Discrete Mathematics

Complete Course Notes

BS/ADP CS-IT-SE

Prepared by:

Sohaib Hasan

HOD Mathematics
Horizon College Chakwal

linkedin.com/in/sohaibhassan05
+923335904314

sohaibhassan199@gmail.com

@plotlab01

Contents

Chapter 1

Logic and Proof Techniques

Propositions and Connectives

Logic is the foundation of all mathematical reasoning. Before we can prove theorems, solve problems, or write algorithms, we need a precise language to express ideas. That language is **propositional logic**. In this section we learn what a proposition is, how to combine propositions using connectives, and how to evaluate the truth of compound statements.

Definition 1.1 — Proposition

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

Key Points:

- Every proposition has a **truth value**: either **True (T)** or **False (F)**.
- Propositions are usually denoted by lowercase letters: p, q, r, s, ...
- Questions, commands, and exclamations are **NOT** propositions.
- A proposition cannot be *sometimes true* — its truth value must be definite.

Example 1: Identifying Propositions

Classify each of the following as a **proposition** or **not a proposition**. If it is a proposition, state its truth value.

Solution:

Sentence	Proposition?	Truth Value
"Islamabad is the capital of Pakistan."	✓ Yes	True
"$2 + 2 = 5$"	✓ Yes	False
"What time is it?"	× No	—
"Close the door!"	× No	—
"$x + 1 = 5$"	× No	—
"Every even number greater than 2 is the sum of two primes."	✓ Yes	Unknown
"The moon is made of cheese."	✓ Yes	False

Note: "$x+1=5$" is **not** a proposition because its truth value depends on the value of x — it is called a **predicate** (covered in Section 1.4). The Goldbach conjecture (last row) is a proposition even though mathematicians have not yet proved or disproved it; it is still either true or false.

Example 2: Propositions from Everyday Life

Let us form propositions from situations a CS student encounters daily.

Solution:

Define the following propositions:

- p : "Today is Friday." *(Truth value depends on the day)*
- q : "The lab is open." *(Truth value depends on schedule)*
- r : "17 is a prime number." True
- s : "All dogs are cats." False

Each of p, q, r, s is a valid proposition because each is a declarative sentence with a definite (though sometimes contextual) truth value. We will use p and q throughout this chapter to build compound statements.

Definition 1.2 — Negation ($\neg$)

The **negation** of a proposition p, written $\neg p$ (read: "not p"), is the proposition that is **true when p is false**, and **false when p is true**.

Truth Table for Negation:

p	$\neg p$
T	F
F	T

Key Points:

- $\neg p$ simply **flips** the truth value of p.
- Applying negation **twice** returns the original: $\neg(\neg p) \equiv p$.
- In English, negation is expressed by inserting "not" or using "It is not the case that ..."

Definition 1.3 — Conjunction ($\wedge$)

The **conjunction** of propositions p and q, written $p \wedge q$ (read: "p **and** q"), is true **only when both p and q are true**.

Truth Table for Conjunction:

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

Key Points:

- $p \wedge q$ is true in **only 1 out of 4** possible cases.
- Think of it as a strict "both must pass" condition.
- In English: "and", "but", "however", "moreover" can all represent $\wedge$.

Definition 1.4 — Disjunction ($\vee$)

The **disjunction** of propositions p and q, written $p \vee q$ (read: "p **or** q"), is true when **at least one of p or q is true**.

Truth Table for Disjunction:

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

Key Points:

- $p \vee q$ is false in **only 1 out of 4** possible cases (when both are false).
- This is the **inclusive or** — both can be true simultaneously.
- The **exclusive or** $p \oplus q$ is true only when *exactly one* is true.

Definition 1.5 — Exclusive Or ($\oplus$)

The **exclusive or** of p and q, written $p \oplus q$, is true when **exactly one** of p and q is true (but not both).

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Note: In daily English, "or" often means exclusive or. For example: "You can have tea **or** coffee" usually means you cannot have both. In mathematics, however, $\vee$ is always *inclusive or* unless stated otherwise.

Definition 1.6 — Conditional Statement ($\to$)

The **conditional statement** "if p then q", written $p \to q$, is false **only when** p **is true and** q **is false**. In all other cases it is true.

p is called the **hypothesis** (antecedent) and q is called the **conclusion** (consequent).

Truth Table for Conditional:

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

Ways to read $p \to q$:

- "If p, then q"
- "p implies q"
- "p only if q"
- "q is necessary for p"
- "p is sufficient for q"

Important: When the hypothesis p is **false**, the conditional is **vacuously true** regardless of q. Think: "If pigs can fly, I will give you \$100." Since pigs cannot fly, this promise is never broken — the statement is true.

Definition 1.7 — Biconditional ($\leftrightarrow$)

The **biconditional** "p if and only if q", written $p \leftrightarrow q$ (abbreviated **iff**), is true when p and q have the **same truth value**.

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

Note that $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$. This equivalence appears directly in past paper 2020 Q1(xiv).

Example 3: Translating English to Symbolic Logic

Let p = "It is raining" and q = "She will go to college." (This exact example appeared in **Past Paper 2021 Q1(ix)**.)

Solution:

Express each English sentence symbolically:

English Sentence	Symbolic Form
It is raining.	p
It is not raining.	$\neg p$
It is raining and she will go to college.	$p \wedge q$
It is raining and she will **not** go to college.	$p \wedge \neg q$
It is raining or she will go to college.	$p \vee q$
If it is raining, she will go to college.	$p \to q$
She will go to college if and only if it is raining.	$q \leftrightarrow p$

Note: The answer to Past Paper 2021 Q1(ix) is $\boxed{p \wedge \neg q}$.

Example 4: Building a Compound Truth Table

Construct the truth table for $\neg p \vee q$.

Solution:

Strategy: We evaluate column by column — first compute $\neg p$, then combine with q using $\vee$.

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

Observation: Compare this truth table with $p \to q$:

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

Conclusion: The columns for $\neg p \vee q$ and $p \to q$ are **identical**. Therefore:

$$\boxed{p \to q \;\equiv\; \neg p \vee q}$$

This is one of the most important logical equivalences and will be used in proofs throughout this chapter.

Example 5: Three-Variable Truth Table

Construct the truth table for $(p \oplus q) \wedge (p \oplus \neg q)$.
(This exact expression appeared in ***Past Paper 2021 Q3(i)****.)*

Solution:

Step 1: For three variables we would need $2^3 = 8$ rows, but here we have only p and q, so $2^2 = 4$ rows suffice.

Step 2: Build columns one operation at a time.

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

Conclusion: The final column is **always False**. Therefore $(p \oplus q) \wedge (p \oplus \neg q)$ is a **contradiction** (a statement that is always false regardless of the truth values of its variables).

$$\boxed{(p \oplus q) \wedge (p \oplus \neg q) \;\equiv\; \mathbf{F}}$$

Theorem 1.1 — Logical Equivalence of Conditional

For any propositions p and q:

$$p \to q \;\equiv\; \neg p \vee q$$

That is, the conditional "if p then q" is logically equivalent to "not p or q".

Proof of Theorem 1.1

Proof:

We need to show that $p \to q$ and $\neg p \vee q$ have identical truth values for every possible combination of truth values of p and q.

Step 1: Enumerate all cases.
There are $2^2 = 4$ possible truth-value assignments for (p, q).

Step 2: Evaluate both sides for each case.

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

Step 3: Compare columns.
In every row, the column for $p \to q$ and the column for $\neg p \vee q$ show the **same truth value**.

Conclusion: Since $p \to q$ and $\neg p \lor q$ agree on all possible inputs, by the definition of logical equivalence:

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

Definition 1.8 — Related Conditionals

Given the conditional $p \to q$, three related propositions are defined:

Name	Symbolic Form	Read as
Converse	$q \to p$	"If q, then p"
Inverse	$\neg p \to \neg q$	"If not p, then not q"
Contrapositive	$\neg q \to \neg p$	"If not q, then not p"

Critical Fact:

- The **contrapositive** is *always* logically equivalent to the original: $p \to q \equiv \neg q \to \neg p$
- The **converse** and **inverse** are *not* equivalent to the original.
- The converse and inverse *are* equivalent to each other.

Example 6: Converse Inverse and Contrapositive

Let p = "It is raining" and q = "The ground is wet." Write the conditional, converse, inverse, and contrapositive. Then determine which pairs are logically equivalent.

(Past Paper 2022 Q1(xii) directly tests this concept.)

Solution:

Statement	English	Symbolic
Conditional	If it is raining, then the ground is wet.	$p \to q$
Converse	If the ground is wet, then it is raining.	$q \to p$
Inverse	If it is not raining, then the ground is not wet.	$\neg p \to \neg q$
Contrapositive	If the ground is not wet, then it is not raining.	$\neg q \to \neg p$

Equivalence check:

- $p \to q \equiv \neg q \to \neg p$ ✓ Equivalent
- $q \to p \equiv \neg p \to \neg q$ ✓ Equivalent
- $p \to q \not\equiv q \to p$ × Not Equivalent

Intuitive check: The ground can be wet because a pipe burst — not because of rain. So the converse being true does not follow from the original conditional being true.

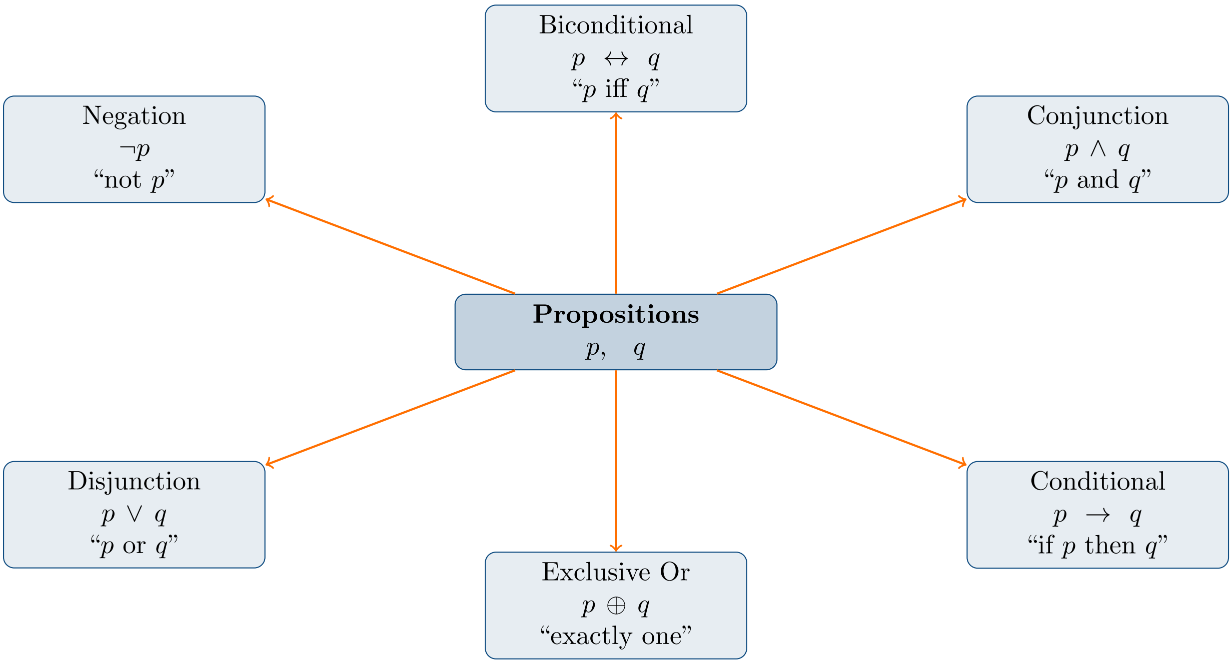


Figure 1.1: The six fundamental logical connectives built from propositions p and q.

Definition 1.9 — Operator Precedence

When parentheses are absent, logical operators are evaluated in the following order (from highest to lowest precedence):

Priority	Operator	Symbol
1 (highest)	Negation	$\neg$
2	Conjunction	$\wedge$
3	Disjunction	$\vee$
4	Conditional	$\rightarrow$
5 (lowest)	Biconditional	$\leftrightarrow$

Example: $\neg p \wedge q \vee r \rightarrow s$ is parsed as $\big((\neg p) \wedge q\big) \vee r \rightarrow s$, which equals $\big[\big((\neg p) \wedge q\big) \vee r\big] \rightarrow s$.

Example 7: Applying Operator Precedence

Given $p = \mathrm{T}$, $q = \mathrm{F}$, $r = \mathrm{T}$, evaluate $\neg p \vee q \rightarrow p \wedge r$.

Solution:

Step 1: Apply precedence to determine grouping.

$$\neg p \vee q \rightarrow p \wedge r \;=\; \big[(\neg p) \vee q\big] \rightarrow \big[p \wedge r\big]$$

Step 2: Substitute truth values.

$$\neg p = \neg \mathrm{T} = \mathrm{F}$$
$$\neg p \vee q = \mathrm{F} \vee \mathrm{F} = \mathrm{F}$$
$$p \wedge r = \mathrm{T} \wedge \mathrm{T} = \mathrm{T}$$

Step 3: Evaluate the conditional.

$$\mathrm{F} \to \mathrm{T} = \mathbf{T}$$

Final Answer: $\boxed{\text{True}}$

(When the hypothesis is False, the conditional is always True — vacuous truth.)

Section 1.1 Summary — Propositions & Connectives

Connective	Symbol	True when...	False when...
Negation	$\neg p$	p is F	p is T
Conjunction	$p \wedge q$	Both T	At least one F
Disjunction	$p \vee q$	At least one T	Both F
Exclusive Or	$p \oplus q$	Exactly one T	Both same
Conditional	$p \to q$	p is F, or q is T	p is T and q is F
Biconditional	$p \leftrightarrow q$	Both same	Different values

Key Equivalences to Memorise:

- $p \to q \ \equiv\ \neg p \vee q$
- $p \to q \ \equiv\ \neg q \to \neg p$ (contrapositive)
- $p \leftrightarrow q \ \equiv\ (p \to q) \wedge (q \to p)$
- $\neg(\neg p) \ \equiv\ p$ (double negation)

Past Paper Connection:

- **2020 Q1(v):** Define tautology → Section 1.2
- **2021 Q1(ix):** $p \wedge \neg q$ translation → Example 3 above
- **2022 Q1(xii):** Converse & contrapositive → Definition 1.8
- **2024 Q5:** Symbolic representation → Example 3 type

Truth Tables, Tautologies, and Contradictions

Definition 1.10 — Truth Table

A **truth table** is a table that lists all possible truth-value combinations of the propositional variables in a compound proposition, together with the resulting truth value of the compound proposition for each combination.

Key Points:

- If a compound proposition contains n distinct variables, its truth table has $\mathbf{2^n}$ rows.
- Columns are built **left to right**, one operation at a time, following operator precedence.
- The **final column** always corresponds to the entire compound proposition.
- Variables are listed with alternating T/F patterns: the rightmost variable alternates every row, the next every 2 rows, the next every 4 rows, and so on.

Row count rule:

$$\text{Number of rows} = 2^n \quad \text{where } n = \text{number of distinct variables}$$

Definition 1.11 — Tautology

A compound proposition is called a **tautology** if it is **true for every possible truth-value assignment** of its propositional variables.

Key Points:

- A tautology is also called a **logically valid** statement.
- No matter what truth values you assign to its variables, the result is always **T**.
- Tautologies are used as the foundation of valid **rules of inference**.
- Notation: We write $\models \varphi$ to indicate that φ is a tautology.

