$A \cup A^c = U$ and $A \cap A^c = \emptyset$
Double Complement	$(A^c)^c = A$
Idempotent Laws	$A \cup A = A$ and $A \cap A = A$

Example 6
Prove: $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Both sides equal the set of elements in exactly one of A or B (the symmetric difference). We can verify using membership tables or by showing set containment in both directions.

5.2.4 Cartesian Products

Definition 8
The **ordered pair** (a, b) is distinct from (c, d) unless $a = c$ and $b = d$.

The **Cartesian product** of sets A and B is:

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

Example 7
If $A = \{1, 2\}$ and $B = \{x, y, z\}$:

$$A \times B = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}$$

Note $|A \times B| = |A| \cdot |B| = 2 \times 3 = 6$.

Remark
The Cartesian product $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the familiar xy-plane. More generally, $\mathbb{R}^n$ is n-dimensional Euclidean space.

5.3 Functions Defined on General Sets

5.3.1 Definition and Notation

Definition 9

A **function** f from a set A to a set B, written $f : A \to B$, is a rule that assigns to each element $x \in A$ exactly one element $f(x) \in B$.

- A is the **domain** of f
- B is the **codomain** of f
- $f(x)$ is the **image** of x under f
- The **range** (or **image**) of f is $\{f(x) \mid x \in A\} \subseteq B$

Important

A function must be:

- **Well-defined:** every element of the domain has an image
- **Single-valued:** each element of the domain has exactly one image

A relation that assigns multiple outputs to one input is not a function.

Example 8

- $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is a function (domain $\mathbb{R}$, codomain $\mathbb{R}$, range $[0, \infty)$)
- $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(n) = 2n + 1$ is a function
- The relation $h(x) = \pm\sqrt{x}$ on $\mathbb{R}$ is **not** a function (two outputs for $x > 0$)

5.3.2 Image and Preimage

Definition 10

Let $f : A \to B$.

- The **image of a set $S \subseteq A$** under f is $f(S) = \{f(x) \mid x \in S\}$
- The **preimage** (or **inverse image**) of a set $T \subseteq B$ is $f^{-1}(T) = \{x \in A \mid f(x) \in T\}$

Example 9

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$.

- $f(\{-2, -1, 0, 1, 2\}) = \{0, 1, 4\}$
- $f^{-1}(\{4\}) = \{-2, 2\}$
- $f^{-1}([-1, 4]) = [-2, 2]$
- $f^{-1}(\{-1\}) = \emptyset$ (no real number squares to -1)

5.4 One-to-One, Onto, and Inverse Functions

5.4.1 Injective Functions

Definition 11

A function $f : A \to B$ is **injective** (or **one-to-one**) if no two distinct elements of A map to the same element of B:

$$\forall x_1, x_2 \in A, \quad f(x_1) = f(x_2) \to x_1 = x_2$$

Equivalently (by contrapositive): $x_1 \neq x_2 \to f(x_1) \neq f(x_2)$.

Example 10

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 2$ is injective. (If $3x_1 + 2 = 3x_2 + 2$ then $x_1 = x_2$.)
- $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x^2$ is **not** injective. ($g(-1) = g(1) = 1$ but $-1 \neq 1$.)
- $h : \mathbb{Z} \to \mathbb{Z}$, $h(n) = 2n$ is injective. (If $2n_1 = 2n_2$ then $n_1 = n_2$.)

Note

To **prove** f is injective: assume $f(x_1) = f(x_2)$ and derive $x_1 = x_2$.

To **disprove** injectivity: find $x_1 \neq x_2$ with $f(x_1) = f(x_2)$.

5.4.2 Surjective Functions

Definition 12

A function $f : A \to B$ is **surjective** (or **onto**) if every element of B is the image of at least one element of A:

$$\forall y \in B, \exists x \in A \text{ such that } f(x) = y$$

Equivalently, the range of f equals the codomain: $f(A) = B$.

Example 11

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 2$ is surjective. (Given $y \in \mathbb{R}$, take $x = \frac{y-2}{3}$.)
- $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x^2$ is **not** surjective. (No $x \in \mathbb{R}$ satisfies $x^2 = -1$.)
- $h : \mathbb{Z} \to \mathbb{Z}$, $h(n) = 2n$ is **not** surjective. (The odd integer 1 has no preimage.)
- $h : \mathbb{Z} \to \{\text{even integers}\}$, $h(n) = 2n$ **is** surjective (with restricted codomain).

Note

To **prove** f is surjective: given an arbitrary $y \in B$, construct $x \in A$ with $f(x) = y$.

To **disprove** surjectivity: exhibit $y \in B$ with no $x \in A$ satisfying $f(x) = y$.

5.4.3 Bijective Functions

Definition 13
A function $f : A \to B$ is **bijective** (a **bijection** or **one-to-one correspondence**) if it is both injective and surjective.

Example 12
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 2$ is bijective (injective and surjective over $\mathbb{R}$)
- $f : \{1, 2, 3\} \to \{a, b, c\}$, $f(1) = a, f(2) = b, f(3) = c$ is bijective

Theorem 2
A function $f : A \to B$ is bijective if and only if it has an inverse function.

5.4.4 Inverse Functions

Definition 14
If $f : A \to B$ is bijective, its **inverse function** $f^{-1} : B \to A$ is defined by:

$$f^{-1}(y) = x \leftrightarrow f(x) = y$$

The inverse satisfies: $f^{-1}(f(x)) = x$ for all $x \in A$, and $f(f^{-1}(y)) = y$ for all $y \in B$.

Example 13
For $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 2$: solving $y = 3x + 2$ for x gives $f^{-1}(y) = \frac{y-2}{3}$.

Verify: $f^{-1}(f(x)) = f^{-1}(3x + 2) = \frac{3x+2-2}{3} = x$ ✓

Important
A function has an inverse if and only if it is bijective. This is why both injectivity and surjectivity matter; injectivity guarantees the inverse is well-defined (no two inputs share an output), and surjectivity guarantees the inverse is defined on all of B.

5.5 Composition of Functions

5.5.1 Definition and Examples

Definition 15
Let $f : A \to B$ and $g : B \to C$. The **composition** of g and f, written $g \circ f$ (read "g composed with f"), is the function $g \circ f : A \to C$ defined by:

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

Important
For $g \circ f$ to be defined, the codomain of f must equal (or be a subset of) the domain of g. Note also that $g \circ f$ applies f first, then g; the order matters.

Example 14
Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x + 1$.
- $(g \circ f)(x) = g(f(x)) = f(x) + 1 = x^2 + 1$
- $(f \circ g)(x) = f(g(x)) = (x + 1)^2 = x^2 + 2x + 1$

Since $g \circ f \neq f \circ g$, composition is generally **not commutative**.

5.5.2 Properties of Composition

Theorem 3
Composition of functions is **associative**:

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

whenever the compositions are defined.

Theorem 4
- The composition of two injective functions is injective
- The composition of two surjective functions is surjective
- The composition of two bijective functions is bijective

Proof
We prove the injective case. Let $f : A \to B$ and $g : B \to C$ both be injective.

Suppose $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then $g(f(x_1)) = g(f(x_2))$.

Since g is injective, $f(x_1) = f(x_2)$. Since f is injective, $x_1 = x_2$.

Therefore $g \circ f$ is injective. □

Theorem 5
If $f : A \to B$ is bijective, then $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$, where $\mathrm{id}_{A(x)} = x$ is the identity function on A.

5.6 Cardinalities

5.6.1 Finite and Infinite Sets

Definition 16
A set A is **finite** if $A = \emptyset$ or if A has exactly n elements for some positive integer n. In the latter case, the **cardinality** of A is n, written $|A| = n$.

A set that is not finite is **infinite**.

Example 15
- $|\{a, b, c\}| = 3$
- $|\emptyset| = 0$

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all infinite

5.6.2 Comparing Cardinalities

Definition 17
Two sets A and B have the **same cardinality**, written $|A| = |B|$, if there exists a bijection $f : A \to B$.

$|A| \leq |B|$ if there exists an injection $f : A \to B$.

$|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$.

Remark
For finite sets, this agrees with the usual notion of size. For infinite sets, this provides a precise way to compare "sizes" of infinite collections; with surprising results.

Example 16
The sets $\mathbb{N} = \{0, 1, 2, 3, l...\}$ and $E = \{0, 2, 4, 6, l...\}$ (even naturals) have the same cardinality. The bijection $f : \mathbb{N} \to E$ defined by $f(n) = 2n$ witnesses this.

This seems paradoxical; E is a proper subset of $\mathbb{N}$, yet $|E| = |\mathbb{N}|$. This is a characteristic property of infinite sets.

5.7 Countable and Uncountable Sets

5.7.1 Countably Infinite Sets

Definition 18
A set A is **countably infinite** if $|A| = |\mathbb{N}|$, i.e., if there is a bijection $f : \mathbb{N} \to A$.

A set is **countable** if it is finite or countably infinite. A set that is not countable is **uncountable**.

Theorem 6
The integers $\mathbb{Z}$ are countably infinite.

Proof
Define $f : \mathbb{N} \to \mathbb{Z}$ by:

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

This gives the enumeration $0, -1, 1, -2, 2, -3, 3, l...$, which is a bijection from $\mathbb{N}$ to $\mathbb{Z}$. □

Theorem 7
The rational numbers $\mathbb{Q}$ are countably infinite.

Proof
Arrange all positive rationals $\frac{p}{q}$ (in lowest terms) in an infinite grid indexed by (p, q). Traverse this grid diagonally to produce an enumeration of all positive rationals. Adding 0 and the negative rationals gives a bijection from $\mathbb{N}$ to $\mathbb{Q}$. □

Theorem 8
A countable union of countable sets is countable.

5.7.2 Uncountable Sets and Cantor's Theorem

Theorem 9 (Cantor's Theorem)
The set of real numbers $\mathbb{R}$ is uncountable. Moreover, $|\mathbb{R}| > |\mathbb{N}|$.

Proof
We prove $(0, 1) \subset \mathbb{R}$ is uncountable using **Cantor's diagonal argument**.

Suppose, for contradiction, that $(0, 1)$ is countable. Then its elements can be listed:

$$r_1 = 0.d_{11}d_{12}d_{13}...$$

$$r_2 = 0.d_{21}d_{22}d_{23}...$$

$$r_3 = 0.d_{31}d_{32}d_{33}...$$

$$\vdots$$

Define $x = 0.x_1x_2x_3l...$ where $x_n = 5$ if $d_{nn} \neq 5$, and $x_n = 6$ if $d_{nn} = 5$.

Then $x \in (0, 1)$, but $x \neq r_n$ for every n (they differ in the n-th decimal place). This contradicts our assumption that the list contains all elements of $(0, 1)$.

Therefore $(0, 1)$; and hence $\mathbb{R}$; is uncountable. □

Theorem 10 (Cantor's Power Set Theorem)
For any set A, $|A| < |\mathcal{P}(A)|$. In particular, no set can be placed in bijection with its own power set.