Simple example: $p \vee \neg p$ is always true (Law of Excluded Middle).

Definition 1.12 — Contradiction

A compound proposition is called a **contradiction** if it is **false for every possible truth-value assignment** of its propositional variables.

Key Points:

- A contradiction is the exact **opposite** of a tautology.
- No matter what truth values you assign, the result is always **F**.
- The negation of a tautology is always a contradiction, and vice versa.

Simple example: $p \wedge \neg p$ is always false (Law of Non-Contradiction).

Definition 1.13 — Contingency

A compound proposition is called a **contingency** if it is **neither a tautology nor a contradiction** — that is, it is true for some assignments and false for others.

Example: $p \wedge q$ is true when both are T, and false otherwise. It is a contingency.

Example 1: Verifying a Tautology — $p \vee \neg p$

Show that $p \vee \neg p$ is a tautology using a truth table.

Solution:

This proposition has $n = 1$ variable, so we need $2^1 = 2$ rows.

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

Conclusion: The final column is **all T**. Therefore $p \vee \neg p$ is a **tautology**.

$$\boxed{p \vee \neg p \;\equiv\; \mathbf{T}}$$

This is known as the **Law of Excluded Middle**: every proposition is either true or its negation is true — there is no middle ground.

Example 2: Verifying a Contradiction — $p \wedge \neg p$

Show that $p \wedge \neg p$ is a contradiction using a truth table.

Solution:

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

Conclusion: The final column is **all F**. Therefore $p \wedge \neg p$ is a **contradiction**.

$$\boxed{p \wedge \neg p \;\equiv\; \mathbf{F}}$$

This is the **Law of Non-Contradiction**: a proposition and its negation cannot both be true at the same time.

Example 3: Two-Variable Tautology — Past Paper 2020 Q1(xiv)

Using a truth table, show whether the following is a tautology or not:

$$(P \leftrightarrow Q) \;\leftrightarrow\; \big[(P \to Q) \wedge (Q \to P)\big]$$

Solution:

Step 1: Count rows. Two variables P and Q, so $2^2 = 4$ rows.

Step 2: Build intermediate columns.

P	Q	$P \to Q$	$Q \to P$	$(P{\to}Q) \wedge (Q{\to}P)$	$P \leftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Step 3: Evaluate the outer biconditional.

P	Q	$P \leftrightarrow Q$	$(P{\leftrightarrow}Q) \leftrightarrow [(P{\to}Q) \wedge (Q{\to}P)]$
T	T	T	$T \leftrightarrow T = \mathbf{T}$
T	F	F	$F \leftrightarrow F = \mathbf{T}$
F	T	F	$F \leftrightarrow F = \mathbf{T}$
F	F	T	$T \leftrightarrow T = \mathbf{T}$

Conclusion: All entries in the final column are **T**, so the statement is a **tautology**.

$$\boxed{(P \leftrightarrow Q) \;\leftrightarrow\; [(P \to Q) \wedge (Q \to P)] \;\equiv\; \mathbf{T}}$$

This confirms the fundamental definition: $p \leftrightarrow q$ means exactly $(p \to q) \wedge (q \to p)$.

Example 4: De Morgan's Law as Tautology — Past Paper 2024 Q6(i)

Draw a truth table for $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$.

Solution:

Step 1: $n = 2$ variables $\Rightarrow 2^2 = 4$ rows.

Step 2: Build columns systematically.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Step 3: Apply the biconditional to the two highlighted columns.

P	Q	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$
T	T	F	F	**T**
T	F	T	T	**T**
F	T	T	T	**T**
F	F	T	T	**T**

Conclusion: The statement is a **tautology**. This proves **De Morgan's First Law**:

$$\boxed{\neg(P \wedge Q) \;\equiv\; \neg P \vee \neg Q}$$

Example 5: Negation of a Tautology — Past Paper 2024 Q6(ii)

Draw a truth table for $\neg\big(\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)\big)$.

Solution:

Key Insight: From Example 4 we know that $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ is a tautology (always T). Negating a tautology gives a **contradiction** (always F).

Verification:

P	Q	$\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$	$\neg\big(\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)\big)$
T	T	T	**F**
T	F	T	**F**
F	T	T	**F**
F	F	T	**F**

Conclusion: The final column is **all F**. This is a **contradiction** — confirming that the negation of a tautology is always a contradiction.

$$\boxed{\neg\big(\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)\big) \;\equiv\; \mathbf{F}}$$

Example 6: Three-Variable Truth Table — Past Paper 2021 Q3(iii)

Construct a truth table for $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$.

Solution:

Step 1: $n = 3$ variables $\Rightarrow 2^3 = 8$ rows.

Step 2: Standard variable ordering: p changes every 4 rows, q every 2 rows, r every row.

p	q	r	$\neg p$	$\neg q$	$\neg p \leftrightarrow \neg q$	$q \leftrightarrow r$	$(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$
T	T	T	F	F	T	T	T
T	T	F	F	F	T	F	F
T	F	T	F	T	F	F	T
T	F	F	F	T	F	T	F
F	T	T	T	F	F	T	F
F	T	F	T	F	F	F	T
F	F	T	T	T	T	F	F
F	F	F	T	T	T	T	T

Conclusion: The final column is **not all T and not all F**, so this is a **contingency** — it is sometimes true and sometimes false.

Theorem 1.2 — Tautology and Contradiction Relationship

If φ is a tautology, then $\neg\varphi$ is a contradiction. Conversely, if φ is a contradiction, then $\neg\varphi$ is a tautology.

$$\varphi \equiv \mathbf{T} \implies \neg\varphi \equiv \mathbf{F}$$

$$\varphi \equiv \mathbf{F} \implies \neg\varphi \equiv \mathbf{T}$$

Proof of Theorem 1.2

Proof:

Step 1: Setup.

Let φ be a compound proposition containing variables $p_1, p_2, \ldots, p_n$. Suppose φ is a tautology, meaning for every truth-value assignment $\mathcal{A}$ to $p_1, \ldots, p_n$:

$$\mathcal{A}(\varphi) = \mathbf{T}$$

Step 2: Evaluate $\neg\varphi$ under any assignment.

Let $\mathcal{A}$ be any truth-value assignment. By the definition of negation:

$$\mathcal{A}(\neg\varphi) = \mathbf{T} \iff \mathcal{A}(\varphi) = \mathbf{F}$$

Since φ is a tautology, $\mathcal{A}(\varphi) = \mathbf{T}$ for all $\mathcal{A}$. Therefore $\mathcal{A}(\varphi) \neq \mathbf{F}$ for any $\mathcal{A}$, which means $\mathcal{A}(\neg\varphi) = \mathbf{F}$ for all $\mathcal{A}$.

Step 3: Conclude.

Since $\neg\varphi$ evaluates to $\mathbf{F}$ under every truth-value assignment, $\neg\varphi$ satisfies the definition of a contradiction.

The converse follows by the same argument with the roles of φ and $\neg\varphi$ exchanged, using the fact that $\neg(\neg\varphi) \equiv \varphi$.

Conclusion: φ is a tautology if and only if $\neg\varphi$ is a contradiction. □

Example 7: Proving a Tautology — Past Paper 2023 Q2(ii)

Show that $(p \wedge q) \to p$ is a tautology.

Solution:

Method 1: Truth Table

p	q	$p \wedge q$	$(p \wedge q) \to p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

The final column is **all T**. ✓ Tautology confirmed.

Method 2: Logical Reasoning (no truth table)

The conditional $p \wedge q \to p$ is false *only* when the hypothesis $p \wedge q$ is **true** and the conclusion p is **false**.

But if $p \wedge q$ is true, then by the definition of conjunction, p must be true. This is a direct contradiction — the hypothesis being true forces the conclusion to be true.

Therefore the conditional **can never be false**.

Conclusion:

$$\boxed{(p \land q) \to p \ \equiv \ \mathbf{T}}$$

This is known as the **Simplification** rule of inference and is used directly in logical proofs.

Example 8: Two-Variable Tautology — Past Paper 2021 Q3(ii)

Construct a truth table for $(\neg p \leftrightarrow \neg q) \to (p \leftrightarrow q)$.

Solution:

Step 1: $n = 2 \Rightarrow 2^2 = 4$ rows.

p	q	$\neg p$	$\neg q$	$\neg p \leftrightarrow \neg q$	$p \leftrightarrow q$	$(\neg p \leftrightarrow \neg q) \to (p \leftrightarrow q)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

Conclusion: All T — this is a **tautology**.

$$\boxed{(\neg p \leftrightarrow \neg q) \to (p \leftrightarrow q) \ \equiv \ \mathbf{T}}$$

Intuitively: if "not p" and "not q" have the same truth value, then p and q must also have the same truth value.

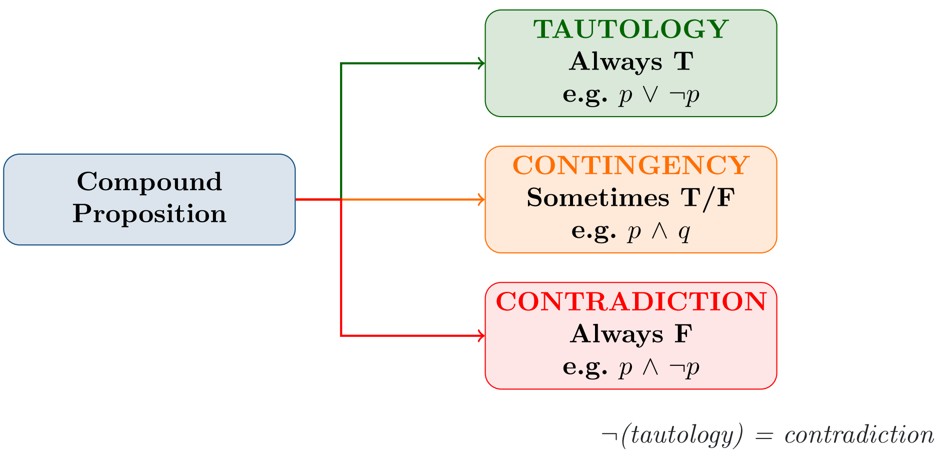


Figure 1.2: Classification of compound propositions by their truth-value patterns.

Definition 1.14 — Satisfiability

A compound proposition is called **satisfiable** if there exists at least one truth-value assignment that makes it **true**.

Key Points:

- Every **tautology** is satisfiable (it is true under all assignments).
- Every **contingency** is satisfiable (it is true under some assignments).
- A **contradiction** is the only type that is **not satisfiable**.
- Satisfiability is a central concept in computer science (the SAT problem).

Type	Always True?	Satisfiable?
Tautology	✓ Yes	✓ Yes
Contingency	× No	✓ Yes
Contradiction	× No	× No

(Past Paper 2025 Q1(v) directly asks: "What is a satisfiable statement?")

Example 9: Satisfiability Check

Determine whether each of the following is satisfiable:

(a) $p \wedge \neg p$

(b) $p \vee q$

(c) $p \rightarrow p$

Solution:

(a) $p \wedge \neg p$:

From Example 2, this is a **contradiction** — always F. There is no assignment making it true. $\Rightarrow$ **Not satisfiable.**

(b) $p \vee q$:

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

True for 3 out of 4 assignments — this is a **contingency**. $\Rightarrow$ **Satisfiable.**

(c) $p \rightarrow p$:

p	$p \rightarrow p$
T	T
F	T

Always T — this is a **tautology**. $\Rightarrow$ **Satisfiable.**

Section 1.2 Summary — Truth Tables, Tautologies & Contradictions

Classification at a Glance:

Type	Truth Pattern	Example
Tautology	All rows: T	$p \lor \neg p$
Contradiction	All rows: F	$p \land \neg p$
Contingency	Mix of T and F	$p \land q$

Truth Table Construction Steps:

1. Count distinct variables $n \Rightarrow$ table has 2^n rows.
2. List variables with standard alternating T/F pattern.
3. Add one column per sub-expression, following operator precedence.
4. Final column = the whole proposition.
5. Check: all T $\Rightarrow$ tautology; all F $\Rightarrow$ contradiction; mixed $\Rightarrow$ contingency.

Past Paper Connection:

- **2020 Q1(v) & Q1(xiv):** Tautology definition and verification → Examples 1, 3
- **2021 Q3(i)(ii)(iii):** Truth tables for compound propositions → Examples 5, 6, 8
- **2023 Q2(ii):** $(p \land q) \to p$ tautology → Example 7
- **2024 Q6(i)(ii):** De Morgan truth tables → Examples 4, 5
- **2025 Q1(v):** Satisfiable statement → Definition 1.14

Logical Equivalences and Laws of Logic

Definition 1.15 — Logical Equivalence

Two compound propositions φ and ψ are **logically equivalent**, written $\varphi \equiv \psi$, if they have **identical truth values** for every possible truth-value assignment of their variables.

Key Points:

- $\varphi \equiv \psi$ if and only if $\varphi \leftrightarrow \psi$ is a **tautology**.
- The symbol $\equiv$ means "logically equivalent" — it is **not** the same as $\leftrightarrow$ (which is a connective inside logic).
- Logical equivalence is an **equivalence relation**: it is reflexive, symmetric, and transitive.
- We can **substitute** one side for the other inside any larger formula without changing its truth value.

Theorem 1.3 — Laws of Propositional Logic

The following logical equivalences hold for all propositions p, q, and r. These are the fundamental laws used to simplify compound propositions.

Identity Laws:

$$p \wedge \mathbf{T} \equiv p \qquad p \vee \mathbf{F} \equiv p$$

Domination Laws:

$$p \vee \mathbf{T} \equiv \mathbf{T} \qquad p \wedge \mathbf{F} \equiv \mathbf{F}$$

Idempotent Laws:

$$p \vee p \equiv p \qquad p \wedge p \equiv p$$

Double Negation Law:

$$\neg(\neg p) \equiv p$$

Commutative Laws:

$$p \vee q \equiv q \vee p \qquad p \wedge q \equiv q \wedge p$$

Associative Laws:

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

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

Distributive Laws:

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

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

De Morgan's Laws:

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

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

Absorption Laws:

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

Negation Laws:

$$p \vee \neg p \equiv \mathbf{T} \qquad p \wedge \neg p \equiv \mathbf{F}$$

Contrapositive Law:

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

Exportation Law:

$$(p \wedge q) \to r \;\equiv\; p \to (q \to r)$$

Proof of De Morgan's First Law: $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Proof (by Truth Table):

Step 1: We need $2^2 = 4$ rows for variables p and q.

Step 2: Evaluate both sides independently.

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

Step 3: The columns for $\neg(p \wedge q)$ and $\neg p \vee \neg q$ are **identical** in every row: F, T, T, T.

Conclusion:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad \square$$

Intuitive meaning: "It is not the case that both p and q are true" is the same as saying "either p is false or q is false (or both)."

Proof of De Morgan's Second Law: $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Proof (by Truth Table):

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

Both columns produce F, F, F, T — they are identical.

Conclusion:

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad \square$$

Intuitive meaning: "Neither p nor q is true" is the same as "p is false **and** q is false."

Example 1: Applying De Morgan's Laws — Past Paper 2024 Q1(i)

State De Morgan's Laws in set theory and use them to find the negation of:

(a) Carlos will bicycle or run tomorrow.

(b) Ibrahim is smart and hardworking.

(Part (b) directly from Past Paper 2023 Q1(iv).)

Solution:

(a) Let p = "Carlos will bicycle" and q = "Carlos will run tomorrow."
Original statement: $p \vee q$
Negation: $\neg(p \vee q) \equiv \neg p \wedge \neg q$
In English: "Carlos will not bicycle **and** will not run tomorrow."

(b) Let p = "Ibrahim is smart" and q = "Ibrahim is hardworking."
Original statement: $p \wedge q$

Negation: $\neg(p \land q) \equiv \neg p \lor \neg q$
In English: "Ibrahim is not smart **or** is not hardworking."

Common Mistake: Students often negate "Ibrahim is smart and hardworking" as "Ibrahim is not smart and not hardworking." This is wrong — the **and** must change to **or** when negating a conjunction (De Morgan's Law).

Example 2: Simplification Using Laws of Logic

Simplify $\neg(\neg p \land q) \land (p \lor q)$ using logical laws.

Solution:

We apply laws step by step, naming each law used.

$$\begin{aligned}
&\neg(\neg p \land q) \land (p \lor q) && \\
&\equiv (\neg(\neg p) \lor \neg q) \land (p \lor q) && \text{De Morgan's Law} \\
&\equiv (p \lor \neg q) \land (p \lor q) && \text{Double Negation Law} \\
&\equiv p \lor (\neg q \land q) && \text{Distributive Law} \\
&\equiv p \lor \mathbf{F} && \text{Negation Law: } q \land \neg q \equiv \mathbf{F} \\
&\equiv p && \text{Identity Law}
\end{aligned}$$

Result:

$$\boxed{\neg(\neg p \land q) \land (p \lor q) \;\equiv\; p}$$

This is exactly the type of simplification asked in Past Paper 2025 Q1(iv).

Example 3: Laws of Logic Proof — Past Paper 2025 Q1(iv)

Using laws of logic, show that:

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

Solution:

Expression	Law Applied
$\neg(\neg p \land q) \land (p \lor q)$	Given
$(\neg\neg p \lor \neg q) \land (p \lor q)$	De Morgan's Law
$(p \lor \neg q) \land (p \lor q)$	Double Negation Law
$p \lor (\neg q \land q)$	Distributive Law
$p \lor \mathbf{F}$	Negation Law
p	Identity Law

Conclusion: $\neg(\neg p \land q) \land (p \lor q) \equiv p$ ✓

Example 4: Conditional Tautology Without Truth Table — Past Paper 2025 Q1(ii)

Show that $\neg(p \to q) \to \neg q$ is a tautology **without using a truth table**.

Solution:

We convert the conditional to disjunction form and simplify algebraically.

Expression	Law Applied
$\neg(p \to q) \to \neg q$	Given
$\neg(p \to q) \to \neg q$	(rewrite conditional)
$\neg[\neg(p \to q)] \lor \neg q$	$A \to B \equiv \neg A \lor B$
$(p \to q) \lor \neg q$	Double Negation Law
$(\neg p \lor q) \lor \neg q$	$p \to q \equiv \neg p \lor q$
$\neg p \lor (q \lor \neg q)$	Associative Law
$\neg p \lor \mathbf{T}$	Negation Law: $q \lor \neg q \equiv \mathbf{T}$
$\mathbf{T}$	Domination Law

Conclusion: The expression simplifies to **T**, confirming it is a **tautology**. ✓

$$\boxed{\neg(p \to q) \to \neg q \;\equiv\; \mathbf{T}}$$

Example 5: Proving Logical Equivalence — Past Paper 2023 Q2(i)

Prove that $\neg p \leftrightarrow q \;\equiv\; p \leftrightarrow \neg q$ using logical equivalences.

Solution:

Recall: $A \leftrightarrow B \equiv (A \to B) \land (B \to A)$ and $A \to B \equiv \neg A \lor B$.

Left-hand side:

$$\begin{aligned}
\neg p \leftrightarrow q &\equiv (\neg p \to q) \land (q \to \neg p) \\
&\equiv (p \lor q) \land (\neg q \lor \neg p) \\
&\equiv (p \lor q) \land \neg(q \land p) && \text{De Morgan on } \neg q \lor \neg p \\
&\equiv (p \lor q) \land \neg(p \land q) && \text{Commutative Law}
\end{aligned}$$

Right-hand side:

$$\begin{aligned}
p \leftrightarrow \neg q &\equiv (p \to \neg q) \land (\neg q \to p) \\
&\equiv (\neg p \lor \neg q) \land (q \lor p) \\
&\equiv \neg(p \land q) \land (p \lor q) && \text{De Morgan; Commutative} \\
&\equiv (p \lor q) \land \neg(p \land q) && \text{Commutative Law}
\end{aligned}$$

Both sides simplify to $(p \lor q) \land \neg(p \land q)$.

Conclusion:

$$\boxed{\neg p \leftrightarrow q \;\equiv\; p \leftrightarrow \neg q} \quad ✓$$

Example 6: XOR and Biconditional — Past Paper 2025 Q1(x)

Show that $\neg(p \oplus q)$ and $p \leftrightarrow q$ are logically equivalent.

Solution:

Method: Truth Table.
Recall: $p \oplus q$ is true when exactly one of p, q is true.

p	q	$p \oplus q$	$\neg(p \oplus q)$	$p \leftrightarrow q$
T	T	F	T	T
T	F	T	F	F
F	T	T	F	F
F	F	F	T	T

The columns for $\neg(p \oplus q)$ and $p \leftrightarrow q$ are identical: T, F, F, T.
Conclusion:

$$\boxed{\neg(p \oplus q) \;\equiv\; p \leftrightarrow q}$$

Intuition: $p \oplus q$ is true when p and q *differ*. Negating that gives truth when they are the *same* — which is exactly what the biconditional means.

Example 7: Finding the Dual — Past Paper 2025 Q1(i)

Find the dual of $(p \vee \mathbf{F}) \wedge (q \vee \mathbf{T})$.

Solution:

Definition of Dual: To find the dual of a compound proposition, replace every $\vee$ with $\wedge$, every $\wedge$ with $\vee$, every $\mathbf{T}$ with $\mathbf{F}$, and every $\mathbf{F}$ with $\mathbf{T}$. *Do not change the propositional variables or negations.*

Original: $(p \vee \mathbf{F}) \wedge (q \vee \mathbf{T})$

Step-by-step substitution:

- Outer $\wedge \longrightarrow \vee$
- First $\vee \longrightarrow \wedge$
- $\mathbf{F} \longrightarrow \mathbf{T}$
- Second $\vee \longrightarrow \wedge$
- $\mathbf{T} \longrightarrow \mathbf{F}$

Dual:

$$\boxed{(p \wedge \mathbf{T}) \vee (q \wedge \mathbf{F})}$$

Simplification of the dual using laws:

$$\begin{aligned}(p \wedge \mathbf{T}) \vee (q \wedge \mathbf{F}) &\equiv p \vee \mathbf{F} && \text{Identity Law; Domination Law}\\ &\equiv p && \text{Identity Law}\end{aligned}$$

Simplification of the original for comparison:

$$\begin{aligned}(p \vee \mathbf{F}) \wedge (q \vee \mathbf{T}) &\equiv p \wedge \mathbf{T} && \text{Identity Law; Domination Law}\\ &\equiv p && \text{Identity Law}\end{aligned}$$

Note: Both the original and its dual simplify to p in this case, but this is a coincidence — duals are generally not equivalent to the original.

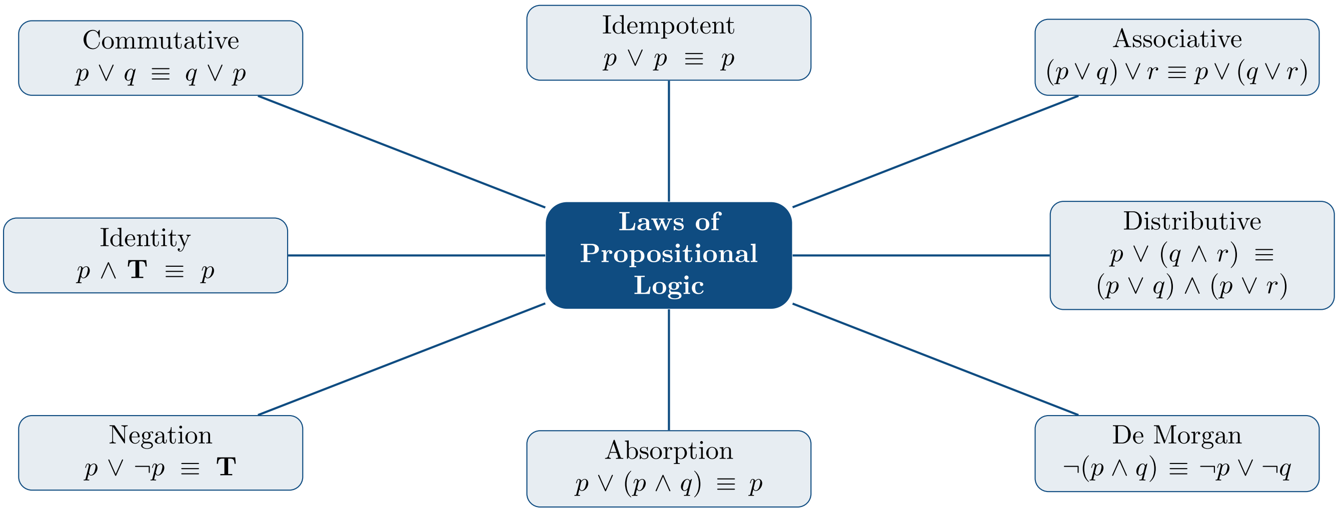


Figure 1.3: The eight families of logical laws for propositional logic.

Example 8: Associative Law — Past Paper 2021 Q1(iii)

State the associative law of union for three sets and verify it logically.

Solution:

The associative law of union for sets A, B, C states:

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

Logical counterpart: The analogous law for propositions is:

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

Verification by truth table ($n = 3$, so $2^3 = 8$ rows):

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$q \vee r$	$p \vee (q \vee r)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	T	F	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

Columns 5 and 7 are identical. ✓

$$\boxed{(p \vee q) \vee r \;\equiv\; p \vee (q \vee r)}$$

Section 1.3 Summary — Logical Equivalences & Laws

Strategy for Algebraic Simplification:

1. Replace conditionals: $p \to q \equiv \neg p \vee q$.
2. Apply **De Morgan's Laws** to push negations inward.
3. Apply **Double Negation** to eliminate $\neg\neg$.
4. Use **Distributive Laws** to factor or expand.
5. Use **Absorption**, **Idempotent**, and **Negation Laws** to reduce.
6. Apply **Identity** and **Domination Laws** to reach the simplest form.

Most Tested Laws (from past papers):

Law	Equivalence
De Morgan 1	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
De Morgan 2	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Conditional	$p \to q \equiv \neg p \vee q$
Contrapositive	$p \to q \equiv \neg q \to \neg p$
Double Negation	$\neg\neg p \equiv p$
Biconditional	$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
XOR–Biconditional	$\neg(p \oplus q) \equiv p \leftrightarrow q$

Past Paper Connection:

- **2021 Q1(iii):** Associative law of union $\to$ Example 8
- **2023 Q1(iv):** De Morgan negations in English $\to$ Example 1
- **2023 Q2(i):** Proving $\neg p \leftrightarrow q \equiv p \leftrightarrow \neg q$ $\to$ Example 5
- **2024 Q1(i):** De Morgan's law in set theory $\to$ Example 1
- **2025 Q1(i):** Dual of a proposition $\to$ Example 7
- **2025 Q1(ii):** Tautology without truth table $\to$ Example 4
- **2025 Q1(iv):** Laws of logic simplification $\to$ Examples 2, 3
- **2025 Q1(x):** XOR and biconditional equivalence $\to$ Example 6

Predicate Logic and Quantifiers

Propositional logic deals with complete statements that are already true or false. But many mathematical statements involve variables — for example, "$x > 5$" or "x is a prime number." These are **not** propositions by themselves because their truth value depends on what x is. To handle such statements, we need **predicate logic** (also called *first-order logic*), which extends propositional logic with **predicates** and **quantifiers**.

Definition 1.16 — Predicate

A **predicate** is a statement involving one or more variables whose truth value depends on the value(s) assigned to those variables. A predicate with variable x is written $P(x)$ and is called a **propositional function**.

Key Points:

- $P(x)$ is **not** a proposition — it becomes one only when a specific value is substituted for x.
- The set of all allowable values for a variable is called the **domain** (or *universe of discourse*).
- Predicates can have more than one variable: $P(x, y)$, $Q(x, y, z)$, etc.
- Once all variables are assigned values, $P(x)$ becomes a proposition with a definite truth value.

Example: Let $P(x)$ denote "$x > 5$."

- $P(6)$: "$6 > 5$" True
- $P(3)$: "$3 > 5$" False
- $P(x)$: not yet a proposition (truth value unknown until x is specified)

Example 1: Evaluating Predicates — Past Paper 2022 Q1(iv)

Let $P(x)$ denote the statement "$x > 5$." What are the truth values of $P(5)$ and $P(4)$?

Solution:

- $P(5)$: Substitute $x = 5 \Rightarrow$ "$5 > 5$" $\Rightarrow$ **False** (5 is not strictly greater than 5)
- $P(4)$: Substitute $x = 4 \Rightarrow$ "$4 > 5$" $\Rightarrow$ **False** (4 is not greater than 5)

Answer: $P(5) = \mathbf{F}$ and $P(4) = \mathbf{F}$.

For $P(x)$ to be true, we need $x > 5$, i.e., $x \geq 6$ for integer values. For example, $P(6) =$ True, $P(100) =$ True.

Definition 1.17 — Universal Quantifier ($\forall$)

The **universal quantification** of $P(x)$, written $\forall x\, P(x)$ (read: "**for all** x, $P(x)$" or "**for every** x, $P(x)$"), is the proposition that claims $P(x)$ is true **for every element** x in the domain.

Symbol	$\forall$ (inverted A — think "**A**ll")
Read as	"for all", "for every", "for each", "for any"
True when	$P(x)$ holds for **every** element in the domain
False when	There exists **at least one** element where $P(x)$ is false

Key Points:

- To **disprove** $\forall x\, P(x)$, it suffices to find **one** element x_0 where $P(x_0)$ is false. This element is called a **counterexample**.
- $\forall x\, P(x)$ is equivalent to the conjunction of $P(a)$ over all elements a in the domain.
- The domain must always be specified — the truth of $\forall x\, P(x)$ depends heavily on what the domain is.

Definition 1.18 — Existential Quantifier ($\exists$)

The **existential quantification** of $P(x)$, written $\exists x\, P(x)$ (read: "**there exists** an x such that $P(x)$"), is the proposition that claims $P(x)$ is true for **at least one element** x in the domain.

Symbol	$\exists$ (reversed E — think "**E**xists")
Read as	"there exists", "for some", "there is at least one"
True when	$P(x)$ holds for **at least one** element in the domain
False when	$P(x)$ is false for **every** element in the domain

Key Points:

- To **prove** $\exists x\, P(x)$, it suffices to find **one** specific element x_0 where $P(x_0)$ is true. This is called a **witness**.
- $\exists x\, P(x)$ is equivalent to the disjunction of $P(a)$ over all elements a in the domain.
- Past Paper 2021 Q1(i) directly asks: "Define existential quantification with a suitable example."