Remark
Cantor's theorems establish that there are infinitely many "sizes" of infinity:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < ...$$

The cardinality $|\mathbb{N}|$ is denoted $\aleph_0$ ("aleph-null"), and $|\mathbb{R}| = 2^{\aleph_0}$. Whether there is a cardinality strictly between $\aleph_0$ and $2^{\aleph_0}$; the **Continuum Hypothesis** cannot be resolved from the standard axioms of set theory.

6 Relations

Relations are a generalisation of functions. Whereas a function assigns to each input exactly one output, a relation between two sets merely specifies which pairs of elements are "related". Many fundamental mathematical structures — divisibility, congruence modulo n, set inclusion, and ordering — are most naturally expressed as relations. This chapter develops the theory of relations, culminating in two of the most important classes: equivalence relations (which generalise equality) and partial orders (which generalise $\leq$ on the integers).

In this chapter we study:

- **Relations on sets:** how to define and represent a relation between two sets
- **Properties of relations:** reflexivity, symmetry, antisymmetry, and transitivity
- **Equivalence relations:** relations that partition a set into disjoint classes
- **Partial orders:** relations that generalise the notion of ordering

6.1 Relations on Sets

A relation between two sets formalises the notion of a connection or association between elements. Unlike a function, a relation does not require every element of the domain to be associated with anything, and an element may be associated with multiple elements of the codomain.

6.1.1 Definition and Representation

Definition 1

Let A and B be sets. A **binary relation** R from A to B is a subset of the Cartesian product $A \times B$:

$$R \subseteq A \times B$$

If $(a, b) \in R$, we say that a is **related to** b by R, written aRb. If $(a, b) \notin R$, we write $a \not R b$.

A **relation on A** is a relation from A to A; that is, a subset of $A \times A$.

Example 1

Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$. Then $R = \{(1, a), (1, b), (3, a)\}$ is a relation from A to B. We have $1Ra$ and $3Ra$, but $2 \not R a$.

Example 2

The **divides** relation on $\mathbb{Z}^+$: define aRb if and only if $a \mid b$. Then:

- $2R6$ (since $2 \mid 6$)

- $3 R 12$ (since $3 \mid 12$)
- $5 \not R 7$ (since $5 \nmid 7$)

Example 3
The **less-than-or-equal** relation $\leq$ on $\mathbb{Z}$ is a relation on $\mathbb{Z}$: $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \leq b\}$.

6.1.2 Relations as Sets of Ordered Pairs

Since a relation is simply a set of ordered pairs, all set operations apply. The **domain** and **range** of a relation can be defined analogously to functions.

Definition 2
Let R be a relation from A to B.
- The **domain** of R is $\text{dom}(R) = \{a \in A \mid \exists b \in B, (a, b) \in R\}$
- The **range** of R is $\text{ran}(R) = \{b \in B \mid \exists a \in A, (a, b) \in R\}$
- The **inverse** of R is $R^{-1} = \{(b, a) \mid (a, b) \in R\} \subseteq B \times A$

Example 4
Let $R = \{(1, 2), (1, 4), (3, 2)\}$ on $A = \{1, 2, 3, 4\}$. Then:
- $\text{dom}(R) = \{1, 3\}$
- $\text{ran}(R) = \{2, 4\}$
- $R^{-1} = \{(2, 1), (4, 1), (2, 3)\}$

Remark
Every function $f : A \to B$ is also a relation from A to B; namely, $R_f = \{(a, f(a)) \mid a \in A\}$. Functions are therefore special relations in which every element of A appears exactly once as a first component.

6.1.3 Directed Graphs of Relations

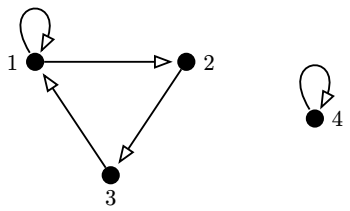
A relation on a finite set can be visualised as a **directed graph** (or **digraph**), which provides an intuitive picture of which elements are related.

Definition 3
Let R be a relation on a set A. The **directed graph** of R has:
- A **vertex** (node) for each element of A
- A **directed edge** (arrow) from a to b whenever $(a, b) \in R$

Note
- A **loop** at vertex a represents the pair $(a, a) \in R$.
- An arrow from a to b does not imply an arrow from b to a (unless $(b, a) \in R$ also holds).

Example 5
Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (1, 2), (2, 3), (3, 1), (4, 4)\}$. The directed graph has:

- Loops at 1 and 4
- Arrows: $1 \to 2$, $2 \to 3$, $3 \to 1$



Directed graph of $R = \{(1, 1), (1, 2), (2, 3), (3, 1), (4, 4)\}$ on $A = \{1, 2, 3, 4\}$. Vertices 1 and 4 carry self-loops; vertices 1, 2, 3 form a directed 3-cycle.

6.2 Reflexivity, Symmetry, and Transitivity

Relations on a set can possess several structural properties. These properties describe how elements relate to themselves (reflexivity), how the relation behaves when its pairs are reversed (symmetry and antisymmetry), and how it chains through intermediate elements (transitivity). Understanding these properties is the key to classifying relations into the important types studied later in this chapter.

6.2.1 Reflexive Relations

Definition 4
A relation R on a set A is **reflexive** if every element of A is related to itself:

$$\forall a \in A, \quad aRa$$

Equivalently, $(a, a) \in R$ for all $a \in A$.

Example 6

- The relation $\leq$ on $\mathbb{Z}$ is reflexive, since $a \leq a$ for all $a \in \mathbb{Z}$.
- The divides relation on $\mathbb{Z}^+$ is reflexive, since $a \mid a$ for all $a \in \mathbb{Z}^+$.
- Equality $=$ on any set is reflexive.
- The relation $<$ on $\mathbb{Z}$ is **not** reflexive, since $a < a$ is false for all a.

Note
In the directed graph of a reflexive relation, every vertex has a loop.

Definition 5
A relation R on a set A is **irreflexive** if no element is related to itself:

$$\forall a \in A, \quad (a, a) \notin R$$

Example 7
The strict order $<$ on $\mathbb{Z}$ is irreflexive. The relation "is a proper subset of" on sets is irreflexive.

6.2.2 Symmetric and Antisymmetric Relations

Definition 6
A relation R on a set A is **symmetric** if, whenever a is related to b, then b is also related to a:

$$\forall a, b \in A, \quad aRb \to bRa$$

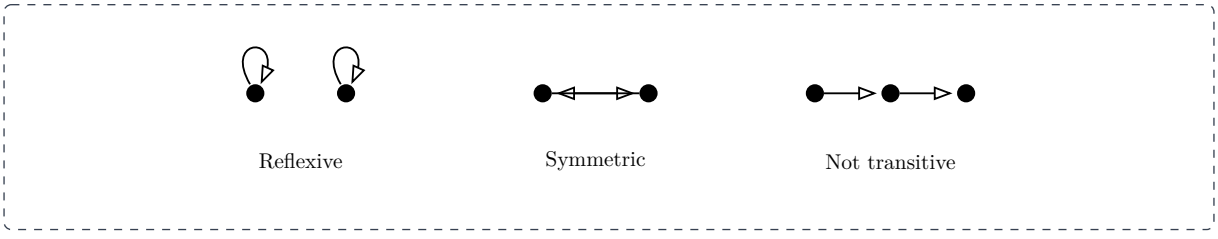
Definition 7
A relation R on a set A is **antisymmetric** if, whenever a is related to b and b is related to a, then a and b must be the same element:

$$\forall a, b \in A, \quad (aRb \land bRa) \to a = b$$

Equivalently: if $a \neq b$ and aRb, then $b \not R a$.

Example 8
- The relation $=$ on $\mathbb{Z}$ is both symmetric and antisymmetric.
- The relation "has the same parity as" on $\mathbb{Z}$ is symmetric (if a and b are both even, then so are b and a), but not antisymmetric.
- The divides relation on $\mathbb{Z}^+$ is antisymmetric: if $a \mid b$ and $b \mid a$, then $a = b$.
- The relation $\leq$ on $\mathbb{Z}$ is antisymmetric: if $a \leq b$ and $b \leq a$, then $a = b$.
- The strict order $<$ is antisymmetric (vacuously: there are no a, b with $a < b$ and $b < a$).

Note
Symmetric and antisymmetric are not opposites. A relation can be both (e.g., $=$), one but not the other, or neither (e.g., $R = \{(1,2),(2,1),(1,3)\}$ is neither symmetric nor antisymmetric on $\{1,2,3\}$).



Visual intuition for common relation properties on a finite set. Left: reflexive (every vertex has a loop). Middle: symmetric (arrows come in opposite-direction pairs). Right: not transitive example: $1 \to 2$ and $2 \to 3$ but no arrow $1 \to 3$.

6.2.3 Transitive Relations

Definition 8

A relation R on a set A is **transitive** if, whenever a is related to b and b is related to c, then a is related to c:

$$\forall a, b, c \in A, \quad (aRb \land bRc) \to aRc$$

Example 9

- The relation $\leq$ on $\mathbb{Z}$ is transitive: if $a \leq b$ and $b \leq c$, then $a \leq c$.
- The divides relation on $\mathbb{Z}^+$ is transitive: if $a \mid b$ and $b \mid c$, then $a \mid c$ (proved in Chapter 3).
- Congruence modulo n is transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
- The relation $R = \{(1,2),(2,3)\}$ on $\{1,2,3\}$ is **not** transitive, since $(1,2)$ and $(2,3)$ are in R but $(1,3)$ is not.

Note

To disprove transitivity, find a, b, c (not necessarily distinct) such that aRb and bRc but $a \not R c$.

Example 10

Determine which properties the following relation on $A = \{1,2,3,4\}$ satisfies:

$$R = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(3,4),(4,3)\}$$

- **Reflexive:** $(1,1),(2,2),(3,3),(4,4) \in R$. ✓
- **Symmetric:** $(1,2) \in R$ and $(2,1) \in R$; $(3,4) \in R$ and $(4,3) \in R$. ✓
- **Antisymmetric:** $(1,2)$ and $(2,1)$ are both in R but $1 \neq 2$. ✗
- **Transitive:** $(1,2)$ and $(2,1)$ are in R; is $(1,1)$ in R? Yes. $(3,4)$ and $(4,3)$ are in R; is $(3,3)$ in R? Yes. ✓

6.3 Equivalence Relations

An equivalence relation is one that behaves like equality. It captures the idea of two elements being "the same in some respect" without necessarily being identical. Congruence modulo n, having the same birthday, and being parallel lines are all equivalence relations.

6.3.1 Definition and Examples

Definition 9

A relation R on a set A is an **equivalence relation** if it is:

1. **Reflexive:** aRa for all $a \in A$
2. **Symmetric:** if aRb, then bRa
3. **Transitive:** if aRb and bRc, then aRc

Example 11

Congruence modulo n: Define aRb if and only if $n \mid (a-b)$ (equivalently, $a \equiv b \pmod{n}$). This is an equivalence relation on $\mathbb{Z}$ for any positive integer n:

- **Reflexive:** $n \mid (a-a) = 0$. ✓
- **Symmetric:** If $n \mid (a-b)$, then $n \mid (-(a-b)) = (b-a)$. ✓
- **Transitive:** If $n \mid (a-b)$ and $n \mid (b-c)$, then $n \mid ((a-b)+(b-c)) = (a-c)$. ✓

Example 12

Define a relation R on $\mathbb{Z}$ by: aRb if and only if $a-b$ is even (i.e., a and b have the same parity). This is an equivalence relation:

- **Reflexive:** $a-a=0$ is even. ✓
- **Symmetric:** If $a-b$ is even, then $b-a=-(a-b)$ is even. ✓
- **Transitive:** If $a-b$ and $b-c$ are even, then $a-c=(a-b)+(b-c)$ is even. ✓

Example 13

Define a relation on the set of all triangles: triangle T_1 is related to triangle T_2 if they are similar (same angles). This is an equivalence relation.