Example 2: Existential Quantification — Past Paper 2021 Q1(i)

Define existential quantification with a suitable example. Also evaluate $\exists x\, P(x)$ where $P(x)$ is "$x^2 > 10$" with domain $\{1, 2, 3, 4, 5\}$.

Solution:

Definition: $\exists x\, P(x)$ means "there exists at least one element x in the domain for which $P(x)$ is true."

Evaluation: We check $P(x) : x^2 > 10$ for each element.

x	x^2	$x^2 > 10$?
1	1	False
2	4	False
3	9	False
4	16	True
5	25	True

Since $P(4)$ is true (and $P(5)$ is true), there **exists** at least one element making $P(x)$ true. The witness is $x_0 = 4$.
Conclusion: $\exists x\, P(x) = \boxed{\textbf{True}}$

Example 3: Universal Quantification with Counterexample

Let $P(x)$ be "$x^2 \geq x$" with domain $\mathbb{R}$ (all real numbers). Determine if $\forall x\, P(x)$ is true or false.

Solution:

Claim: $\forall x\, (x^2 \geq x)$ — "For every real number x, $x^2 \geq x$."

Testing with examples:

- $x = 3$: $9 \geq 3$ ✓
- $x = 0$: $0 \geq 0$ ✓
- $x = -1$: $1 \geq -1$ ✓
- $x = 0.5$: $0.25 \geq 0.5$? $\times$ **False!**

Counterexample found: $x_0 = 0.5$ gives $P(0.5) = \text{False}$.
Conclusion: $\forall x\, P(x)$ is **False**.

Note: To disprove a universal statement, we only need **one** counterexample. We do *not* need to show it fails everywhere.

Definition 1.19 — Uniqueness Quantifier ($\exists!$)

The **uniqueness quantifier** $\exists!\, x\, P(x)$ (read: "there exists a **unique** x such that $P(x)$") asserts that $P(x)$ is true for **exactly one** element in the domain.

Example: $\exists!\, x\, (x^2 = 0)$ over the reals is **True** because only $x = 0$ satisfies $x^2 = 0$.

Definition 1.20 — Negation of Quantified Statements

The negation of a quantified statement is found by swapping the quantifier and negating the predicate:

Statement	Negation	Read as
$\forall x\, P(x)$	$\exists x\, \neg P(x)$	"There exists x such that $P(x)$ is false"
$\exists x\, P(x)$	$\forall x\, \neg P(x)$	"For all x, $P(x)$ is false"

Key Points:

- These are the **De Morgan's Laws for quantifiers**.
- The negation of "all students passed" is "some student did not pass" — **not** "all students did not pass."
- The negation of "some student failed" is "all students passed."

Theorem 1.4 — De Morgan's Laws for Quantifiers

For any predicate $P(x)$ over a domain D:

$$\neg\forall x\, P(x) \;\equiv\; \exists x\, \neg P(x)$$

$$\neg\exists x\, P(x) \;\equiv\; \forall x\, \neg P(x)$$

Proof of Theorem 1.4 — De Morgan's Laws for Quantifiers

Proof of the first law: $\neg\forall x\, P(x) \;\equiv\; \exists x\, \neg P(x)$

Step 1: What does $\neg\forall x\, P(x)$ mean?
$\forall x\, P(x)$ is true *only if* $P(x)$ holds for *every* element in the domain D. Its negation is true when this *fails* — i.e., when $P(x)$ is false for *at least one* element.

Step 2: Express the failure condition.
$\forall x\, P(x)$ fails $\iff$ there exists some element $x_0 \in D$ with $P(x_0) = \mathbf{F}$, i.e., $\neg P(x_0) = \mathbf{T}$.

Step 3: Recognise the definition.
The condition "there exists $x_0 \in D$ such that $\neg P(x_0)$ is true" is exactly the definition of $\exists x\, \neg P(x)$.

Conclusion:

$$\neg\forall x\, P(x) \;\equiv\; \exists x\, \neg P(x) \quad \square$$

The second law $\neg\exists x\, P(x) \equiv \forall x\, \neg P(x)$ follows by an identical argument with the roles of $\forall$ and $\exists$ exchanged.

Example 4: Negating Quantified Statements — Past Paper 2023 Q1(iii)

Find the negation of the statement: "All goats are mammals."

Solution:

Step 1: Identify the structure.
Let $G(x)$ = "x is a goat" and $M(x)$ = "x is a mammal."
The statement is: $\forall x\,(G(x) \to M(x))$

Step 2: Apply De Morgan's Law for quantifiers.

$$\begin{aligned}\neg[\forall x\,(G(x) \to M(x))] &\equiv \exists x\,\neg(G(x) \to M(x)) \\ &\equiv \exists x\,\neg(\neg G(x) \lor M(x)) && [p \to q \equiv \neg p \lor q] \\ &\equiv \exists x\,(G(x) \land \neg M(x)) && \text{[De Morgan's Law]}\end{aligned}$$

Step 3: Translate back to English.
$\exists x\,(G(x) \land \neg M(x))$: "There exists an x that is a goat **and** is not a mammal."
Answer: The negation is:

"There exists a goat that is not a mammal."

Common Mistake: The negation of "All goats are mammals" is **not** "All goats are not mammals" — that would be a much stronger claim. The correct negation only requires *one* goat to fail to be a mammal.

Definition 1.21 — Nested Quantifiers

When quantifiers appear one after another, they are called **nested quantifiers**. The order of different quantifiers **matters**.

Expression	Meaning	Order matters?
$\forall x\,\forall y\,P(x,y)$	For all x and all y, $P(x,y)$	No (same quantifier)
$\exists x\,\exists y\,P(x,y)$	There exist x and y such that $P(x,y)$	No (same quantifier)
$\forall x\,\exists y\,P(x,y)$	For every x, there exists a y such that $P(x,y)$	Yes
$\exists x\,\forall y\,P(x,y)$	There exists an x such that for all y, $P(x,y)$	Yes

Critical Note: $\forall x\,\exists y\,P(x,y)$ and $\exists x\,\forall y\,P(x,y)$ are **not** equivalent in general.
Example with $P(x,y) : y > x$ over integers:

- $\forall x\,\exists y\,(y > x)$: For every integer, there is a larger one — True
- $\exists x\,\forall y\,(y > x)$: There is an integer larger than all others — False

Example 5: Expressing Statements with Quantifiers — Past Paper 2025 Q2

Let $S(x)$ = "x is a student," $F(x)$ = "x is a faculty member," $A(x,y)$ = "x has asked y a question," where the domain consists of all people in the school.

Express each statement using quantifiers:

(i) Every student has asked Professor Gross a question.

(ii) Some student has not asked any faculty member a question.

(iii) There is a faculty member who has asked every other faculty member a question.

Solution:

Let g denote Professor Gross (a constant in the domain).

(i) Every student has asked Professor Gross a question.
We need: for all x, if x is a student, then x has asked g a question.

$$\boxed{\forall x\,\big(S(x) \to A(x,\,g)\big)}$$

(ii) Some student has not asked any faculty member a question.
We need: there exists a student x such that for every faculty member y, x has not asked y.

$$\boxed{\exists x\,\big(S(x) \land \forall y\,(F(y) \to \neg A(x,\,y))\big)}$$

(iii) There is a faculty member who has asked every other faculty member a question.
We need: there exists a faculty member x such that for every other faculty member y (i.e., $y \neq x$), x has asked y.

$$\boxed{\exists x\,\big(F(x) \land \forall y\,(F(y) \land y \neq x \to A(x,\,y))\big)}$$

Example 6: Translating Mathematical Statements — Past Paper 2023 Q1(v)

Translate the statement "The sum of two positive integers is always positive" into a logical expression.

Solution:

Step 1: Identify variables and predicates.
Let the domain be all positive integers $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.
Let x and y be any two positive integers. The statement says their sum $x + y$ is also a positive integer.

Step 2: Write the logical expression.
Since $x, y \in \mathbb{Z}^+$ by assumption of the domain, we need:

$$\boxed{\forall x\,\forall y\,\big((x > 0) \land (y > 0) \to (x + y > 0)\big)}$$

Or more concisely, if the domain is already restricted to positive integers:

$$\forall x\,\forall y\,(x + y > 0)$$

Note: The domain always matters. Specifying the domain as $\mathbb{Z}^+$ vs. $\mathbb{Z}$ (all integers) changes whether the statement needs the explicit positivity conditions.

Example 7: Truth Value of Nested Quantifiers — Past Paper 2024 Q1(vi)

What is the truth value of $\exists x\, \exists y\, P(x, y)$, where $P(x, y)$ means $x \cdot y > 0$ and x, y are real numbers?

Solution:

$\exists x\, \exists y\, P(x, y)$ asks: "Is there at least one pair (x, y) of real numbers such that $x \cdot y > 0$?"

Finding a witness: Take $x = 2$ and $y = 3$.

$$x \cdot y = 2 \times 3 = 6 > 0 \quad \checkmark$$

Since we found a specific pair $(x, y) = (2, 3)$ satisfying $P(x, y)$, the existential statement is true.

Answer:

$$\boxed{\exists x\, \exists y\, P(x, y) = \textbf{True}}$$

Example 8: Free and Bound Variables

Identify the free and bound variables in:

(a) $\exists x\, (x + y = 1)$

(b) $\forall x\, \exists y\, (x^2 + y^2 = 1)$

Solution:

A variable is **bound** if it is governed by a quantifier. Otherwise it is **free**.

(a) $\exists x\, (x + y = 1)$:

- x is **bound** by $\exists x$
- y is **free** — it has no quantifier

This is **not** a proposition (because y is free — its value is unspecified).

(b) $\forall x\, \exists y\, (x^2 + y^2 = 1)$:

- x is **bound** by $\forall x$
- y is **bound** by $\exists y$

All variables are bound, so this **is** a proposition. Over the reals, it is True (for any x with $|x| \leq 1$, we can find $y = \sqrt{1 - x^2}$).

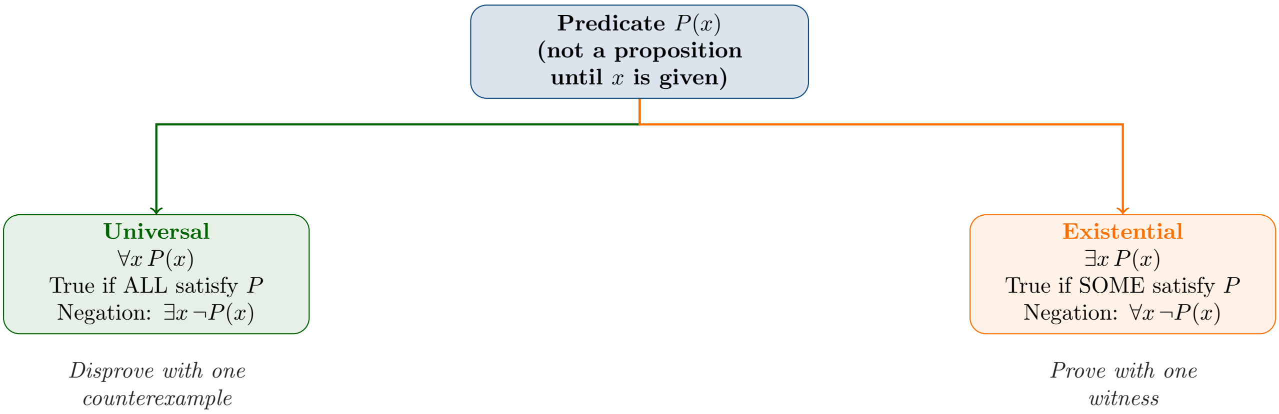


Figure 1.4: From predicates to quantified statements, with negation rules.

Section 1.4 Summary — Predicate Logic & Quantifiers

Quick Reference:

Concept	Symbol	True when	To disprove
Universal	$\forall x\, P(x)$	All elements satisfy P	One counterexample
Existential	$\exists x\, P(x)$	At least one satisfies P	Show all fail
Unique	$\exists!\, x\, P(x)$	Exactly one satisfies P	Show 0 or 2+ satisfy

Negation Rules (De Morgan for Quantifiers):

$$\neg\, \forall x\, P(x) \equiv \exists x\, \neg P(x) \qquad \neg\, \exists x\, P(x) \equiv \forall x\, \neg P(x)$$

Translation Strategy:

1. Identify all variables and assign predicate names.
2. Look for keywords: "all/every/each" $\Rightarrow \forall$; "some/there exists/at least one" $\Rightarrow \exists$.
3. "All A are B" $\Rightarrow \forall x\, (A(x) \to B(x))$.
4. "Some A is B" $\Rightarrow \exists x\, (A(x) \wedge B(x))$.
5. Note: use $\to$ with $\forall$; use $\wedge$ with $\exists$.

Past Paper Connection:

- **2021 Q1(i):** Define existential quantification $\to$ Definition 1.18, Example 2
- **2022 Q1(iv):** Truth value of $P(5)$ and $P(4)$ $\to$ Example 1
- **2023 Q1(iii):** Negation of "All goats are mammals" $\to$ Example 4
- **2023 Q1(v):** Translate sum of integers $\to$ Example 6
- **2024 Q1(vi):** Truth value of $\exists x\, \exists y\, P(x, y)$ $\to$ Example 7
- **2025 Q2:** Full quantifier translation problem $\to$ Example 5

Rules of Inference

Definition 1.22 — Argument and Valid Argument

An **argument** in propositional logic is a sequence of propositions. All propositions except the last are called **premises** (or hypotheses), and the last proposition is the **conclusion**.

An argument is **valid** if whenever all its premises are true, the conclusion is also true. Formally, the argument with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid if and only if:

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q \quad \text{is a } \textbf{tautology}.$$

Key Points:

- A valid argument does **not** guarantee that the conclusion is true — only that *if the premises are true, the conclusion must be true.*
- An argument can be valid even if some premises are false.
- The standard notation for an argument is:

$$\begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ \hline \therefore & q \end{array}$$

The symbol $\therefore$ means "therefore."

Theorem 1.5 — Rules of Inference for Propositional Logic

The following are the fundamental rules of inference. Each is a tautology.

Rule Name	Tautology	Argument Form
Modus Ponens	$(p \wedge (p \to q)) \to q$	$p, \quad p \to q \ \therefore\ q$
Modus Tollens	$(\neg q \wedge (p \to q)) \to \neg p$	$\neg q, \quad p \to q \ \therefore\ \neg p$
Hypothetical Syllogism	$((p \to q) \wedge (q \to r)) \to (p \to r)$	$p \to q,\ q \to r \ \therefore\ p \to r$
Disjunctive Syllogism	$((p \vee q) \wedge \neg p) \to q$	$p \vee q, \quad \neg p \ \therefore\ q$
Addition	$p \to (p \vee q)$	$p \ \therefore\ p \vee q$
Simplification	$(p \wedge q) \to p$	$p \wedge q \ \therefore\ p$
Conjunction	$((p) \wedge (q)) \to (p \wedge q)$	$p, \quad q \ \therefore\ p \wedge q$
Resolution	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	$p \vee q,\ \neg p \vee r \ \therefore\ q \vee r$

Proof of Modus Ponens: $(p \wedge (p \to q)) \to q$

Proof (by Truth Table):

We verify that the formula is a tautology.

p	q	$p \to q$	$p \wedge (p \to q)$	$[p \wedge (p \to q)] \to q$
T	T	T	T	**T**
T	F	F	F	**T**
F	T	T	F	**T**
F	F	T	F	**T**

All entries in the final column are **T**.
Conclusion: Modus Ponens is a tautology, confirming it is a valid rule of inference. □

Intuition: If we know "p" is true and we know "if p then q," then q *must* be true. This is the most natural step in any logical argument.

Proof of Modus Tollens: $(\neg q \wedge (p \to q)) \to \neg p$

Proof (using logical equivalences):

Step 1: Recall that $p \to q \equiv \neg q \to \neg p$ (contrapositive law).

Step 2: Modus Tollens has the form:

$$\neg q \quad \text{and} \quad p \to q \quad \therefore \quad \neg p$$

Step 3: Replace $p \to q$ with its contrapositive $\neg q \to \neg p$:

$$\neg q \quad \text{and} \quad \neg q \to \neg p \quad \therefore \quad \neg p$$

Step 4: This is exactly **Modus Ponens** applied to $\neg q$ and $\neg q \to \neg p$, which we already proved is valid.
Conclusion: Modus Tollens is valid. □

Example 1: Applying Modus Ponens — Past Paper 2025 Q1(xi)

State the Modus Ponens rule of inference and apply it to the following:
Premise 1: "If it is raining, then I will carry an umbrella."
Premise 2: "It is raining."
Conclusion: ?

Solution:

Step 1: Identify propositions.

- Let p = "It is raining"
- Let q = "I will carry an umbrella"

Step 2: Map to Modus Ponens form.

$$\begin{array}{ll} \text{Premise 1:} & p \to q \\ \text{Premise 2:} & p \\ \hline \therefore & q \end{array}$$

Step 3: Apply the rule.

Since we have p (it is raining) and $p \to q$ (if raining then umbrella), by Modus Ponens we conclude q.

Conclusion: "I will carry an umbrella."

$$\boxed{q : \text{"I will carry an umbrella."}}$$

Example 2: Applying Modus Tollens — Past Paper 2023 Q1(ii)

Define the Modus Tollens rule of inference and apply it:

Premise 1: "If Aslam studies hard, then he will pass."
Premise 2: "Aslam did not pass."
Conclusion: ?

Solution:

Modus Tollens: From $p \to q$ and $\neg q$, conclude $\neg p$.

Step 1: Assign propositions.

- p = "Aslam studies hard"
- q = "Aslam will pass"

Step 2: Map to rule form.

$$\begin{array}{ll} \text{Premise 1:} & p \to q \\ \text{Premise 2:} & \neg q \\ \hline \therefore & \neg p \end{array}$$

Conclusion: "Aslam did not study hard."

$$\boxed{\neg p : \text{"Aslam did not study hard."}}$$

Example 3: Hypothetical Syllogism — Past Paper 2020 Q1(xiii)

Identify the rule used and verify it:

$$p \to q, \quad q \to r \quad \therefore \quad p \to r$$

Solution:

Rule identified: Hypothetical Syllogism — if p implies q and q implies r, then p implies r (transitivity of implication).

English example:

- $p \to q$: "If I study, then I understand the material."
- $q \to r$: "If I understand the material, then I pass the exam."

- $\therefore\ p \to r$: "If I study, then I pass the exam."

Verification by truth table ($2^3 = 8$ rows):

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r) \to (p \to r)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	T	T
F	T	T	T	T	T
F	T	F	T	F	T
F	F	T	T	T	T
F	F	F	T	T	T

Conclusion: All T — Hypothetical Syllogism is a tautology.

$$\boxed{(p \to q) \wedge (q \to r) \to (p \to r) \ \equiv\ \mathbf{T}}$$

Example 4: Addition and Simplification — Past Paper 2021 Q1(ii)

Give examples of the Addition rule and the Simplification rule of inference.

Solution:

Addition Rule: From p, conclude $p \vee q$.

Form:

$$\begin{array}{ll} \text{Premise:} & p \\ \hline \therefore & p \vee q \end{array}$$

Example:

- Premise: "It is raining."
- Conclusion: "It is raining **or** the ground is dry."

Note: The added proposition q can be *anything* — even something false or unrelated. The conclusion is still valid because if p is true, then $p \vee q$ is certainly true.

Simplification Rule: From $p \wedge q$, conclude p.

Form:

$$\begin{array}{ll} \text{Premise:} & p \wedge q \\ \hline \therefore & p \end{array}$$

Example:

- Premise: "It is raining **and** it is cold."
- Conclusion: "It is raining."

Verification (Simplification):

p	q	$p \wedge q$	$(p \wedge q) \to p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

All T — ✓ Simplification is valid.

Example 5: Multi-Step Logical Argument

Show that the following argument is valid and find the conclusion:

Premises:

(1) It is not sunny this afternoon and it is colder than yesterday.

(2) We will go swimming only if it is sunny.

(3) If we do not go swimming, then we will take a canoe trip.

(4) If we take a canoe trip, then we will be home by sunset.

Solution:

Step 1: Assign propositions.

- p = "It is sunny this afternoon"
- q = "It is colder than yesterday"
- r = "We will go swimming"
- s = "We will take a canoe trip"
- t = "We will be home by sunset"

Step 2: Translate premises.

(1) $\neg p \wedge q$

(2) $r \to p$

(3) $\neg r \to s$

(4) $s \to t$

Step 3: Apply rules of inference step by step.

Step	Statement	Justification
5	$\neg p$	Simplification from (1): $\neg p \wedge q \Rightarrow \neg p$
6	$\neg r$	Modus Tollens from (2) and (5): $r \to p$, $\neg p \Rightarrow \neg r$
7	s	Modus Ponens from (3) and (6): $\neg r \to s$, $\neg r \Rightarrow s$
8	t	Modus Ponens from (4) and (7): $s \to t$, $s \Rightarrow t$

Conclusion: $\boxed{t}$ — "We will be home by sunset."

Definition 1.23 — Rules of Inference for Quantified Statements

The following rules extend propositional rules of inference to predicate logic.

Rule	Form	Meaning
Universal Instantiation	$\forall x\, P(x) \;\therefore\; P(c)$	If true for all, true for specific c
Universal Generalization	$P(c) \;\therefore\; \forall x\, P(x)$	If true for arbitrary c, true for all
Existential Instantiation	$\exists x\, P(x) \;\therefore\; P(c)$ for some c	Name the witness c
Existential Generalization	$P(c) \;\therefore\; \exists x\, P(x)$	One example proves existence

Important: Universal Generalization requires that c be a **completely arbitrary** element — no special assumptions may be made about it. Otherwise the generalization is invalid.

Example 6: Wumpus World Inference — Past Paper 2023 Q7

In a Wumpus world, we know the following facts:

(1) There is no Wumpus in room $(1, 1)$.

(2) There is no pit adjacent to room $(1, 1)$ (no Breeze in $(1, 1)$).

(3) If there is a Wumpus in a room, then adjacent rooms have Stench.

(4) If there is a pit in a room, then adjacent rooms have Breeze.

(5) Room $(1, 2)$ is adjacent to $(1, 1)$.

Use rules of inference to show that room $(1, 2)$ is **safe** (no Wumpus, no Pit).

Solution:

Assign propositions:

- W_{ij} = "There is a Wumpus in room (i, j)"
- P_{ij} = "There is a Pit in room (i, j)"
- S_{ij} = "There is Stench in room (i, j)"
- B_{ij} = "There is Breeze in room (i, j)"

Known facts:

(1) $\neg W_{11}$ (no Wumpus in (1,1))

(2) $\neg B_{11}$ (no Breeze in (1,1))

(3) $W_{12} \to S_{11}$ (Wumpus in (1,2) $\Rightarrow$ Stench in (1,1))

(4) $P_{12} \to B_{11}$ (Pit in (1,2) $\Rightarrow$ Breeze in (1,1))

Step	Statement	Justification
5	$\neg S_{11}$	From (1): no Wumpus anywhere near (1,1)
6	$\neg W_{12}$	Modus Tollens: (3) $W_{12} \to S_{11}$, $\neg S_{11}$
7	$\neg P_{12}$	Modus Tollens: (4) $P_{12} \to B_{11}$, $\neg B_{11}$
8	$\neg W_{12} \wedge \neg P_{12}$	Conjunction of (6) and (7)

Conclusion: Room $(1, 2)$ has neither a Wumpus nor a Pit.

$$\boxed{\neg W_{12} \wedge \neg P_{12} \quad \Rightarrow \quad \text{Room } (1,2) \text{ is } \textbf{safe}.}$$

Example 7: Conjunction Rule — Past Paper 2024 Q1(iii)

Define the conjunction rule of inference. Apply it to the following:
Premise 1: "Aslam is good in Maths."
Premise 2: "Aslam is a CS student."
Conclusion: ?
Let m = "Aslam is good in Maths" and c = "Aslam is a CS student."

Solution:

Conjunction Rule: If p is true and q is true, we may conclude $p \wedge q$.

$$\begin{array}{ll} \text{Premise 1:} & m \\ \text{Premise 2:} & c \\ \hline \therefore & m \wedge c \end{array}$$

Conclusion:

$$\boxed{m \wedge c : \text{"Aslam is good in Maths \textbf{and} is a CS student."}}$$

Verification:

m	c	$(m \wedge c)$ (from m and c)
T	T	T

When both premises are true, the conjunction is true. ✓

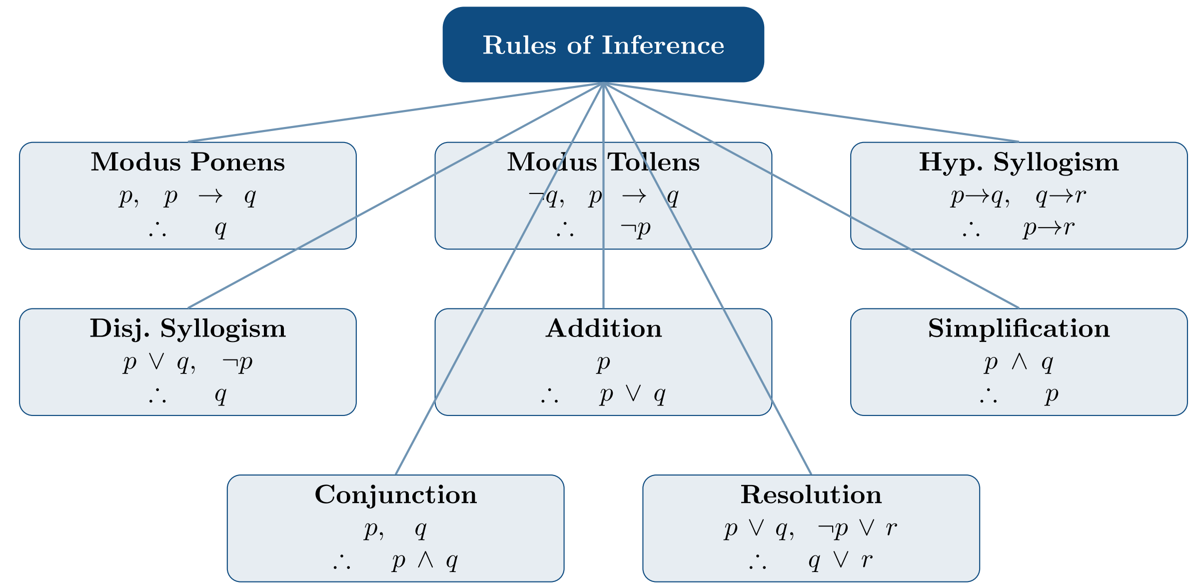


Figure 1.5: The eight fundamental rules of inference in propositional logic.

Section 1.5 Summary — Rules of Inference

The Eight Rules at a Glance:

Rule	Premises	Conclusion
Modus Ponens	$p,\ p \to q$	q
Modus Tollens	$\neg q,\ p \to q$	$\neg p$
Hyp. Syllogism	$p \to q,\ q \to r$	$p \to r$
Disj. Syllogism	$p \lor q,\ \neg p$	q
Addition	p	$p \lor q$
Simplification	$p \land q$	p
Conjunction	$p,\ q$	$p \land q$
Resolution	$p \lor q,\ \neg p \lor r$	$q \lor r$

Strategy for Multi-Step Arguments:

1. Assign a propositional variable to each atomic statement.
2. Translate all premises into symbolic form.
3. Apply rules one at a time, labelling each step with the rule used.
4. Build toward the desired conclusion systematically.
5. Common pattern: Simplification $\to$ Modus Tollens $\to$ Modus Ponens $\to$ Conjunction.

Past Paper Connection:

- **2020 Q1(xiii):** Name the rule $p{\to}q,\ q{\to}r\ \therefore\ p{\to}r$ $\to$ Hypothetical Syllogism, Example 3
- **2021 Q1(ii):** Addition and Simplification examples $\to$ Example 4

- **2023 Q1(ii):** Define Modus Tollens → Proof + Example 2
- **2023 Q7:** Wumpus world inference → Example 6
- **2024 Q1(iii):** Conjunction rule → Example 7
- **2025 Q1(xi):** State Modus Ponens → Proof + Example 1

Proof Techniques

A **proof** is a valid argument that establishes the truth of a mathematical statement. Every theorem in mathematics — no matter how complex — is ultimately justified by a chain of logical steps starting from known facts. In this section we study the four most important proof techniques used throughout discrete mathematics and computer science: **direct proof**, **proof by contraposition**, **proof by contradiction**, and **proof by mathematical induction**.

Definition 1.24 — Direct Proof

A **direct proof** of $p \to q$ proceeds by:

Step 1: Assume the hypothesis p is true.

Step 2: Use definitions, known theorems, and logical steps.

Step 3: Derive the conclusion q directly.

Key Points:

- The most natural and straightforward proof method.
- Works best when the hypothesis directly gives useful information.
- Always begin: "*Assume p is true. We will show q.*"

Example 1: Direct Proof — Even Number

Theorem: If n is an even integer, then n^2 is also even.

Solution:

Identify: $p =$ "n is even", $\quad q =$ "n^2 is even."

Proof:
Step 1: Assume p. Let n be an even integer.
Step 2: Use the definition. By definition of even, there exists an integer k such that:

$$n = 2k$$

Step 3: Derive q. Squaring both sides:

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

Let $m = 2k^2$. Since k is an integer, m is also an integer, and:

$$n^2 = 2m$$

By definition of even, n^2 is even.

Conclusion: If n is even, then n^2 is even. $\square$

Example 2: Direct Proof — Sum of Odd Numbers

Theorem: If m and n are both odd integers, then $m + n$ is even.

Solution:

Proof:
Step 1: Assume p. Let m and n be odd integers.
Step 2: Apply definition. By definition of odd, there exist integers j and k such that:

$$m = 2j + 1 \qquad \text{and} \qquad n = 2k + 1$$

Step 3: Derive q. Adding:

$$\begin{aligned} m + n &= (2j + 1) + (2k + 1) \\ &= 2j + 2k + 2 \\ &= 2(j + k + 1) \end{aligned}$$

Let $m' = j + k + 1$, which is an integer. Then $m + n = 2m'$, which is even by definition.

Conclusion: The sum of two odd integers is even. $\square$

Definition 1.25 — Proof by Contraposition

A **proof by contraposition** proves $p \to q$ by instead proving its logically equivalent contrapositive $\neg q \to \neg p$.

Step 1: Assume $\neg q$ (the negation of the conclusion).

Step 2: Derive $\neg p$ (the negation of the hypothesis).