Example 14

The relation $<$ on $\mathbb{Z}$ is **not** an equivalence relation; it is not reflexive ($a < a$ is false) and not symmetric.

6.3.2 Equivalence Classes

When a set is equipped with an equivalence relation, its elements are naturally grouped according to which elements they are related to.

Definition 10

Let R be an equivalence relation on a set A, and let $a \in A$. The **equivalence class of a**, denoted $[a]$ (or $\overline{a}$), is the set of all elements of A that are related to a:

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

Any element $b \in [a]$ is called a **representative** of the class.

Example 15
Let R be congruence modulo 3 on $\mathbb{Z}$. The equivalence classes are:

$$[0] = \{..., -6, -3, 0, 3, 6, ...\} \quad \text{(multiples of 3)}$$
$$[1] = \{..., -5, -2, 1, 4, 7, ...\} \quad \text{(integers congruent to 1 mod 3)}$$
$$[2] = \{..., -4, -1, 2, 5, 8, ...\} \quad \text{(integers congruent to 2 mod 3)}$$

Note that $[0] = [3] = [6] = ...$ (every element of a class is a valid representative).

Theorem 1
Let R be an equivalence relation on A. For all $a, b \in A$:

1. $a \in [a]$ (every element belongs to its own equivalence class)
2. $[a] = [b]$ if and only if aRb
3. Either $[a] = [b]$ or $[a] \cap [b] = \emptyset$ (equivalence classes are either identical or disjoint)

Proof
(1) Since R is reflexive, aRa, so $a \in [a]$.

(2) ($\rightarrow$) Suppose $[a] = [b]$. Since $a \in [a] = [b]$, we have aRb.

($\leftarrow$) Suppose aRb. Let $x \in [a]$, so xRa. By transitivity, xRb, so $x \in [b]$. Hence $[a] \subseteq [b]$. By symmetry, bRa, so a symmetric argument gives $[b] \subseteq [a]$. Therefore $[a] = [b]$.

(3) Suppose $[a] \cap [b] \neq \emptyset$. Then there exists $c \in [a] \cap [b]$, so cRa and cRb. By symmetry, aRc, and by transitivity with cRb, we get aRb. By part (2), $[a] = [b]$.□

Important
Property (3) of the theorem above is the key property: equivalence classes either coincide or are completely disjoint. There is no partial overlap.

6.3.3 Partitions

Equivalence classes naturally divide a set into non-overlapping groups. The formal name for such a grouping is a partition.

Definition 11
A **partition** of a set A is a collection $\mathcal{P} = \{A_1, A_2, A_3, ...\}$ of non-empty subsets of A such that:

1. The subsets are **pairwise disjoint:** $A_i \cap A_j = \emptyset$ whenever $i \neq j$
2. Their **union covers A:** $A_1 \cup A_2 \cup A_3 \cup ... = A$

Each A_i is called a **block** (or **cell**) of the partition.

Example 16
Let $A = \{1, 2, 3, 4, 5, 6\}$. Then $\mathcal{P} = \{\{1, 3, 5\}, \{2, 4\}, \{6\}\}$ is a partition of A into three blocks.

Example 17
The equivalence classes of congruence modulo 3 on $\mathbb{Z}$ form a partition of $\mathbb{Z}$ into three blocks: $[0]$, $[1]$, and $[2]$.

6.3.4 The Connection Between Equivalence Relations and Partitions

Equivalence relations and partitions are two descriptions of the same phenomenon.

Theorem 2
Let R be an equivalence relation on a non-empty set A. Then the collection of all distinct equivalence classes of R forms a partition of A.

Conversely, every partition of A defines an equivalence relation on A: declare aRb if and only if a and b belong to the same block of the partition.

Proof
Equivalence relation → partition:

We must verify the two conditions for a partition.

- **Non-empty:** By reflexivity, $a \in [a]$, so each equivalence class is non-empty.
- **Pairwise disjoint:** By part (3) of the previous theorem, any two equivalence classes are either equal or disjoint.
- **Union covers A:** Since $a \in [a]$ for every $a \in A$, every element belongs to some class, so $A = \cup_{a \in A} [a]$.

Partition → equivalence relation:

Define aRb if and only if a and b are in the same block. Then:

- **Reflexive:** Every a is in the same block as itself.
- **Symmetric:** If a and b are in the same block, then b and a are in the same block.
- **Transitive:** If a and b are in the same block, and b and c are in the same block, then (since blocks are disjoint) all three are in the same block, so a and c are in the same block.

□

Example 18
The partition $\{\{1, 3, 5\}, \{2, 4, 6\}\}$ of $\{1, 2, 3, 4, 5, 6\}$ corresponds to the equivalence relation "has the same parity". Its equivalence classes are the odd integers and the even integers.

6.4 Partial Order Relations

A partial order generalises the familiar "less than or equal to" relation on the integers. The term "partial" reflects the fact that not every pair of elements need be comparable; some elements may be incomparable.

6.4.1 Definition and Examples

Definition 12

A relation R on a set A is a **partial order** if it is:

1. **Reflexive:** aRa for all $a \in A$
2. **Antisymmetric:** if aRb and bRa, then $a = b$
3. **Transitive:** if aRb and bRc, then aRc

A set A together with a partial order R is called a **partially ordered set** (or **poset**), written (A, R).

The partial order is commonly denoted $\preceq$; we write $a \preceq b$ for aRb.

Example 19

- $(\mathbb{Z}, \leq)$ is a poset. The relation $\leq$ is reflexive, antisymmetric, and transitive.
- $(\mathbb{Z}^+, |)$ is a poset: $a \mid a$; if $a \mid b$ and $b \mid a$ then $a = b$; if $a \mid b$ and $b \mid c$ then $a \mid c$.
- $(\mathcal{P}(A), \subseteq)$ is a poset for any set A: $B \subseteq B$; if $B \subseteq C$ and $C \subseteq B$ then $B = C$; if $B \subseteq C$ and $C \subseteq D$ then $B \subseteq D$.
- The strict less-than relation $<$ on $\mathbb{Z}$ is **not** a partial order, as it is not reflexive.

Definition 13

In a poset $(A, \preceq)$, two elements a and b are **comparable** if $a \preceq b$ or $b \preceq a$. Otherwise they are **incomparable**.

Example 20

In the poset $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$, the sets $\{1\}$ and $\{2\}$ are incomparable (neither is a subset of the other), while $\{1\} \subseteq \{1, 2\}$ so they are comparable.

Definition 14

Let $(A, \preceq)$ be a poset. An element $m \in A$ is:

- a **minimal element** if there is no $x \in A$ with $x \preceq m$ and $x \neq m$
- a **maximal element** if there is no $x \in A$ with $m \preceq x$ and $x \neq m$
- the **least element** (or **minimum**) if $m \preceq a$ for all $a \in A$
- the **greatest element** (or **maximum**) if $a \preceq m$ for all $a \in A$

Remark

A least element is always minimal, but a minimal element need not be a least element. A poset may have many minimal elements but at most one least element.

6.4.2 Hasse Diagrams

Hasse diagrams are a compact visual representation of a poset that eliminates the redundancy present in a full directed graph.

Definition 15

The **Hasse diagram** of a finite poset $(A, \preceq)$ is drawn as follows:

1. Represent each element as a vertex
2. If $a \preceq b$ and $a \neq b$ and there is no c with $a \preceq c \preceq b$ (i.e., b **covers** a), draw a line from a upward to b
3. Omit loops (reflexive pairs) and edges that are implied by transitivity

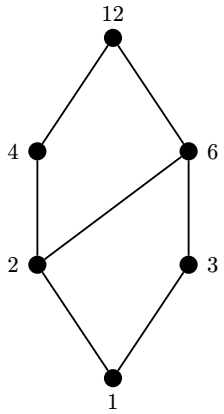
Example 21

The Hasse diagram for the poset $(\mathcal{P}(\{a, b, c\}), \subseteq)$ has $\emptyset$ at the bottom, the three singletons $\{a\}, \{b\}, \{c\}$ in the middle, the three two-element sets $\{a, b\}, \{a, c\}, \{b, c\}$ above them, and $\{a, b, c\}$ at the top. Each set is connected by a line to the sets that cover it (those obtained by adding exactly one element).

Example 22

The Hasse diagram of $\left(D_{\{12\}}, |\right)$, where $D_{\{12\}} = \{1, 2, 3, 4, 6, 12\}$ is the set of divisors of 12:

- 1 is at the bottom (the least element)
- 1 is covered by 2 and 3
- 2 is covered by 4 and 6
- 3 is covered by 6
- 4 and 6 are covered by 12
- 12 is at the top (the greatest element)



Hasse diagram of $(D_{12}, |)$, where $D_{12} = \{1, 2, 3, 4, 6, 12\}$. Upward position indicates divisibility; each edge represents a cover relation. The element 1 is the unique minimum and 12 the unique maximum.

Note
In a Hasse diagram, upward movement corresponds to the direction of the relation: $a \preceq b$ means b is higher than a in the diagram (or at the same level if $a = b$, but only the strict coverings are drawn).

6.4.3 Totally Ordered Sets

Definition 16
A partial order on A is a **total order** (or **linear order**) if every pair of elements is comparable:

$$\forall a, b \in A, \quad a \preceq b \quad \text{or} \quad b \preceq a$$

A set with a total order is called a **totally ordered set** (or **chain**).

Example 23
- $(\mathbb{Z}, \leq)$ is totally ordered: for any two integers a and b, either $a \leq b$ or $b \leq a$.
- $(\mathbb{Q}, \leq)$ and $(\mathbb{R}, \leq)$ are totally ordered.
- $(\mathcal{P}(\{1,2\}), \subseteq)$ is **not** totally ordered: $\{1\}$ and $\{2\}$ are incomparable.
- $\left(D_{\{12\}}, |\right)$ is **not** totally ordered: 4 and 6 are incomparable (neither divides the other).

Theorem 3
Every finite totally ordered set has a least element and a greatest element.

Remark
Total orders arise naturally in the context of sorting algorithms and comparison-based data structures, where any two elements must be comparable. Partial orders arise in contexts such as task scheduling (some tasks must precede others, but many are independent), compiler optimisation, and lattice theory in algebra.

7 Algebraic Structures

The integers, rationals, reals, and complex numbers all support arithmetic with rich structural properties that can be studied in the abstract. By identifying the essential axioms behind operations, abstract algebra yields general theorems applicable simultaneously to all structures satisfying those axioms. This chapter introduces two fundamental algebraic structures: **groups**, which capture the notion of a set with a single associative operation admitting an identity and inverses; and **fields**, which generalise the arithmetic of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ by requiring two compatible operations linked by distributivity.