Key Points:

- Valid because $p \to q \equiv \neg q \to \neg p$.
- Use this method when a direct proof seems difficult but the contrapositive is easier to work with.
- Always state: "*We prove the contrapositive: assume $\neg q$.*"
- Past Paper 2023 Q1(vi) directly asks: "Define converse" — students often confuse contrapositive with converse. Contrapositive $\equiv$ original; converse $\not\equiv$ original.

Example 3: Proof by Contraposition

Theorem: If n^2 is odd, then n is odd.

Solution:

Identify: $p =$ "n^2 is odd", $q =$ "n is odd."
Contrapositive: $\neg q \to \neg p$, i.e., "If n is even, then n^2 is even."

Proof (of the contrapositive):
Step 1: Assume $\neg q$. Assume n is even.
Step 2: Apply definition. There exists an integer k such that $n = 2k$.
Step 3: Derive $\neg p$.

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

This is even, i.e., n^2 is **not** odd, which is $\neg p$.

Since we proved $\neg q \to \neg p$, the original statement $p \to q$ ("if n^2 is odd, then n is odd") is also proved.

Conclusion: If n^2 is odd, then n is odd. □

Definition 1.26 — Proof by Contradiction (Reductio ad Absurdum)

A **proof by contradiction** proves a proposition p by:

Step 1: Assume $\neg p$ (the negation of what we want to prove).

Step 2: Derive a **contradiction** — a statement of the form $r \wedge \neg r$, which is always false.

Step 3: Conclude that $\neg p$ must be false, so p must be true.

Key Points:

- Based on the tautology: $(\neg p \to \mathbf{F}) \to p$.
- If assuming $\neg p$ leads to a logical impossibility, then $\neg p$ is false, so p must be true.
- Particularly useful for proving things are **irrational**, **infinite**, or **unique**.
- Always begin: "*Assume for contradiction that $\neg p$ is true.*"

Example 4: Proof by Contradiction — Irrationality of $\sqrt{2}$

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

Solution:

Step 1: Assume the negation.
Assume for contradiction that $\sqrt{2}$ is **rational**. Then there exist integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ (the fraction is in lowest terms) such that:

$$\sqrt{2} = \frac{a}{b}$$

Step 2: Derive consequences.
Squaring both sides:

$$2 = \frac{a^2}{b^2} \implies a^2 = 2b^2$$

So a^2 is even. By Example 3 (contrapositive result), if a^2 is even then a is even. Write $a = 2k$ for some integer k.

Step 3: Continue deriving.
Substituting $a = 2k$:

$$(2k)^2 = 2b^2 \implies 4k^2 = 2b^2 \implies b^2 = 2k^2$$

So b^2 is even, which means b is also even.
Step 4: Reach the contradiction.
Both a and b are even, so $2 \mid a$ and $2 \mid b$, meaning $\gcd(a, b) \geq 2$. But we assumed $\gcd(a, b) = 1$. This is a contradiction:

$$\gcd(a, b) = 1 \quad \text{AND} \quad \gcd(a, b) \geq 2 \qquad \Rightarrow \quad \mathbf{F}$$

Step 5: Conclude.
The assumption that $\sqrt{2}$ is rational leads to a contradiction. Therefore:
Conclusion: $\sqrt{2}$ is **irrational**. □

Example 5: Proof by Contradiction — Conditional Statement

Theorem: If n is an integer and n^2 is odd, then n is odd.
(Prove using contradiction, as an alternative to Example 3.)

Solution:

To prove $p \to q$ by contradiction, assume p is true and q is false, and derive a contradiction.
Step 1: Assume $p \wedge \neg q$.
Assume n^2 is odd (p **is true**) and n is even ($\neg q$ **is true**).
Step 2: Derive.
Since n is even, write $n = 2k$ for integer k. Then:

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

So n^2 is **even** — but we assumed n^2 is **odd**.
Step 3: Contradiction.

$$n^2 \text{ is odd} \quad \text{AND} \quad n^2 \text{ is even} \quad \Rightarrow \quad \mathbf{F}$$

Conclusion: The assumption $\neg q$ is false, so q ("n is odd") must be true. □

Definition 1.27 — Proof by Mathematical Induction

Mathematical induction is a proof technique used to prove that a proposition $P(n)$ is true for all positive integers $n \geq n_0$.

A proof by induction consists of **two steps**:

Step 1 — Base Case: Prove that $P(n_0)$ is true (usually $n_0 = 1$).

Step 2 — Inductive Step: Assume $P(k)$ is true for some arbitrary $k \geq n_0$ (this assumption is called the **inductive hypothesis**). Then prove that $P(k+1)$ is also true.

Key Points:

- Think of induction like a chain of dominoes: if the first falls (base case) and each domino knocks over the next (inductive step), then all dominoes fall.
- The inductive hypothesis is an **assumption**, not a proof — we assume $P(k)$ and use it to *prove* $P(k+1)$.
- Never use $P(k+1)$ to prove $P(k+1)$ — this is circular reasoning.
- **Strong induction** assumes $P(1), P(2), \ldots, P(k)$ are all true to prove $P(k+1)$ (covered in Past Paper 2023 Q1(vii)).

Theorem 1.6 — Sum of First n Positive Integers

For every positive integer n:

$$\sum_{i=1}^{n} i \;=\; 1+2+3+\cdots+n \;=\; \frac{n(n+1)}{2}$$

Proof of Theorem 1.6 by Mathematical Induction

Proof:

Let $P(n)$ denote the statement $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Step 1 — Base Case ($n = 1$):

→ Left-hand side: $\displaystyle\sum_{i=1}^{1} i = 1$

→ Right-hand side: $\dfrac{1 \cdot (1+1)}{2} = \dfrac{2}{2} = 1$

Both sides equal 1, so $P(1)$ is true. ✓

Step 2 — Inductive Step:

Assume $P(k)$ is true for some integer $k \geq 1$ (**inductive hypothesis**):

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

We must show $P(k+1)$ is true, i.e.:

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

➔ **Starting from the left-hand side of $P(k+1)$:**

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \qquad \text{(by the inductive hypothesis)} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

This is exactly the right-hand side of $P(k+1)$. ✓

Conclusion: By the principle of mathematical induction, $P(n)$ is true for all positive integers n. □

Example 6: Induction — Sum of Squares

Prove by induction that for all positive integers n:

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

Solution:

Let $P(n)$: $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

Base Case $(n = 1)$:

LHS $= 1^2 = 1$ RHS $= \dfrac{1 \cdot 2 \cdot 3}{6} = 1$ ✓

Inductive Step:

Assume $P(k)$: $\displaystyle\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$.

Show $P(k+1)$: $\displaystyle\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \sum_{i=1}^{k} i^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \qquad \text{(inductive hypothesis)} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)\left[k(2k+1) + 6(k+1)\right]}{6} \\
&= \frac{(k+1)(2k^2 + k + 6k + 6)}{6} \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}
\end{aligned}$$

This matches the RHS of $P(k+1)$. ✓
Conclusion: By induction, the formula holds for all $n \geq 1$. □

Example 7: Induction — Powers of 2

Prove by induction that for all non-negative integers n:

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Solution:

Let $P(n)$: $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

Base Case ($n = 0$):
LHS $= 2^0 = 1$ RHS $= 2^{0+1} - 1 = 2 - 1 = 1$ ✓

Inductive Step:

Assume $P(k)$: $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$.

Show $P(k+1)$: $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$.

$$\begin{aligned}
\sum_{i=0}^{k+1} 2^i &= \sum_{i=0}^{k} 2^i + 2^{k+1} \\
&= (2^{k+1} - 1) + 2^{k+1} \qquad \text{(inductive hypothesis)} \\
&= 2 \cdot 2^{k+1} - 1 \\
&= 2^{k+2} - 1
\end{aligned}$$

This matches $P(k+1)$. ✓
Conclusion: The formula holds for all $n \geq 0$. □

Definition 1.28 — Strong Induction

In **strong induction** (also called *complete induction*), the inductive hypothesis is strengthened: instead of assuming only $P(k)$, we assume $P(1), P(2), \ldots, P(k)$ are **all true**, and use this to prove $P(k+1)$.

Comparison with ordinary induction:

Feature	Ordinary Induction	Strong Induction
Base case	Prove $P(1)$	Prove $P(1)$ (sometimes more)
Inductive hypothesis	Assume $P(k)$	Assume $P(1), \ldots, P(k)$
Inductive step	Prove $P(k+1)$	Prove $P(k+1)$
Power	Less flexible	More flexible

Note: Strong induction and ordinary induction are **logically equivalent** — any theorem provable by one can be proved by the other. Strong induction is simply more convenient in some cases. (Past Paper 2023 Q1(vii) asks to differentiate between these two.)

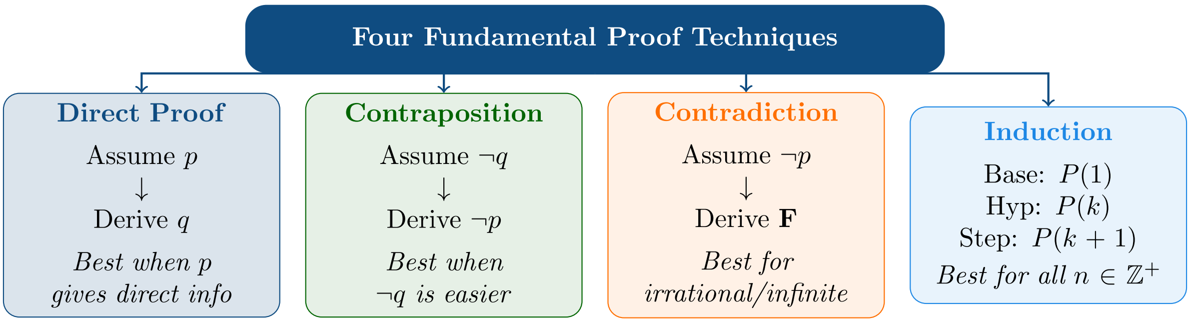


Figure 1.6: Choosing the right proof technique based on the structure of the theorem.

Example 8: Proof by Contradiction — Big-O — Past Paper 2020 Q5(a)

Show that n^2 is **not** $O(n)$.

Solution:

Recall: $f(n)$ is $O(g(n))$ if there exist positive constants C and k such that:

$$f(n) \leq C \cdot g(n) \quad \text{for all } n > k$$

Step 1: Assume for contradiction that n^2 IS $O(n)$.
Then there exist positive constants C and k such that for all $n > k$:

$$n^2 \leq C \cdot n$$

Step 2: Derive consequences.

Dividing both sides by n (valid since $n > 0$):

$$n \leq C \quad \text{for all } n > k$$

Step 3: Reach the contradiction.

This claims n is bounded above by the constant C for all $n > k$. But n grows without bound — for any constant C, we can choose $n = \lfloor C \rfloor + 1 > k$ (by taking k large enough), giving $n > C$. This contradicts $n \leq C$.

Conclusion: n^2 is **not** $O(n)$. □

Section 1.6 Summary — Proof Techniques

When to Use Which Technique:

Technique	When to use	Key move
Direct Proof	p gives useful info	Assume p, derive q
Contraposition	$\neg q$ is easier to use	Assume $\neg q$, derive $\neg p$
Contradiction	Proving irrationality, infinity	Assume $\neg p$, derive $\mathbf{F}$
Induction	All $n \in \mathbb{Z}^+$	Base + inductive step
Strong Induction	Need earlier cases	Assume $P(1), \ldots, P(k)$

Induction Checklist:

1. State $P(n)$ clearly.
2. Prove the base case explicitly.
3. Write: "Assume $P(k)$ is true for some $k \geq 1$."
4. Write: "We will show $P(k+1)$ is true."
5. Start from the LHS of $P(k+1)$, use the inductive hypothesis, reach the RHS.
6. Conclude: "By induction, $P(n)$ holds for all $n \geq 1$."

Key Formulas Proved by Induction:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \qquad \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Past Paper Connection:

- **2020 Q5(a):** n^2 is not $O(n)$ → Example 8
- **2023 Q1(vi):** Define converse (vs. contrapositive) → Definition 1.25
- **2023 Q1(vii):** Differentiate induction and strong induction → Definition 1.28

Practice Exercises

Q1. Let p = "The program compiles" and q = "The output is correct." Write the following in symbolic form:

(i) The program compiles but the output is not correct.

(ii) If the program does not compile, then the output is not correct.

(iii) The output is correct if and only if the program compiles.

(iv) The program does not compile or the output is correct.

(v) It is not the case that the program compiles and the output is correct.

Q2. Construct a complete truth table for each of the following:

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

(ii) $\neg(p \lor q) \leftrightarrow (\neg p \land \neg q)$

(iii) $(p \oplus q) \leftrightarrow \neg(p \leftrightarrow q)$

For each, state whether the result is a tautology, contradiction, or contingency.

Q3. Given p = T, q = F, r = T, evaluate each of the following without constructing a full truth table:

(i) $p \land (\neg q \lor r)$

(ii) $(p \to q) \leftrightarrow (\neg p \lor q)$

(iii) $\neg(p \land q) \lor (q \to r)$

(iv) $(p \oplus q) \land (q \oplus r)$

Q4. Write each of the following English sentences in symbolic form. Define your propositional variables clearly before translating.

(i) "You can access the internet only if you have a valid password."

(ii) "The server is down or the network is congested, but not both."

(iii) "Whenever it snows, classes are cancelled."

(iv) "A necessary condition for passing the exam is attending all lectures."

(v) "Either the database is full or the query failed, and the report was not generated."

Q5. For the conditional "If a number is divisible by 6, then it is divisible by 2," write the:

(i) Converse

(ii) Inverse

(iii) Contrapositive

(iv) Negation of the original conditional

State which of the above are logically equivalent to the original conditional and explain why.

Q6. Using only the laws of propositional logic (no truth tables), simplify each expression to its simplest equivalent form. Name every law you use.

(i) $p \wedge (p \vee q)$

(ii) $(p \vee q) \wedge (\neg p \vee q)$

(iii) $\neg(\neg p \vee \neg q) \vee \neg(p \wedge q)$

Q7. Show that each of the following is a tautology **without using a truth table**. Use only logical equivalences and laws.

(i) $\neg(p \wedge \neg p)$

(ii) $(p \to q) \vee (q \to p)$

(iii) $\big[(p \to q) \wedge (q \to r)\big] \to (p \to r)$

Q8. Apply De Morgan's Laws to find the negation of each of the following statements. Express your final answer in plain English.

(i) "Ali is rich and happy."

(ii) "The car is fast or expensive."

(iii) "It is raining and the roads are wet."

(iv) "Sara will pass all her courses or take a gap year."

Q9. Find the **dual** of each of the following compound propositions:

(i) $(p \wedge \mathbf{T}) \vee (q \wedge \mathbf{F})$

(ii) $(p \vee q) \wedge \neg r$

(iii) $\neg p \wedge (q \vee \mathbf{T})$

After finding each dual, simplify both the original and the dual using the laws of logic.

Q10. Prove the following logical equivalences using a series of logical equivalences. Name each law applied at every step.

(i) $p \to (p \to q) \;\equiv\; p \to q$

(ii) $(p \wedge q) \to r \;\equiv\; p \to (q \to r)$

Q11. Let the domain be all integers. Determine the truth value of each quantified statement. Justify your answer by providing a witness (for existence) or a counterexample (for universals that are false).