In this chapter we study:

- **Groups:** sets equipped with one binary operation satisfying closure, associativity, identity, and inverses

- **Fields:** sets with two binary operations linked by distributivity, generalising the arithmetic of familiar number systems

7.1 Groups

A group is the simplest and most fundamental algebraic structure. The integers under addition, the non-zero rationals under multiplication, and the integers modulo n under addition all form groups. Abstracting their common features reveals properties that hold for all groups simultaneously.

7.1.1 Definition and Examples

Definition 1

A **group** is an ordered pair $(G, *)$ where G is a non-empty set and $*$ is a binary operation on G satisfying the following four axioms:

1. **Closure:** For all $a, b \in G$, $a * b \in G$.
2. **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
3. **Identity:** There exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
4. **Inverses:** For each $a \in G$, there exists $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e.$$

If additionally $a * b = b * a$ for all $a, b \in G$, the group is called **abelian** (or **commutative**).

Note

Closure is sometimes taken as implicit in the requirement that $*$ is a binary operation on G, since a binary operation on G maps $G \times G$ into G by definition. Many texts therefore list only three group axioms: associativity, identity, and inverses.

Example 1

Integers under addition. $(\mathbb{Z}, +)$ is an abelian group. The identity is 0, since $a + 0 = 0 + a = a$. The inverse of a is $-a$, since $a + (-a) = 0$. Closure and associativity are standard properties of integer arithmetic.

Example 2

Non-zero rationals under multiplication. $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group. The identity is 1, and the inverse of $a \neq 0$ is $\frac{1}{a}$, which belongs to $\mathbb{Q} \setminus \{0\}$. The set $\mathbb{Q}$ itself does not form a group under multiplication because 0 has no multiplicative inverse.

Example 3

Integers modulo n. Let $n \geq 2$ be a positive integer. The set $\mathbb{Z}_n = \{[0], [1], ..., [n - 1]\}$ of residue classes modulo n, equipped with addition modulo n (denoted $+_n$), is

an abelian group. The identity is $[0]$, and the inverse of $[a]$ is $[n-a]$, since $[a] +_n [n-a] = [n] = [0]$.

Example 4
The real numbers $(\mathbb{R}, +)$ and the complex numbers $(\mathbb{C}, +)$ are abelian groups under addition, with identity 0 and inverse $-a$.

Example 5
The trivial group. The set $\{e\}$ with the single operation $e * e = e$ is a group, called the **trivial group**. It is the unique group of order 1.

Example 6
Non-examples.

- $(\mathbb{Z}, \times)$ is not a group: while 1 serves as an identity, an integer such as 2 has no multiplicative inverse in $\mathbb{Z}$.
- $(\mathbb{N}, +)$ is not a group: the identity 0 exists, but a positive integer a has no additive inverse in $\mathbb{N}$ (since $-a \notin \mathbb{N}$).

For finite groups, the binary operation can be displayed compactly in a table.

Definition 2
A **Cayley table** (or **operation table**) for a finite group $(G, *)$ is an $n \times n$ table, where $n = |G|$, whose rows and columns are each indexed by the elements of G in some fixed order. The entry in the row labelled a and the column labelled b is $a * b$.

Example 7
The Cayley table for $(\mathbb{Z}_4, +_4)$:

$+_4$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Note
In a group's Cayley table, every element appears exactly once in each row and exactly once in each column. This is the **Latin square property**, and it follows from the cancellation laws proved in the next section.

7.1.2 Elementary Properties of Groups

Several important properties follow directly from the group axioms.

Theorem 1 (Uniqueness of the identity)
In any group $(G, *)$, the identity element is unique.

Proof
Suppose e and e' are both identity elements of G. Then:

$$e = e * e' = e',$$

where the first equality uses e' as an identity applied to e, and the second uses e as an identity applied to e'. Hence $e = e'$. □

Theorem 2 (Uniqueness of inverses)
In any group $(G, *)$, every element has a unique inverse.

Proof
Let $a \in G$ and suppose $b, c \in G$ both satisfy $a * b = b * a = e$ and $a * c = c * a = e$. Then:

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c,$$

where associativity is used at the third step. Hence $b = c$. □

Theorem 3 (Cancellation laws)
Let $(G, *)$ be a group and let $a, b, c \in G$.

- **Left cancellation:** If $a * b = a * c$, then $b = c$.
- **Right cancellation:** If $b * a = c * a$, then $b = c$.

Proof
We prove left cancellation; the proof of right cancellation is analogous. Suppose $a * b = a * c$. Multiplying both sides on the left by a^{-1}:

$$a^{-1} * (a * b) = a^{-1} * (a * c).$$

By associativity, $(a^{-1} * a) * b = (a^{-1} * a) * c$, so $e * b = e * c$, and therefore $b = c$. □

Theorem 4
In any group $(G, *)$, for all $a, b \in G$:
1. $(a^{-1})^{-1} = a$.
2. $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof
(1) Since $a * a^{-1} = a^{-1} * a = e$, the element a satisfies the defining property of the inverse of a^{-1}. By the uniqueness of inverses, $(a^{-1})^{-1} = a$.

(2) We verify that $b^{-1} * a^{-1}$ is the inverse of $a * b$ by checking both products equal e:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e,$$

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e.$$

By the uniqueness of inverses, $(a * b)^{-1} = b^{-1} * a^{-1}$. □

Remark
The formula $(a * b)^{-1} = b^{-1} * a^{-1}$ is sometimes called the **socks-and-shoes property**: to undo the combined effect of two operations, reverse the order. This reversal is necessary in non-abelian groups where $a * b \neq b * a$ in general.

7.1.3 Subgroups
A subgroup is a subset of a group that is itself a group under the same operation.

Definition 3
Let $(G, *)$ be a group. A non-empty subset $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if $(H, *)$ is a group under the same operation. This requires:
1. **Closure:** For all $a, b \in H$, $a * b \in H$.
2. **Identity:** The identity e of G belongs to H.
3. **Inverses:** For all $a \in H$, $a^{-1} \in H$.

Associativity is inherited automatically from G.

Note
The identity condition is implied by non-emptiness and closure under inverses: for any $a \in H$, we have $a^{-1} \in H$, and then $e = a * a^{-1} \in H$ by closure. Many texts therefore state the subgroup conditions as: non-emptiness, closure under the operation, and closure under inverses.

Example 8
Every group G has at least two subgroups:

- The **trivial subgroup** $\{e\}$, containing only the identity.
- G itself.

These are the **improper** subgroups of G. A subgroup H with $\{e\} \subset H \subset G$ is called a **proper** subgroup.

Example 9
Even integers. $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$:
- **Closure:** the sum of two even integers is even.
- **Identity:** $0 \in 2\mathbb{Z}$.
- **Inverses:** if $a \in 2\mathbb{Z}$ then $-a \in 2\mathbb{Z}$.

Example 10
$(\{1, -1\}, \times)$ is a subgroup of $(\mathbb{Q} \setminus \{0\}, \times)$:
- **Closure:** $1 \times 1 = 1$, $1 \times (-1) = -1$, $(-1) \times (-1) = 1$.
- **Identity:** $1 \in \{1, -1\}$.
- **Inverses:** $1^{-1} = 1$ and $(-1)^{-1} = -1$.

The following criterion gives a concise way to verify that a subset is a subgroup.

Theorem 5 (Subgroup Test)
Let $(G, *)$ be a group and let H be a non-empty subset of G. Then H is a subgroup of G if and only if

$$\forall a, b \in H, \quad a * b^{-1} \in H.$$

Proof
($\rightarrow$) If H is a subgroup and $a, b \in H$, then $b^{-1} \in H$ by closure under inverses, and $a * b^{-1} \in H$ by closure under the operation.

($\leftarrow$) Suppose H is non-empty and $a * b^{-1} \in H$ for all $a, b \in H$.
- **Identity:** Since H is non-empty, choose any $a \in H$. Setting $b = a$ gives $a * a^{-1} = e \in H$.
- **Inverses:** For any $a \in H$, we have $e \in H$. Applying the hypothesis with first element e and second element a: $e * a^{-1} = a^{-1} \in H$.
- **Closure:** For any $a, b \in H$, the previous step gives $b^{-1} \in H$. Applying the hypothesis with a and b^{-1}: $a * \left(b^{-1}\right)^{-1} = a * b \in H$.

□

Definition 4
The **order** of a group G, written $|G|$, is the cardinality of the set G. A group is **finite** if $|G|$ is finite, and **infinite** otherwise.

Example 11
$|\mathbb{Z}_n| = n$ for all $n \geq 1$. The groups $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all infinite.

7.2 Fields

The integers, rationals, reals, and complex numbers all support both addition and multiplication, with the two operations linked by distributivity. A field is the abstract structure capturing exactly these properties.

7.2.1 Definition and Examples

Definition 5
A **field** is a set F together with two binary operations $+$ (addition) and $\times$ (multiplication) satisfying:

1. $(F, +)$ is an abelian group with identity element 0 (the **additive identity**).
2. $(F \setminus \{0\}, \times)$ is an abelian group with identity element 1 (the **multiplicative identity**).
3. **Distributivity:** For all $a, b, c \in F$,

$$a \times (b + c) = (a \times b) + (a \times c).$$

The additive inverse of a is written $-a$; the multiplicative inverse of a non-zero a is written a^{-1} (or $\frac{1}{a}$).

Remark
A field can equivalently be described as a commutative ring with unity (satisfying $1 \neq 0$) in which every non-zero element has a multiplicative inverse.

Example 12
Standard infinite fields.

- $(\mathbb{Q}, +, \times)$: the rational numbers form a field.
- $(\mathbb{R}, +, \times)$: the real numbers form a field.
- $(\mathbb{C}, +, \times)$: the complex numbers form a field.

In each case, the field axioms are the familiar arithmetic properties of those number systems.

Example 13
Finite fields $\mathbb{F}_p$. Let p be a prime. The set $\mathbb{Z}_p = \{[0], [1], ..., [p-1]\}$ with addition $+_p$ and multiplication $\times_p$ modulo p forms a field, denoted $\mathbb{F}_p$:

- $(\mathbb{Z}_p, +_p)$ is an abelian group (shown in the Groups section above).
- Every non-zero $[a]$ has a multiplicative inverse modulo p: since p is prime and $1 \leq a \leq p-1$, we have $\gcd(a, p) = 1$. By Bézout's identity, there exist integers u, v with $au + pv = 1$, so $[a] \times_p [u] = [1]$.
- Distributivity holds because it holds in $\mathbb{Z}$.

For example, in $\mathbb{F}_5$: $[2]^{-1} = [3]$ since $2 \times 3 = 6 \equiv 1 \pmod 5$, and $[4]^{-1} = [4]$ since $4 \times 4 = 16 \equiv 1 \pmod 5$.

Example 14
Non-examples.