(i) $\forall x\,(x^2 \geq 0)$

(ii) $\exists x\,(x^2 = -1)$

(iii) $\forall x\,(x^2 > x)$

(iv) $\exists x\,(x^2 = x)$

(v) $\forall x\, \exists y\, (x + y = 0)$

Q12. Write the negation of each statement, pushing the negation sign as far inward as possible. Then translate the negation back into plain English.

(i) $\forall x\, (P(x) \to Q(x))$

(ii) $\exists x\, (P(x) \land \neg Q(x))$

(iii) $\forall x\, \forall y\, (x + y = y + x)$

(iv) $\exists x\, \forall y\, (x \cdot y = 0)$

Q13. Let $L(x, y)$ denote "x loves y," where the domain is all people. Express each of the following in plain English and then determine whether it is the same as, stronger than, or weaker than the others.

(i) $\forall x\, \exists y\, L(x, y)$

(ii) $\exists y\, \forall x\, L(x, y)$

(iii) $\exists x\, \exists y\, L(x, y)$

(iv) $\forall x\, \forall y\, L(x, y)$

Q14. Identify the rule of inference used in each of the following arguments. State the rule by name and write it in symbolic form.

(i) "It is below freezing now. Therefore, it is below freezing or it is raining."

(ii) "It is below freezing and raining. Therefore, it is below freezing."

(iii) "If it rains, the picnic is cancelled. It did not rain. Therefore, the picnic was not cancelled." (Is this valid? Explain.)

(iv) "If you study, you will pass. If you pass, you will graduate. Therefore, if you study, you will graduate."

(v) "Either the butler or the maid committed the crime. The butler did not commit it. Therefore, the maid committed it."

Q15. Determine whether each of the following arguments is **valid** or **invalid**. If valid, name the rule. If invalid, explain the fallacy.

(i) Premises: $p \to q,\ q$. Conclusion: p.

(ii) Premises: $p \to q,\ \neg p$. Conclusion: $\neg q$.

(iii) Premises: $p \lor q,\ \neg q \lor r$. Conclusion: $p \lor r$.

(iv) Premises: $p \to q,\ p \to r$. Conclusion: $q \to r$.

Q16. Using the rules of inference, show that the conclusion follows from the premises. Show every step and name the rule used.

Premises:

(1) $\neg p \vee q$

(2) $\neg q \vee r$

(3) $\neg r$

Conclusion: $\neg p$

Q17. Prove each of the following using a **direct proof**:

(i) If n is an odd integer, then n^2 is odd.

(ii) If m is even and n is odd, then $m + n$ is odd.

(iii) If n is an integer divisible by 3, then n^2 is divisible by 9.

Q18. Prove each of the following using **proof by contraposition**:

(i) If n^2 is even, then n is even.

(ii) If $3n + 2$ is odd, then n is odd.

(iii) If the product mn is odd, then both m and n are odd.

Q19. Prove each of the following using **proof by contradiction**:

(i) $\sqrt{3}$ is irrational.

(ii) There is no greatest even integer.

(iii) If n^2 is odd, then n is odd (use contradiction this time).

Q20. Prove each of the following by **mathematical induction**:

(i) $\displaystyle\sum_{i=1}^{n}(2i - 1) = n^2$ (sum of first n odd numbers)

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

(iii) $2^n < n!$ for all integers $n \geq 4$

(iv) $n^2 \leq 2^n$ for all integers $n \geq 4$

Exam Preparation Tips for Chapter 1

- **Q1–Q5** target objective-type questions (2 marks each in past papers).
- **Q6–Q10** target 12-mark subjective questions on equivalences and laws.
- **Q11–Q13** cover predicate logic, which appears in both objective and subjective parts every year.
- **Q14–Q16** cover rules of inference — always present in at least one subjective question.

- **Q17–Q20** cover all four proof techniques — induction questions appear almost every year; master the template in Definition 1.27.
- For induction proofs, always state $P(n)$, prove the base case explicitly, state the inductive hypothesis formally, and show every algebra step.

Chapter 2

Set Theory and Relations

Sets

A **set** is one of the most primitive and powerful concepts in all of mathematics. Every branch of mathematics — number theory, graph theory, logic, analysis — is built on the foundation of sets. In computer science, sets appear in databases, programming languages, algorithms, and formal verification.

Definition 2.1 — Set

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

Notation:

- Sets are denoted by **capital letters**: $A, B, C, S, \ldots$
- Elements are denoted by **lowercase letters**: $a, b, x, y, \ldots$
- $a \in A$ means "a **is an element of** A" (read: "a is in A")
- $a \notin A$ means "a **is not an element of** A"
- Sets are **unordered**: $\{1, 2, 3\} = \{3, 1, 2\} = \{2, 3, 1\}$
- Elements are **distinct**: $\{1, 1, 2\}$ is the same set as $\{1, 2\}$

Definition 2.2 — Three Ways to Describe a Set

1. Roster (Enumeration) Method: List all elements explicitly inside braces.

$$A = \{1,\ 2,\ 3,\ 4,\ 5\}$$

2. Set-Builder (Predicate) Notation: Describe elements by a property $P(x)$.

$$A = \{x \mid P(x)\} \quad \text{or} \quad A = \{x : P(x)\}$$

Read: "the set of all x such that $P(x)$ is true."

3. Verbal Description: Describe in plain words, e.g. "the set of all even positive integers less than 10."

Standard Number Sets:

Symbol	Name	Elements
$\mathbb{N}$	Natural numbers	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	Integers	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}^+$	Positive integers	$\{1, 2, 3, \ldots\}$
$\mathbb{Q}$	Rational numbers	$\{p/q \mid p, q \in \mathbb{Z},\ q \neq 0\}$
$\mathbb{R}$	Real numbers	All points on the number line
$\mathbb{C}$	Complex numbers	$\{a + bi \mid a, b \in \mathbb{R}\}$

Example 1: Describing Sets in Multiple Ways

Let A be the set of odd positive integers less than 10.

Solution:

Roster method:

$$A = \{1,\ 3,\ 5,\ 7,\ 9\}$$

Set-builder notation:

$$A = \{x \in \mathbb{Z}^+ \mid x \text{ is odd and } x < 10\}$$

or equivalently:

$$A = \{x \mid x = 2k - 1,\ k \in \mathbb{Z}^+,\ x < 10\}$$

Cardinality: $|A| = 5$ (the set has 5 elements)

Membership checks:

- $3 \in A$ ✓ True
- $4 \in A$ × False
- $11 \in A$ × False (11 is not less than 10)

(Past Paper 2022 Q1(viii) directly asks: "Let A be the set of odd positive integers less than 10. Then $|A| =$?" Answer: $|A| = 5$.)

Definition 2.3 — Special Sets

Empty Set: The set with no elements, written $\emptyset$ or $\{\}$.

$$\emptyset = \{\} \qquad |\emptyset| = 0$$

Universal Set: The set U containing all objects under consideration in a particular context (the "universe of discourse").

Singleton Set: A set with exactly one element, e.g. $\{5\}$ or $\{\emptyset\}$.

Critical Warning:

- $\emptyset \neq \{\emptyset\}$ — the empty set has 0 elements; the set $\{\emptyset\}$ has **1** element (the empty set itself).
- $0 \neq \emptyset$ — zero is a number, not a set.
- $\{0\} \neq \emptyset$ — $\{0\}$ is a set containing the number zero.

Definition 2.4 — Subset and Proper Subset

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

$$A \subseteq B \iff \forall x\,(x \in A \to x \in B)$$

Set A is a **proper subset** of B, written $A \subset B$ (or $A \subsetneq B$), if $A \subseteq B$ **and** $A \neq B$ (i.e., B has at least one element not in A).

Key Properties:

- $\emptyset \subseteq A$ for **every** set A (the empty set is a subset of every set).
- $A \subseteq A$ for every set A (every set is a subset of itself).
- $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$
- If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$ (transitivity).
- $A \not\subseteq B$ means $\exists x\,(x \in A \wedge x \notin B)$.

Example 2: Identifying Subsets

Let $A = \{1, 2\}$, $B = \{1, 2, 3\}$, $C = \{2, 3, 4\}$, $D = \{1, 2\}$.

Determine which of the following are true:

(i) $A \subseteq B$

(ii) $B \subseteq A$

(iii) $A \subset D$

(iv) $A = D$

(v) $\emptyset \subseteq A$

(vi) $A \subseteq C$

Solution:

Statement	Reasoning	True/False
$A \subseteq B$	$1 \in B$ and $2 \in B$, so every element of A is in B	✓ True
$B \subseteq A$	$3 \in B$ but $3 \notin A$, so $B \not\subseteq A$	× False
$A \subset D$	$A \subseteq D$ but $A = D$ (not proper)	× False
$A = D$	Both contain exactly $\{1, 2\}$	✓ True
$\emptyset \subseteq A$	Empty set is subset of every set	✓ True
$A \subseteq C$	$1 \in A$ but $1 \notin C$	× False

Definition 2.5 — Cardinality

The **cardinality** of a set A, written $|A|$ or $\#A$, is the **number of distinct elements** in A.

Set	Cardinality
$\emptyset$	0
$\{a, b, c\}$	3
$\{1, 1, 2, 3\}$	3 (duplicates don't count)
$\{\emptyset\}$	1
$\{\emptyset, \{1\}, \{1, 2\}\}$	3

A set is called **finite** if its cardinality is a non-negative integer. Otherwise it is **infinite** (e.g. $\mathbb{Z}$, $\mathbb{R}$).

Definition 2.6 — Power Set

The **power set** of a set A, written $\mathcal{P}(A)$ or 2^A, is the set of **all subsets** of A, including $\emptyset$ and A itself.

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

Key Formula:

$$\text{If } |A| = n, \text{ then } |\mathcal{P}(A)| = 2^n$$

Why 2^n? Each element of A is *either included or excluded* from a subset — 2 choices per element, n elements, so $2 \times 2 \times \cdots \times 2 = 2^n$ subsets in total.

Theorem 2.1 — Cardinality of the Power Set

If A is a finite set with $|A| = n$, then:

$$|\mathcal{P}(A)| = 2^n$$

In particular, $|\mathcal{P}(\emptyset)| = 2^0 = 1$, since $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Example 3: Power Set — Past Paper 2020 Q1(xi)

Find the power set of $A = \{1, 3, 5\}$.

Solution:

$|A| = 3$, so $|\mathcal{P}(A)| = 2^3 = 8$ subsets.

Systematic enumeration (by number of elements in each subset):

Subset Size	Subsets
0 elements	$\emptyset$
1 element	$\{1\}, \quad \{3\}, \quad \{5\}$
2 elements	$\{1, 3\}, \quad \{1, 5\}, \quad \{3, 5\}$
3 elements	$\{1, 3, 5\}$

Therefore:

$$\boxed{\mathcal{P}(A) = \{\, \emptyset,\ \{1\},\ \{3\},\ \{5\},\ \{1, 3\},\ \{1, 5\},\ \{3, 5\},\ \{1, 3, 5\} \,\}}$$

Verification: $|\mathcal{P}(A)| = 8 = 2^3$ ✓

Example 4: Power Set of the Empty Set — Past Paper 2022 Q1(x)

What is the power set of the empty set $\emptyset$?

Solution:

$|\emptyset| = 0$, so $|\mathcal{P}(\emptyset)| = 2^0 = 1$.
The only subset of the empty set is the empty set itself.

$$\boxed{\mathcal{P}(\emptyset) = \{\emptyset\}}$$

Common Mistake: Students often write $\mathcal{P}(\emptyset) = \emptyset$ (the empty set). This is wrong. $\mathcal{P}(\emptyset)$ is **not empty** — it contains one element: the empty set. Always remember:

$$|\mathcal{P}(\emptyset)| = 2^0 = 1 \neq 0$$

Definition 2.7 — Ordered Pair and Cartesian Product

An **ordered pair** (a, b) is a pair of elements where order matters: $(a, b) \neq (b, a)$ in general.

The **Cartesian product** of sets A and B, written $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$:

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

Cardinality: $|A \times B| = |A| \cdot |B|$

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

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\} \qquad |A \times B| = 4$$

Note: $A \times B \neq B \times A$ in general (order of pairs is reversed).

Example 5: Cartesian Product and Subsets

Let $A = \{0, 1\}$ and $B = \{a, b, c\}$.

(a) Find $A \times B$.

(b) Find $B \times A$.

(c) Is $A \times B = B \times A$?

(d) How many subsets does $A \times B$ have?

Solution:

(a)

$$A \times B = \{(0,a),\ (0,b),\ (0,c),\ (1,a),\ (1,b),\ (1,c)\} \qquad |A \times B| = 6$$

(b)

$$B \times A = \{(a,0),\ (a,1),\ (b,0),\ (b,1),\ (c,0),\ (c,1)\} \qquad |B \times A| = 6$$

(c) $A \times B \neq B \times A$ because, for example, $(0,a) \in A \times B$ but $(0,a) \notin B \times A$ (since $0 \notin B$). Not equal.

(d) $|A \times B| = 6$, so $|\mathcal{P}(A \times B)| = 2^6 = \boxed{64}$ subsets.

Example 6: Using Set-Builder Notation

Express each set using set-builder notation, then find its cardinality:

(a) The set of all positive integers less than or equal to 100 that are divisible by both 3 and 5.

(b) The set of all real solutions to $x^2 - 5x + 6 = 0$.

Solution:

(a) A number is divisible by both 3 and 5 iff it is divisible by $\mathrm{lcm}(3,5) = 15$.

$$A = \{x \in \mathbb{Z}^+ \mid x \leq 100 \text{ and } 15 \mid x\} = \{15, 30, 45, 60, 75, 90\}$$

$$|A| = \left\lfloor \frac{100}{15} \right\rfloor = 6$$

(b) Solve $x^2 - 5x + 6 = 0$:

$$(x-2)(x-3) = 0 \implies x = 2 \text{ or } x = 3$$

$$B = \{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0\} = \{2, 3\} \qquad |B| = 2$$

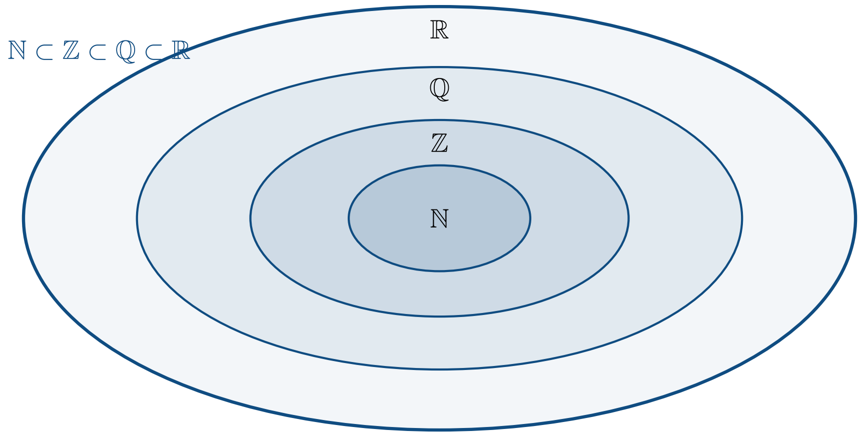
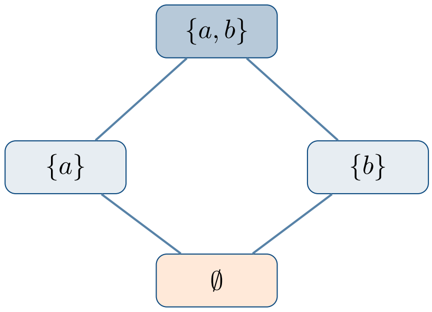


Figure 2.1: The nested subset relationship between standard number sets.

$$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$$



Hasse diagram: each node is a subset; upper nodes contain lower ones

Figure 2.2: Power set of $\{a,b\}$ shown as a Hasse diagram. $|\mathcal{P}(\{a,b\})| = 2^2 = 4$.