- $(\mathbb{Z}, +, \times)$: the integers are not a field, since 2 has no multiplicative inverse in $\mathbb{Z}$ (as $\frac{1}{2} \notin \mathbb{Z}$).
- $(\mathbb{Z}_n, +_n, \times_n)$ for composite n: not a field. In $\mathbb{Z}_6$, for instance, $[2] \times_6 [3] = [0]$ while $[2] \neq [0]$ and $[3] \neq [0]$. A product of two non-zero elements equals zero, which cannot occur in a field (as proved in the next section).

7.2.2 Properties of Fields

The field axioms, together with the group properties established earlier, imply several fundamental arithmetic identities.

Theorem 6
Let F be a field. For all $a \in F$:

$$0 \times a = a \times 0 = 0.$$

Proof
Using $0 = 0 + 0$ and the distributive law:

$$0 \times a = (0 + 0) \times a = (0 \times a) + (0 \times a).$$

Adding $-(0 \times a)$ to both sides yields $0 = 0 \times a$. The identity $a \times 0 = 0$ follows by commutativity of multiplication in a field. □

Theorem 7
Let F be a field. For all $a \in F$:

$$(-1) \times a = -a.$$

Proof
Compute:

$$a + (-1) \times a = (1 \times a) + ((-1) \times a) = (1 + (-1)) \times a = 0 \times a = 0.$$

So $(-1) \times a$ is the additive inverse of a. By the uniqueness of additive inverses in $(F, +)$, we have $(-1) \times a = -a$. □

Theorem 8 (No zero divisors)
Let F be a field. If $a, b \in F$ and $a \times b = 0$, then $a = 0$ or $b = 0$.

Proof
Suppose $a \times b = 0$ and $a \neq 0$. Since F is a field, a^{-1} exists. Multiplying both sides on the left by a^{-1}:

$$b = 1 \times b = (a^{-1} \times a) \times b = a^{-1} \times (a \times b) = a^{-1} \times 0 = 0,$$

where the last step applies the previous theorem with a^{-1} in place of a. Hence $b = 0$. □

Theorem 9
Let F be a field. For all $a, b \in F$:

$$(-a) \times (-b) = a \times b.$$

Proof
Using $-a = (-1) \times a$ and $-b = (-1) \times b$:

$$(-a) \times (-b) = ((-1) \times a) \times ((-1) \times b) = ((-1) \times (-1)) \times (a \times b).$$

It remains to show $(-1) \times (-1) = 1$. By the previous theorem with $a = -1$, we have $(-1) \times (-1) = -(-1)$. Since $(-1) + 1 = 0$, the additive inverse of -1 is 1, so $-(-1) = 1$. Therefore $(-a) \times (-b) = a \times b$. □

Definition 6
The **characteristic** of a field F, written $\text{char}(F)$, is the smallest positive integer n such that the n-fold sum of 1 with itself equals 0:

$$1 + 1 + \cdots + 1 = 0$$

(with n terms on the left-hand side). If no such n exists, the characteristic is defined to be 0.

Example 15

- $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$: no finite sum of copies of 1 is zero in any of these fields.
- $\text{char}(\mathbb{F}_p) = p$ for any prime p: in $\mathbb{Z}_p$, the p-fold sum $[1] + [1] + \cdots + [1] = [p] = [0]$, and no smaller positive number of terms gives $[0]$, since p is prime.

Theorem 10

The characteristic of any field is either 0 or a prime number.

Proof

Suppose $\text{char}(F) = p > 0$ and write $p = r \cdot s$ with $r, s \geq 1$. Let u denote the r-fold sum of 1 with itself, and v the s-fold sum. By repeated application of distributivity, $u \times v$ equals the $(r \cdot s)$-fold sum of 1 with itself, which is the p-fold sum and therefore equals 0. By the no-zero-divisors theorem, $u = 0$ or $v = 0$. By the minimality of p as the characteristic, the r-fold sum is 0 only if $r \geq p$, and the s-fold sum is 0 only if $s \geq p$. Since $r \cdot s = p$ and $r, s \geq 1$, this forces $r = 1$ or $s = 1$. Hence p has no non-trivial factorisation and is prime. □

Remark

Fields provide the natural setting for linear algebra: a vector space is defined over a field, and all of matrix theory, including determinants, eigenvalues, and linear systems, rests on field arithmetic. Polynomial arithmetic over a field F (the polynomial ring $F[x]$) admits a Euclidean division algorithm analogous to that for the integers, from which notions of greatest common divisors and irreducible polynomials follow.

The finite fields $\mathbb{F}_p$ and their extensions $\mathbb{F}_{p^k}$ are of central importance in cryptography and coding theory. Public-key cryptographic schemes, including elliptic curve cryptography, perform arithmetic in $\mathbb{F}_p$ or $\mathbb{F}_{2^k}$. Error-correcting codes such as Reed-Solomon codes, used in QR codes and storage devices, are constructed over finite fields and exploit their algebraic structure to detect and correct transmission errors.

8 Counting and Probability

Counting is concerned with determining the number of ways objects can be arranged, selected, or distributed. Rather than listing every possibility, systematic principles allow the total count to be computed directly. This chapter develops the core tools of combinatorics: the addition and multiplication principles, permutations, combinations, selections with repetition, and the binomial theorem. It then introduces the foundations of probability, the inclusion-exclusion principle, and the pigeonhole principle.

In this chapter we study:

- **Introduction to counting:** the addition and multiplication principles, permutations, and combinations
- **Counting selections:** selections with repetition and arrangements with repeated elements
- **Probability:** sample spaces, events, and basic probability rules
- **Binomial coefficients:** Pascal's triangle and the Binomial Theorem
- **Inclusion-exclusion:** counting unions of overlapping sets
- **The Pigeonhole Principle:** a deceptively simple result with powerful consequences

8.1 Introduction to Counting

The goal of combinatorics is to count the elements of a finite set without listing them all. The two most fundamental tools are the addition principle and the multiplication principle, from which all other counting methods are built.

Important

Method Selector (Counting): Use this quick guide before choosing a formula:

- **Addition principle** $(+)$: when you have mutually exclusive cases ("or").
- **Multiplication principle** $(\times)$: when a process has sequential independent steps ("and").
- **Permutations** $P(n,r)$: when order matters, without repetition.
- **Combinations** $\binom{n}{r}$: when order does not matter, without repetition.
- **Selections with repetition** $\binom{n+r-1}{r}$: when order does not matter, with repetition.
- **Arrangements with repeated elements** $\frac{n!}{n_{1!}n_{2!}\cdots n_{k!}}$: when items are not all distinct.

8.1.1 The Addition and Multiplication Principles

Theorem 1 (Addition Principle)

If A and B are disjoint finite sets, then $|A \cup B| = |A| + |B|$.

More generally, if $A_1, A_2, ..., A_k$ are pairwise disjoint finite sets, then

$$|A_1 \cup A_2 \cup ... \cup A_k| = |A_1| + |A_2| + ... + |A_k|.$$

Remark

The addition principle applies when a task can be performed in one of several mutually exclusive ways: the total number of ways equals the sum of the counts for each case.

Theorem 2 (Multiplication Principle)

If a procedure consists of k sequential steps, where step i can be performed in n_i ways regardless of how earlier steps were performed, then the total number of ways to perform the procedure is

$$n_1 \times n_2 \times \cdots \times n_k.$$

Equivalently, if $A_1, A_2, ..., A_k$ are finite sets, then $|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \times |A_2| \times \cdots \times |A_k|$.

Example 1
A student ID number consists of two uppercase letters followed by four digits. How many distinct ID numbers are possible?

There are 26 choices for each letter and 10 choices for each digit. By the multiplication principle:

$$26 \times 26 \times 10 \times 10 \times 10 \times 10 = 26^2 \times 10^4 = 6\{,\}760\{,\}000.$$

Example 2
How many integers between 1 and 100 (inclusive) are divisible by 3 or by 5?

Let A = multiples of 3 in $[1, 100]$ and B = multiples of 5 in $[1, 100]$. Then $|A| = \left\lfloor \frac{100}{3} \right\rfloor = 33$ and $|B| = \left\lfloor \frac{100}{5} \right\rfloor = 20$. Since A and B are not disjoint (e.g., 15 belongs to both), we must use inclusion-exclusion (see Section 7.5). But the addition principle alone does not apply here.

8.1.2 Permutations

Definition 1
A **permutation** of a set of objects is an ordered arrangement of those objects. The number of permutations of n distinct objects is

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1.$$

By convention, $0! = 1$.

Definition 2
A **permutation of n objects taken r at a time** is an ordered selection of r objects from n distinct objects, without repetition. The number of such permutations is denoted $P(n, r)$:

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}.$$

Proof
By the multiplication principle: there are n choices for the first position, $n-1$ for the second, and so on down to $n-r+1$ for the rth position. The product telescopes to $\frac{n!}{(n-r)!}$ upon multiplying numerator and denominator by $(n-r)!$. □

Example 3
In how many ways can a president, vice-president, and treasurer be chosen from a club of 15 members?

The three positions are distinct and no member can hold two, so the answer is

$$P(15,3) = 15 \times 14 \times 13 = 2730.$$

Example 4
How many four-letter strings can be formed from the letters $\{a, b, c, d, e, f\}$ with no letter repeated?

$$P(6,4) = 6 \times 5 \times 4 \times 3 = 360.$$

8.1.3 Combinations

Definition 3
A **combination of n objects taken r at a time** is an unordered selection of r objects from n distinct objects. The number of such combinations is the **binomial coefficient**

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

for $0 \le r \le n$. We define $\binom{n}{r} = 0$ if $r > n$ or $r < 0$.

Proof
Each combination of r objects can be arranged in $r!$ ways (permutations of those r objects). Since every ordered arrangement arises from exactly one combination, $\binom{n}{r} \times r! = P(n,r)$. Solving gives $\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$. □

Example 5
How many 5-card hands can be dealt from a standard 52-card deck?

$$\binom{52}{5} = \frac{52!}{5! \times 47!} = \frac{52 \times 51 \times 50 \times 49 \times 48}{5 \times 4 \times 3 \times 2 \times 1} = 2\{,\}598\{,\}960.$$

Example 6
A committee of 4 is to be chosen from 10 people. How many committees contain at least one specific person p?

Method: Total committees minus those containing no specific person:

$$\binom{10}{4} - \binom{9}{4} = 210 - 126 = 84.$$

Alternatively: committees containing p require choosing 3 more from the remaining 9: $\binom{9}{3} = 84$. ✓

The following properties follow directly from the definition.

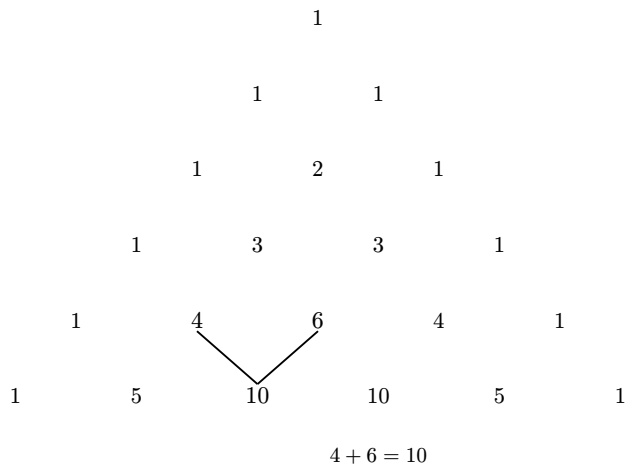
Theorem 3
For integers $0 \le r \le n$:
1. $\binom{n}{0} = \binom{n}{n} = 1$
2. $\binom{n}{1} = \binom{n}{n-1} = n$
3. $\binom{n}{r} = \binom{n}{n-r}$ **(symmetry)**
4. $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ **(Pascal's identity)**

Proof
Properties (1)–(3) follow by direct substitution into the formula.

(4) Combinatorial proof of Pascal's identity: Consider a set S of n objects and fix one element $x \in S$. Every r-element subset of S either contains x or does not.

- Subsets **containing** x: choose the remaining $r-1$ from the $n-1$ objects other than x: $\binom{n-1}{r-1}$ subsets.
- Subsets **not containing** x: choose all r from the $n-1$ objects other than x: $\binom{n-1}{r}$ subsets.

Since these cases partition all r-subsets of S, the total is $\binom{n-1}{r-1} + \binom{n-1}{r}$. □



Pascal triangle motivation for $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. Here $\binom{5}{2} = 10$ is obtained by adding the two entries above it: $\binom{4}{1} = 4$ and $\binom{4}{2} = 6$.

8.2 Counting Selections

Not every counting problem involves distinct objects or no repetition. This section considers selections where elements may be repeated, and arrangements of objects that are not all distinct.

8.2.1 Selections with Repetition

Theorem 4

The number of ways to select r objects from n distinct types, where repetition is allowed and order does not matter, is

$$\binom{n+r-1}{r}.$$

Proof

Stars and bars: represent a selection as a sequence of r stars (objects) divided into n groups (types) by $n-1$ bars. The total length of the sequence is $r+(n-1)$; choosing which r positions are stars determines the selection. Hence the count is $\binom{r+n-1}{r}$. □

Example 7

How many ways can 10 identical chocolates be distributed among 4 children (where some children may receive none)?

Here $r = 10$ chocolates are selected from $n = 4$ types (one per child) with repetition allowed:

$$\binom{10+4-1}{10} = \binom{13}{10} = \binom{13}{3} = 286.$$

Example 8

How many solutions in non-negative integers does $x_1 + x_2 + x_3 = 12$ have?

Each solution assigns 12 to three "types" (variables) with repetition: $\binom{12+3-1}{12} = \binom{14}{12} = \binom{14}{2} = 91$.

Remark

If repetition is allowed and **order matters**, the number of r-length sequences from n types is simply n^r (by the multiplication principle: n choices at each of r positions).

8.2.2 Arrangements with Repeated Elements

Theorem 5

The number of distinct arrangements of n objects in which object type i appears n_i times, where $n_1 + n_2 + \ldots + n_k = n$, is the **multinomial coefficient**

$$\frac{n!}{n_{1!}n_{2!}\cdots n_{k!}}.$$

Proof
There are $n!$ arrangements of all n objects if they were all distinct. Since objects within type i are identical, we divide by $n_{i!}$ for each type to remove the over-counting. This gives $\frac{n!}{n_{1!}n_{2!}\cdots n_{k!}}$. □

Example 9
How many distinct arrangements are there of the letters in MISSISSIPPI?

The letters are: M (once), I (4 times), S (4 times), P (twice). Total letters: $n = 11$.

$$\frac{11!}{1! \times 4! \times 4! \times 2!} = \frac{39916800}{1 \times 24 \times 24 \times 2} = 34650.$$

Example 10
How many arrangements of AABBBC are there?

$$\frac{6!}{2! \times 3! \times 1!} = \frac{720}{2 \times 6 \times 1} = 60.$$

8.3 Introduction to Probability

Probability provides a mathematical framework for quantifying uncertainty and analysing the outcomes of random experiments.

8.3.1 Sample Spaces and Events

Definition 4
A **random experiment** is a procedure whose outcome cannot be predicted with certainty.

The **sample space** S of an experiment is the set of all possible outcomes.

An **event** E is any subset of the sample space. The **complement** of E, written E^c, is the set of all outcomes not in E. Events E and F are **mutually exclusive** if $E \cap F = \emptyset$.

Example 11
Rolling a fair six-sided die: The sample space is $S = \{1, 2, 3, 4, 5, 6\}$. The event "rolling an even number" is $E = \{2, 4, 6\}$, with complement $E^c = \{1, 3, 5\}$.

Example 12
Flipping two fair coins: The sample space is $S = \{HH, HT, TH, TT\}$. The event "at least one head" is $E = \{HH, HT, TH\}$.

8.3.2 Basic Probability Rules

Definition 5
For a finite **uniform sample space** (all outcomes equally likely), the **probability** of an event E is

$$P(E) = |E| \frac{|}{|} S|.$$

Theorem 6 (Probability Axioms (Kolmogorov))
A probability function P on a sample space S satisfies:
1. $P(E) \geq 0$ for every event E
2. $P(S) = 1$
3. If $E_1, E_2, \ldots$ are pairwise mutually exclusive events, then

$$P(E_1 \cup E_2 \cup \ldots) = P(E_1) + P(E_2) + \ldots$$

The following rules are consequences of the axioms.

Theorem 7
For any events E and F in a sample space S:
1. **Complement rule:** $P(E^c) = 1 - P(E)$
2. **Inclusion-exclusion:** $P(E \cup F) = P(E) + P(F) - P(E \cap F)$
3. **Monotonicity:** If $E \subseteq F$, then $P(E) \leq P(F)$

Proof
(1) Since E and E^c are mutually exclusive and $E \cup E^c = S$, axioms (2) and (3) give $P(E) + P(E^c) = 1$.

(2) Write $E \cup F = E \cup (F \setminus E)$, where E and $F \setminus E$ are mutually exclusive. By axiom (3), $P(E \cup F) = P(E) + P(F \setminus E)$. Since $F = (E \cap F) \cup (F \setminus E)$, similarly $P(F) = P(E \cap F) + P(F \setminus E)$. Rearranging gives $P(F \setminus E) = P(F) - P(E \cap F)$, and substituting yields the result.

(3) Write $F = E \cup (F \setminus E)$ with the two sets disjoint. Then $P(F) = P(E) + P(F \setminus E) \geq P(E)$. □

Definition 6
The **conditional probability** of E given F, written $P(E \mid F)$, is defined for $P(F) > 0$ by

$$P(E \mid F) = \frac{P(E \cap F)}{P(F)}.$$

Events E and F are **independent** if $P(E \cap F) = P(E)P(F)$, or equivalently (when $P(F) > 0$) if $P(E \mid F) = P(E)$.

Example 13
A card is drawn at random from a standard 52-card deck. Given that the card is a heart, what is the probability it is a face card?

Let E = face card and F = heart. Then $|E \cap F| = 3$ (J, Q, K of hearts) and $|F| = 13$:

$$P(E \mid F) = \frac{P(E \cap F)}{P(F)} = \frac{\frac{3}{52}}{\frac{13}{52}} = \frac{3}{13}.$$

8.4 Binomial Coefficients

The binomial coefficients $\binom{n}{r}$ arise naturally in expanding powers of sums, and their properties are captured elegantly by Pascal's triangle and the Binomial Theorem.

8.4.1 Pascal's Triangle

Pascal's triangle is an infinite triangular array in which the entry in row n and position k (counting from $n = 0$, $k = 0$) is $\binom{n}{k}$:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
\end{array}$$

Each interior entry equals the sum of the two entries directly above it (Pascal's identity: $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$). The edges are all 1s ($\binom{n}{0} = \binom{n}{n} = 1$).

Note
The sum of row n is $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, which counts the total number of subsets of an n-element set.

8.4.2 The Binomial Theorem

Theorem 8 (Binomial Theorem)
For any real numbers a and b and any non-negative integer n,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Proof
Expand $(a+b)^n = (a+b)(a+b)\cdots(a+b)$ (n factors). Each term in the expansion is obtained by choosing b from k of the n factors and a from the remaining $n-k$. The number of ways to choose which k factors contribute b is $\binom{n}{k}$. Summing over $k = 0, 1, \ldots, n$ gives the result. □

Example 14
$(x+y)^4 = \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$.

Theorem 9
The following identities follow from the Binomial Theorem.

1. Setting $a = b = 1$: $\displaystyle\sum_{k=0}^{n}\binom{n}{k} = 2^n$
2. Setting $a = 1$, $b = -1$: $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$
3. Setting $a = 1$, $b = 1$ and differentiating: $\displaystyle\sum_{k=0}^{n}k\binom{n}{k} = n2^{n-1}$

Example 15
What is the coefficient of x^3y^7 in $(2x-y)^{10}$?

Using the Binomial Theorem with $a = 2x$ and $b = -y$:

$$\binom{10}{7}(2x)^3(-y)^7 = \binom{10}{7}\cdot 8x^3\cdot(-1)^7y^7 = 120\times 8\times(-1)x^3y^7 = -960x^3y^7.$$

The coefficient is -960.

8.5 Inclusion and Exclusion

The inclusion-exclusion principle extends the addition rule to sets that are not necessarily disjoint, by carefully accounting for elements counted multiple times.

8.5.1 The Inclusion-Exclusion Principle for Two Sets

Theorem 10
For any two finite sets A and B,

$$|A\cup B| = |A| + |B| - |A\cap B|.$$

Proof
Every element of $A\cup B$ is in A, in B, or both. When we compute $|A|+|B|$, elements in $A\cap B$ are counted twice. Subtracting $|A\cap B|$ corrects the count to exactly once per element. □

Example 16
How many integers from 1 to 100 are divisible by 3 or by 5?

Let A = multiples of 3 in $[1,100]$ and B = multiples of 5 in $[1,100]$. Then $|A| = 33$, $|B| = 20$, and $|A \cap B|$ = multiples of 15 in $[1,100] = 6$. By inclusion-exclusion:

$$|A \cup B| = 33 + 20 - 6 = 47.$$

8.5.2 The General Inclusion-Exclusion Principle

Theorem 11 (Inclusion-Exclusion Principle)
For finite sets $A_1, A_2, \ldots, A_n$,

$$\begin{aligned}|A_1 \cup \ldots \cup A_n| = &\sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| \\ &+ \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots \\ &+ (-1)^{n+1} \, |A_1 \cap A_2 \cap \ldots \cap A_n|.\end{aligned}$$

In summation notation:

$$|A_1 \cup \ldots \cup A_n| = \sum_{\emptyset \neq S \subseteq \{1,\ldots,n\}} (-1)^{|S|+1} \, \Big|\bigcap_{i \in S} A_i\Big|.$$

Example 17
Three sets A, B, C with $|A| = 10$, $|B| = 8$, $|C| = 6$, $|A \cap B| = 4$, $|A \cap C| = 3$, $|B \cap C| = 2$, $|A \cap B \cap C| = 1$. Then:

$$|A \cup B \cup C| = 10 + 8 + 6 - 4 - 3 - 2 + 1 = 16.$$

8.5.3 Applications to Counting

Definition 7
A **derangement** of $\{1, 2, \ldots, n\}$ is a permutation σ such that $\sigma(i) \neq i$ for all i; that is, no element occupies its original position. The number of derangements of n elements is denoted D_n.

Theorem 12

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{(-1)^n}{n!}\right).$$

As $n \to \infty$, $\frac{D_n}{n!} \to \frac{1}{e} \approx 0.3679$, so approximately 36.8% of all permutations of a large set are derangements.

Proof
Let A_i be the set of permutations that fix i (i.e., $\sigma(i) = i$). Then $|A_i| = (n-1)!$, $|A_i \cap A_j| = (n-2)!$, and more generally $|A_{\{i_1\}} \cap \ldots \cap A_{\{i_k\}}| = (n-k)!$. There are $\binom{n}{k}$ choices of k indices. By inclusion-exclusion, the number of permutations fixing at least one element is:

$$\sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!}.$$

Subtracting from $n!$ gives $D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$. □

Example 18
$D_3 = 3!\left(1 - 1 + \frac{1}{2} - \frac{1}{6}\right) = 6 \times \frac{1}{3} = 2$. The two derangements of $\{1, 2, 3\}$ are $(2, 3, 1)$ and $(3, 1, 2)$.

8.6 The Pigeonhole Principle

The Pigeonhole Principle is a simple combinatorial observation with far-reaching consequences in mathematics and computer science.

8.6.1 Statement and Basic Applications

Theorem 13 (Pigeonhole Principle)
If $n + 1$ or more objects are distributed among n boxes, then at least one box contains two or more objects.

Proof
Suppose, for the sake of contradiction, that every box contains at most one object. Then the total number of objects is at most n, contradicting the assumption that there are $n + 1$ or more. □

Example 19
In any group of 13 or more people, at least two were born in the same month. (12 months are the "boxes"; the people are the "objects".)

Example 20
Among any 5 integers, at least two have the same remainder when divided by 4. (The four possible remainders $\{0, 1, 2, 3\}$ are the boxes.)

Example 21
Let S be any set of 10 integers. Show that two distinct non-empty subsets of S have the same sum.

S has $2^{\{10\}} - 1 = 1023$ non-empty subsets. Each subset sum lies between 1 and at most $10 \times \max(S)$. When $S \subseteq \{1, ..., 55\}$, for example, each sum is at most 550, but there are 1023 subsets — far fewer "boxes" than "objects".

8.6.2 The Generalised Pigeonhole Principle

Theorem 14 (Generalised Pigeonhole Principle)
If n objects are distributed among k boxes, then at least one box contains at least $\lceil n/k \rceil$ objects.

Proof
Suppose every box contains at most $\lceil n/k \rceil - 1$ objects. Since $\lceil n/k \rceil - 1 < n/k$, the total number of objects is less than $k \times (n/k) = n$, a contradiction. □

Example 22
In a group of 85 people, at least $\lceil 85/12 \rceil = \lceil 7.08... \rceil = 8$ share a birth month.

Example 23
Show that among any 11 integers, two have the same last digit.

The last digit (units digit) is one of $\{0, 1, ..., 9\}$ — ten possible values. By the Pigeonhole Principle, at least $\lceil 11/10 \rceil = 2$ of the integers share a last digit.

Remark
The Pigeonhole Principle can also be applied in continuous settings. For example, among any five points placed inside a unit square, two must lie within distance $\frac{\sqrt{2}}{2}$ of each other (divide the square into four smaller squares of side $\frac{1}{2}$; by the Pigeonhole Principle, two points share a sub-square, and the diagonal of that sub-square has length $\frac{\sqrt{2}}{2}$).

9 Graph Theory

Graphs are mathematical structures used to model pairwise relationships between objects. A graph consists of a set of vertices (representing the objects) and a set of edges (representing the relationships). This deceptively simple structure captures an enormous variety of real-world situations: road networks, social connections, circuit layouts, scheduling dependencies, and communication networks can all be modelled as graphs. This chapter introduces the fundamental definitions, properties, and theorems of graph theory.

In this chapter we study:

- **Introduction to graphs:** definitions, types, and the degree of a vertex
- **Walks, trails, and circuits:** movement through graphs, and the classical results of Euler and Hamilton

- **Matrix representations:** encoding graphs as adjacency and incidence matrices
- **Trees:** acyclic connected graphs and their properties

9.1 Introduction to Graphs

9.1.1 Definitions and Terminology

Definition 1

A **graph** $G = (V, E)$ consists of a non-empty finite set V of **vertices** (or **nodes**) and a set E of **edges**, where each edge is an unordered pair $\{u, v\}$ of distinct vertices. We say:

- u and v are **adjacent** (or **neighbours**) if $\{u, v\} \in E$;
- an edge $e = \{u, v\}$ is **incident** to both u and v;
- a vertex with no incident edges is **isolated**.

The **order** of G is $|V|$ (the number of vertices); the **size** of G is $|E|$ (the number of edges).

Note

Unless stated otherwise, all graphs in this chapter are **simple**: no loops (edges from a vertex to itself) and no multiple edges between the same pair of vertices.

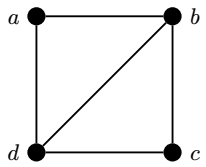
Definition 2

A **loop** is an edge $\{v, v\}$ from a vertex to itself. A **multigraph** allows multiple edges between the same pair of vertices. A graph permitting both loops and multiple edges is a **pseudograph**.

A **directed graph** (or **digraph**) $G = (V, E)$ has **directed edges** (arcs) which are ordered pairs (u, v); the vertex u is the **tail** and v is the **head** of the arc.

Example 1

Let $V = \{a, b, c, d\}$ and $E = \{\{a, b\}, \{b, c\}, \{c, d\}, \{a, d\}, \{b, d\}\}$. Then $G = (V, E)$ is a graph of order 4 and size 5. Vertices a and c are not adjacent; vertices b and d are adjacent.



The graph $G = (V, E)$ with $V = \{a, b, c, d\}$ and $E = \{\{a, b\}, \{b, c\}, \{c, d\}, \{a, d\}, \{b, d\}\}$, which has order 4 and size 5. Vertex a and vertex c share no edge.

9.1.2 Types of Graphs

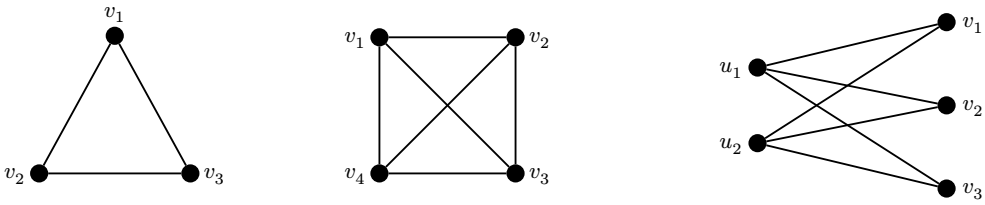
Definition 3

- The **complete graph** K_n is the graph on n vertices in which every pair of distinct vertices is joined by an edge. It has $\binom{n}{2} = \frac{n(n-1)}{2}$ edges.
- The **cycle** C_n $(n \geq 3)$ is the graph with vertices $v_1, v_2, ..., v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, ..., \{v_{\{n-1\}}, v_n\}, \{v_n, v_1\}$.
- The **path** P_n is the graph with vertices $v_1, v_2, ..., v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, ..., \{v_{\{n-1\}}, v_n\}$.
- A graph $G = (V, E)$ is **bipartite** if V can be partitioned into two non-empty sets X and Y such that every edge has one endpoint in X and one in Y. The sets X and Y are the **parts**.
- The **complete bipartite graph** $K_{\{m,n\}}$ has parts X (m vertices) and Y (n vertices), with every vertex in X adjacent to every vertex in Y, giving mn edges.
- A graph $H = (W, F)$ is a **subgraph** of $G = (V, E)$ if $W \subseteq V$ and $F \subseteq E$. If $W = V$, it is a **spanning subgraph**.

Example 2

K_1: a single vertex with no edges. K_2: two vertices connected by one edge. K_3: a triangle. K_4: four vertices, each pair connected, with $\binom{4}{2} = 6$ edges.

$K_{\{2,3\}}$ has parts $\{u_1, u_2\}$ and $\{v_1, v_2, v_3\}$, with $2 \times 3 = 6$ edges.



Left: the complete graph K_3 (triangle, 3 edges). Centre: the complete graph K_4 (6 edges, every pair joined). Right: the complete bipartite graph $K_{2,3}$ with left part $\{u_1, u_2\}$ and right part $\{v_1, v_2, v_3\}$, giving $2 \times 3 = 6$ edges.

Theorem 1

A graph is bipartite if and only if it contains no odd cycle.

9.1.3 Planar Graphs and Euler's Formula

Definition 4

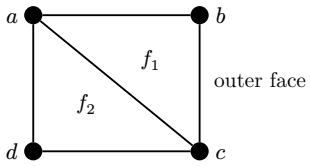
A graph is **planar** if it can be drawn in the plane without edge crossings (except at shared endpoints). Such a drawing is a **plane embedding**. The connected

regions determined by the embedding are called **faces** (including the unbounded outer face).

Theorem 2 (Euler's Formula for Connected Planar Graphs)
If a connected planar graph has V vertices, E edges, and F faces in a plane embedding, then

$$V - E + F = 2.$$

Example 3
A square with one diagonal is planar with $V = 4$, $E = 5$, and $F = 3$ (two bounded triangular faces and one outer face). Hence $V - E + F = 4 - 5 + 3 = 2$.



A planar embedding of a connected graph with $V = 4$, $E = 5$, $F = 3$. The two interior triangles and the exterior region are the three faces, so Euler's formula gives $4 - 5 + 3 = 2$.

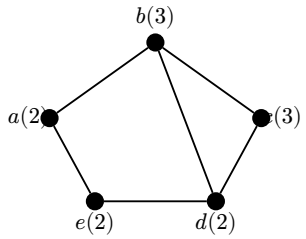
9.1.4 Degree of a Vertex

Definition 5
The **degree** of a vertex v in a graph G, written $\deg(v)$, is the number of edges incident to v. (In a pseudograph, loops contribute 2 to the degree.) The **minimum degree** and **maximum degree** of G are denoted $\delta(G)$ and $\Delta(G)$ respectively.

Theorem 3 (Handshaking Theorem)
For any graph $G = (V, E)$,

$$\sum_{v \in V} \deg(v) = 2|E|.$$

Proof
Each edge $\{u, v\}$ contributes 1 to $\deg(u)$ and 1 to $\deg(v)$, so contributes exactly 2 to the sum $\sum_v \deg(v)$. Summing over all edges gives $2|E|$. □



Handshaking theorem intuition: summing local degrees counts each edge twice, once from each endpoint. Here $(\deg(a), \deg(b), \deg(c), \deg(d), \deg(e)) = (2, 3, 3, 2, 2)$*, so* $\sum \deg(v) = 12 = 2 \times 6 = 2|E|$.

Theorem 4
In any graph, the number of vertices with odd degree is even.

Proof
By the Handshaking Theorem, $\sum_v \deg(v) = 2|E|$, which is even. The sum of even-degree vertices is even; since the total is even, the sum of odd-degree vertices must also be even. A sum of odd numbers is even if and only if there are an even number of them. □

Example 4
In K_5: each vertex has degree 4. Sum of degrees $= 5 \times 4 = 20 = 2 \times 10 = 2|E|$. ✓

In $K_{\{3,4\}}$: vertices in the 3-part have degree 4; vertices in the 4-part have degree 3. Sum $= 3 \times 4 + 4 \times 3 = 24 = 2 \times 12$, so $|E| = 12 = 3 \times 4$. ✓

Definition 6
A graph is **regular** if every vertex has the same degree. A graph where every vertex has degree k is ***k*-regular**. The complete graph K_n is $(n-1)$-regular.

9.2 Walks, Trails, and Circuits

Movement through a graph is formalised by the notions of walks, trails, and paths. The classical problems of Euler and Hamilton ask when a graph can be traversed in particularly structured ways.

9.2.1 Definitions and Examples

Definition 7
Let $G = (V, E)$ be a graph. A **walk** from v_0 to v_n is a finite sequence

$$v_0, e_1, v_1, e_2, v_2, ..., e_n, v_n$$

of alternating vertices and edges, where $e_i = \{v_{\{i-1\}}, v_i\}$ for each i. The **length** of the walk is n (the number of edges).

- A **trail** is a walk with no repeated edges.
- A **path** is a walk with no repeated vertices (and hence no repeated edges).
- A walk is **closed** if $v_0 = v_n$.
- A **circuit** is a closed trail.
- A **cycle** is a closed walk with no repeated vertices (other than $v_0 = v_n$) and length $n \geq 3$.

Theorem 5
If there is a walk from u to v in a graph G, then there is a path from u to v.

Proof
Among all walks from u to v, choose one of minimum length. If this walk had a repeated vertex w (at positions i and j with $i < j$), then removing the portion between the two occurrences of w would yield a shorter walk — contradicting minimality. Hence the walk has no repeated vertices and is a path. □

Definition 8
A graph G is **connected** if there is a path between every pair of distinct vertices. Otherwise G is **disconnected**. The maximal connected subgraphs of G are its **connected components**.

Example 5
The cycle C_5 is connected. The graph consisting of K_3 together with an isolated vertex has two connected components.

9.2.2 Euler Trails and Circuits

Definition 9
A trail that traverses every edge of G exactly once is an **Eulerian trail**. A closed Eulerian trail is an **Eulerian circuit**. A graph is **Eulerian** if it has an Eulerian circuit.

Theorem 6 (Euler's Theorem)
A connected graph G has an Eulerian circuit if and only if every vertex has even degree.

A connected graph G has an Eulerian trail from u to v (with $u \neq v$) if and only if u and v are the only vertices of odd degree.

Proof

Necessity for circuits: In an Eulerian circuit, every time the circuit passes through a vertex w, it uses one edge to enter and one to leave. Since no edge is repeated, each visit uses two previously unused edges. Hence $\deg(w)$ must be even for every w.

Sufficiency for circuits: We use Hierholzer's algorithm. Begin at any vertex v and follow edges (deleting each used edge) until returning to v — this is always possible when all degrees are even (since arriving at any non-start vertex always leaves an unused edge to exit). The resulting closed trail C_1 may not use all edges. If edges remain, some vertex w on C_1 has unused incident edges. Start a new closed trail from w using only unused edges. Splice this trail into C_1 at w. Repeat until no edges remain.

Eulerian trails: Adding an edge between u and v in the "trail" case gives a graph where every vertex has even degree (since only u and v had odd degree). The resulting graph has an Eulerian circuit, which restricted to the original edges gives an Eulerian trail from u to v. □

Example 6

Königsberg bridge problem (Euler, 1736): The city of Königsberg had two islands in the Pregel river, connected to each other and to both banks by seven bridges. Modelling landmasses as vertices and bridges as edges gives a multigraph in which all four vertices have odd degree (3, 3, 3, or 5). Since there are four vertices of odd degree (not two), no Eulerian trail exists. It is impossible to walk across each bridge exactly once.

9.2.3 Hamilton Paths and Circuits

Definition 10

A **Hamiltonian path** in a graph G is a path that visits every vertex exactly once. A **Hamiltonian circuit** is a cycle that visits every vertex exactly once and returns to the starting vertex. A graph that has a Hamiltonian circuit is called **Hamiltonian**.

Remark

Unlike Eulerian circuits, there is no known simple characterisation of Hamiltonian graphs.. The following theorems give sufficient (but not necessary) conditions.

Theorem 7 (Dirac's Theorem)

If G is a simple graph with $n \geq 3$ vertices such that $\deg(v) \geq n/2$ for every vertex v, then G is Hamiltonian.

Theorem 8 (Ore's Theorem)
If G is a simple graph with $n \geq 3$ vertices such that $\deg(u) + \deg(v) \geq n$ for every pair of non-adjacent vertices u and v, then G is Hamiltonian.

Important
Determining whether a graph is Hamiltonian is an NP-complete problem. No polynomial-time algorithm is known (and the existence of one would imply P = NP). This contrasts sharply with Eulerian circuits, for which a linear-time algorithm exists. The Travelling Salesman Problem — finding a minimum-weight Hamiltonian circuit in a weighted graph — is one of the most intensively studied problems in combinatorial optimisation.

9.3 Matrix Representations of Graphs

Graphs can be represented as matrices, enabling algebraic and computational techniques. Two standard representations are the adjacency matrix and the incidence matrix.

9.3.1 Adjacency Matrices

Definition 11
Let $G = (V, E)$ be a graph with vertices labelled $v_1, v_2, \ldots, v_n$ in some fixed order. The **adjacency matrix** of G is the $n \times n$ matrix A where

$$A_{ij} = \begin{cases} 1 \text{ if } \{v_i, v_j\} \in E \\ 0 \text{ otherwise.} \end{cases}$$

Note
For simple undirected graphs: A is symmetric ($A_{ij} = A_{ji}$) and has zeros on the diagonal ($A_{ii} = 0$). For directed graphs, $A_{ij} = 1$ if there is an arc from v_i to v_j; A need not be symmetric.

Theorem 9
The (i, j) entry of A^k equals the number of walks of length k from v_i to v_j.

Proof
By induction on k. For $k = 1$, $A^1 = A$ and the result holds by definition. Suppose it holds for $k - 1$. The (i, j) entry of $A^k = A^{k-1} \times A$ is

$$\left(A^k\right)_{ij} = \sum_{m=1}^{n} \left(A^{k-1}\right)_{im} A_{mj}.$$

By the inductive hypothesis, $\left(A^{k-1}\right)_{im}$ counts walks of length $k-1$ from v_i to v_m. Multiplying by A_{mj} (which is 1 if $\{v_m, v_j\} \in E$ and 0 otherwise) and summing counts walks of length k from v_i to v_j via the penultimate vertex v_m. □

Example 7
The adjacency matrix of K_3 (vertices v_1, v_2, v_3) is

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

The row sums give the degrees: each vertex has degree 2. The matrix A^2 has (i, j) entry equal to the number of walks of length 2 from v_i to v_j.

$$A^2 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

The diagonal entry $\left(A^2\right)_{11} = 2$ counts the two walks of length 2 from v_1 to itself: $v_1 v_2 v_1$ and $v_1 v_3 v_1$.

Remark
The degree of vertex v_i equals the sum of row i of A: $\deg(v_i) = \sum_{j=1}^{n} A_{ij}$. This provides a quick method to read off all degrees from the adjacency matrix.

9.3.2 Incidence Matrices

Definition 12
Let $G = (V, E)$ be a graph with n vertices $v_1, \ldots, v_n$ and m edges $e_1, \ldots, e_m$ in some fixed order. The **incidence matrix** of G is the $n \times m$ matrix M where

$$M_{ij} = \begin{cases} 1 \text{ if } v_i \text{ is an endpoint of } e_j \\ 0 \text{ otherwise.} \end{cases}$$

Note
- Each column of M has exactly two 1s (one per endpoint of each edge), since every edge has exactly two endpoints in a simple graph.
- The sum of row i equals $\deg(v_i)$.
- The sum of all entries equals $2|E|$, consistent with the Handshaking Theorem.

Example 8
Let G have vertices $\{v_1, v_2, v_3, v_4\}$ and edges $e_1 = \{v_1, v_2\}$, $e_2 = \{v_1, v_3\}$, $e_3 = \{v_2, v_4\}$, $e_4 = \{v_3, v_4\}$. The incidence matrix is:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Row sums: v_1 has degree 2, v_2 has degree 2, v_3 has degree 2, v_4 has degree 2. Total: $8 = 2 \times 4 = 2|E|$. ✓

9.4 Trees

Trees are the simplest connected graphs, and their absence of cycles gives them a particularly clean structure. They arise naturally in data structures, algorithm design, and the analysis of networks.

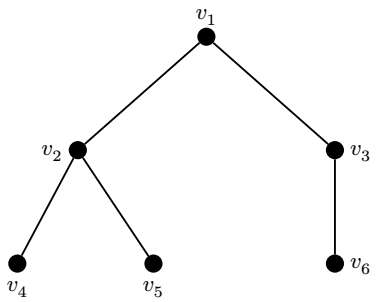
9.4.1 Definitions and Properties

Definition 13

A **tree** is a connected graph that contains no cycles. A graph that contains no cycles but is not necessarily connected is a **forest**; the connected components of a forest are trees.

Example 9

K_1 (single vertex), K_2 (single edge), the path P_n, and any star graph (one central vertex connected to n leaves) are trees. The cycle C_3 is connected but not a tree (it contains a cycle).



A tree on six vertices. Every pair of vertices is connected by exactly one path, and removing any single edge disconnects the graph. The tree has $6 - 1 = 5$ edges.

Theorem 10

The following statements are equivalent for a connected graph G with n vertices:

1. G is a tree (connected and acyclic).
2. G is connected and has exactly $n - 1$ edges.
3. G is acyclic and has exactly $n - 1$ edges.
4. There is exactly one path between every pair of distinct vertices.

5. G is connected, and removing any single edge disconnects G.

Proof

We prove (1) $\to$ (2) by induction on n.

Base case ($n = 1$): A single vertex is a tree with $0 = 1 - 1$ edges. ✓

Inductive step: Suppose all trees with $n - 1$ vertices have $n - 2$ edges. Let T be a tree with $n \geq 2$ vertices. Since T is a finite connected acyclic graph, it has at least one leaf (proved below). Remove a leaf v and its incident edge. The result T' is a connected acyclic graph on $n - 1$ vertices, so by the inductive hypothesis it has $n - 2$ edges. Restoring v adds one edge, giving T exactly $n - 1$ edges. □

Theorem 11

Every tree with $n \geq 2$ vertices has at least two leaves (vertices of degree 1).

Proof

Let $P = v_0, v_1, ..., v_k$ be a longest path in the tree. The endpoints v_0 and v_k must be leaves: if v_0 had a neighbour u other than v_1, then u is not on P (otherwise there would be a cycle), so $u, v_0, v_1, ..., v_k$ would be a longer path, contradicting the maximality of P. By the same argument, v_k is a leaf. Since $k \geq 1$ (any two vertices are connected by a path), $v_0 \neq v_k$, giving two distinct leaves. □