Section 2.1 Summary — Sets, Subsets & Power Sets

Key Facts at a Glance:

Concept	**Formula / Fact**
Cardinality	$\lvert A\rvert$ = number of distinct elements
Subset	$A \subseteq B \iff \forall x\,(x \in A \to x \in B)$
Proper subset	$A \subset B \iff A \subseteq B$ and $A \neq B$
Set equality	$A = B \iff A \subseteq B$ and $B \subseteq A$
Power set size	$\lvert\mathcal{P}(A)\rvert = 2^{\lvert A\rvert}$
Cartesian product	$\lvert A \times B\rvert = \lvert A\rvert \cdot \lvert B\rvert$
Empty set	$\emptyset \subseteq A$ for every set A
$\mathcal{P}(\emptyset)$	$= \{\emptyset\}$, cardinality $= 1$

Power Set Quick Reference:

$\lvert A\rvert$	$\lvert\mathcal{P}(A)\rvert$	Example
0	1	$\mathcal{P}(\emptyset) = \{\emptyset\}$
1	2	$\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}$
2	4	$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$
3	8	$\mathcal{P}(\{1,3,5\})$ has 8 subsets
n	2^n	General formula

Past Paper Connection:

- **2020 Q1(xi):** Power set of $\{1,3,5\} \to$ Example 3
- **2022 Q1(viii):** $\lvert A\rvert$ where A is odd integers $< 10 \to$ Example 1
- **2022 Q1(x):** Power set of $\emptyset \to$ Example 4

Set Operations and Venn Diagrams

Definition 2.8 — Union

The **union** of sets A and B, written $A \cup B$, is the set of all elements that belong to A **or** B (or both):

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Key Points:

- $\cup$ corresponds to the logical connective $\vee$ (OR).
- $A \cup B$ always contains **at least** as many elements as A or B alone.
- $A \subseteq A \cup B$ and $B \subseteq A \cup B$.
- $A \cup A = A$ (idempotent)
- $A \cup \emptyset = A$ (identity)
- $A \cup U = U$ (domination, where U is the universal set)

Definition 2.9 — Intersection

The **intersection** of sets A and B, written $A \cap B$, is the set of all elements that belong to **both** A and B:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Key Points:

- $\cap$ corresponds to the logical connective $\wedge$ (AND).
- $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
- $A \cap A = A$ (idempotent)
- $A \cap \emptyset = \emptyset$ (domination)
- $A \cap U = A$ (identity)
- Two sets are **disjoint** if $A \cap B = \emptyset$.

Definition 2.10 — Complement

The **complement** of set A with respect to universal set U, written $\overline{A}$ or A^c or A', is the set of all elements in U that are **not** in A:

$$\overline{A} = \{x \in U \mid x \notin A\}$$

Key Properties:

- $\overline{A}$ corresponds to the logical connective $\neg$ (NOT).
- $\overline{\overline{A}} = A$ (double complement)
- $A \cup \overline{A} = U$ (complement law)

- $A \cap \overline{A} = \emptyset$ (complement law)
- $\overline{U} = \emptyset$ and $\overline{\emptyset} = U$

Definition 2.11 — Set Difference and Symmetric Difference

The **set difference** (or *relative complement*) of B from A, written $A - B$ or $A \setminus B$, is the set of elements in A but **not** in B:

$$A - B = \{x \mid x \in A \land x \notin B\} = A \cap \overline{B}$$

The **symmetric difference** of A and B, written $A \oplus B$ (or $A \triangle B$), is the set of elements in **exactly one** of A or B:

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

Note: $A \oplus B$ in set theory corresponds to $p \oplus q$ (exclusive or) in propositional logic. Past Paper 2023 Q1(x) asks to draw the Venn diagram for symmetric difference.

Example 1: Computing All Set Operations

Let $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7\}$.
Find: (a) $A \cup B$ (b) $A \cap B$ (c) $\overline{A}$ (d) $A - B$ (e) $B - A$ (f) $A \oplus B$

Solution:

(a) Union — elements in A *or* B:

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$$

(b) Intersection — elements in both A *and* B:

$$A \cap B = \{3, 4, 5\}$$

(c) Complement of A — elements in U but not in A:

$$\overline{A} = \{6, 7, 8\}$$

(d) $A - B$ — elements in A but not in B:

$$A - B = \{1, 2\}$$

(e) $B - A$ — elements in B but not in A:

$$B - A = \{6, 7\}$$

(f) Symmetric difference — elements in exactly one of A, B:

$$A \oplus B = (A - B) \cup (B - A) = \{1, 2\} \cup \{6, 7\} = \{1, 2, 6, 7\}$$

Verification: $A \oplus B = (A \cup B) - (A \cap B) = \{1, 2, 3, 4, 5, 6, 7\} - \{3, 4, 5\} = \{1, 2, 6, 7\}$ ✓

Definition 2.12 — De Morgan's Laws for Sets

For any sets A, B within a universal set U:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Connection to Logic:

These are the set-theory counterparts of De Morgan's Laws for propositions (Section 1.3). The correspondence is:

Set Theory	Propositional Logic
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$

(Past Paper 2024 Q1(i) directly asks: "Define De Morgan's Law in set theory.")

Theorem 2.2 — De Morgan's First Law for Sets

For any sets A and B within universal set U:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Proof of Theorem 2.2 — De Morgan's First Law

Proof (using set-builder notation and logical equivalences):

Step 1: We prove the two sets are equal by showing each is a subset of the other.

(⊆) Show $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$:
Let $x \in \overline{A \cup B}$.

$$\begin{aligned} x \in \overline{A \cup B} &\implies x \notin A \cup B \\ &\implies \neg(x \in A \vee x \in B) \\ &\implies (x \notin A) \wedge (x \notin B) && \text{(De Morgan for logic)} \\ &\implies x \in \overline{A} \wedge x \in \overline{B} \\ &\implies x \in \overline{A} \cap \overline{B} \end{aligned}$$

(⊇) Show $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$:
Let $x \in \overline{A} \cap \overline{B}$.

$$\begin{aligned} x \in \overline{A} \cap \overline{B} &\implies x \in \overline{A} \wedge x \in \overline{B} \\ &\implies (x \notin A) \wedge (x \notin B) \\ &\implies \neg(x \in A \vee x \in B) && \text{(De Morgan for logic)} \\ &\implies x \notin A \cup B \\ &\implies x \in \overline{A \cup B} \end{aligned}$$

Step 2: Conclude equality.
Since $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ and $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$, we have:

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \square$$

Example 2: De Morgan's Law Application — Past Paper 2024 Q1(i)

Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{4, 5, 6, 7, 8\}$.
Verify De Morgan's First Law: $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Solution:

Left-hand side:

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\} \implies \overline{A \cup B} = \{9, 10\}$$

Right-hand side:

$$\overline{A} = \{6, 7, 8, 9, 10\}, \quad \overline{B} = \{1, 2, 3, 9, 10\}$$

$$\overline{A} \cap \overline{B} = \{9, 10\}$$

Both sides equal $\{9, 10\}$. De Morgan's Law verified.

$$\boxed{\overline{A \cup B} = \overline{A} \cap \overline{B} = \{9, 10\}} \quad \checkmark$$

Example 3: Set-Builder Proof of De Morgan — Past Paper 2022 Q6(a)

Use set-builder notation and logical equivalences to establish:

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

Solution:

We prove this by showing membership equivalence:

$$\begin{aligned}
x \in (A \cap B)' &\iff x \notin A \cap B \\
&\iff \neg(x \in A \land x \in B) \\
&\iff (\neg x \in A) \lor (\neg x \in B) && \text{De Morgan's Law for logic} \\
&\iff (x \notin A) \lor (x \notin B) \\
&\iff x \in A' \lor x \in B' \\
&\iff x \in A' \cup B'
\end{aligned}$$

Since $x \in (A \cap B)'$ if and only if $x \in A' \cup B'$:

$$\boxed{(A \cap B)' = A' \cup B'} \quad \square$$

Theorem 2.3 — Laws of Set Theory

The following identities hold for all sets A, B, C within universal set U:

Law Name	**Union Form**	**Intersection Form**
Identity	$A \cup \emptyset = A$	$A \cap U = A$
Domination	$A \cup U = U$	$A \cap \emptyset = \emptyset$
Idempotent	$A \cup A = A$	$A \cap A = A$
Complement	$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$
Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgan	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Double Comp.	$\overline{\overline{A}} = A$	

Venn Diagrams: A **Venn diagram** represents sets as overlapping circles inside a rectangle (the universal set U). Shaded regions indicate the result of set operations.

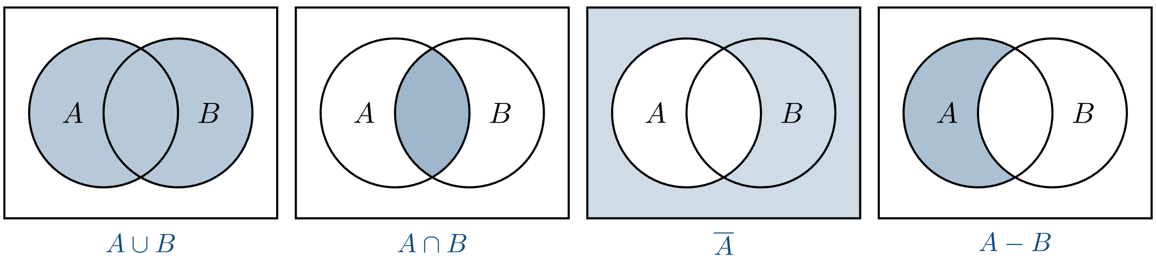


Figure 2.3: Venn diagrams for union, intersection, complement, and set difference.

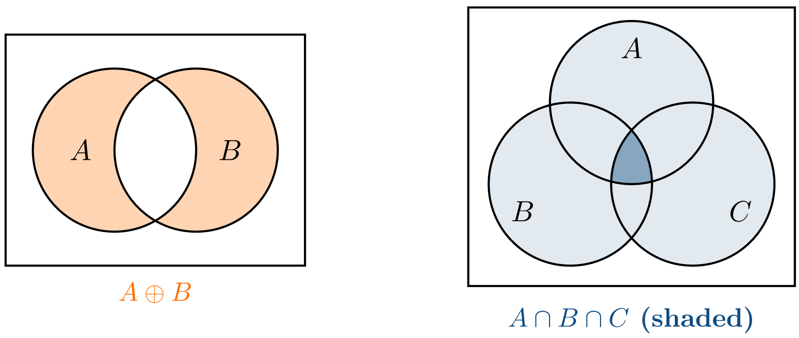


Figure 2.4: Symmetric difference $A \oplus B$ (left) and three-set Venn diagram with $A \cap B \cap C$ highlighted (right).

Example 4: Symmetric Difference Venn Diagram — Past Paper 2023 Q1(x)

Draw the Venn diagram for the symmetric difference of $A = \{1, 3, 5\}$ and $B = \{1, 2, 3\}$. Also compute $A \oplus B$.

Solution:

Step 1: Identify the regions.

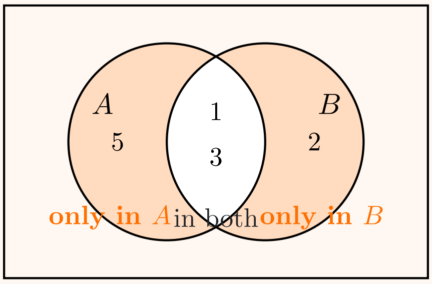
- $A \cap B = \{1, 3\}$ (in both — **not** in symmetric difference)

- $A - B = \{5\}$ (only in A — **in** symmetric difference)
- $B - A = \{2\}$ (only in B — **in** symmetric difference)

Step 2: Compute $A \oplus B$.

$$A \oplus B = (A - B) \cup (B - A) = \{5\} \cup \{2\} = \boxed{\{2, 5\}}$$

Step 3: Venn diagram placement.



The **shaded regions** (only in A or only in B) form $A \oplus B = \{2, 5\}$.

Example 5: Inclusion-Exclusion Principle

In a class of 50 students, 30 like Mathematics, 25 like Computer Science, and 10 like both. How many students like at least one of the two subjects?

Solution:

Let M = set of students who like Maths, C = set who like CS.
Given: $|M| = 30$, $|C| = 25$, $|M \cap C| = 10$.
Apply the Inclusion-Exclusion Principle:

$$|M \cup C| = |M| + |C| - |M \cap C| = 30 + 25 - 10 = \boxed{45}$$

Students who like **neither**: $50 - 45 = 5$.

Note: We subtract $|M \cap C|$ because students in both sets get counted *twice* in $|M| + |C|$, so we correct by subtracting one copy.

Example 6: Simplifying Set Expressions

Simplify $(A \cup B) \cap (A \cup \overline{B})$.

Solution:

Expression	Law Applied
$(A \cup B) \cap (A \cup \overline{B})$	Given
$A \cup (B \cap \overline{B})$	Distributive Law
$A \cup \emptyset$	Complement Law: $B \cap \overline{B} = \emptyset$
A	Identity Law

Result:

$$\boxed{(A \cup B) \cap (A \cup \overline{B}) = A}$$

Logic		**Set Theory**
Proposition p	$\leftrightarrow$	Set A
$\neg p$	$\leftrightarrow$	$\overline{A}$
$p \vee q$	$\leftrightarrow$	$A \cup B$
$p \wedge q$	$\leftrightarrow$	$A \cap B$
$p \oplus q$	$\leftrightarrow$	$A \oplus B$

Double-headed arrows indicate logical correspondence

Figure 2.5: Correspondence between propositional logic connectives and set operations.

Section 2.2 Summary — Set Operations & Venn Diagrams

Operations Quick Reference:

Operation	Symbol	Elements included
Union	$A \cup B$	In A **or** B (or both)
Intersection	$A \cap B$	In **both** A and B
Complement	$\overline{A}$	In U but **not** in A
Difference	$A - B$	In A but **not** in B
Sym. Difference	$A \oplus B$	In **exactly one** of A, B

Inclusion-Exclusion Formula:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Past Paper Connection:

- **2021 Q1(iii):** Associative law of union → Theorem 2.3
- **2022 Q6(a):** Set-builder proof of $(A \cap B)' = A' \cup B'$ → Example 3
- **2023 Q1(iv) & Q1(x):** De Morgan negations; symmetric difference Venn diagram → Examples 2, 4
- **2024 Q1(i):** De Morgan's Law in set theory → Definition 2.12, Example 2

Relations and Their Properties

Definition 2.13 — Binary Relation

A **binary relation** R from set A to set B is a subset of the Cartesian product $A \times B$:

$$R \subseteq A \times B$$

We write $a\,R\,b$ or $(a, b) \in R$ to mean "a is related to b by R."

When $A = B$, we say R is a **relation on** A, meaning $R \subseteq A \times A$.

Key Points:

- A relation is simply a **set of ordered pairs**.
- A relation on A with $|A| = n$ is a subset of $A \times A$, which has n^2 elements. So there are 2^{n^2} possible relations on A.
- Relations can be represented as: a **set of ordered pairs**, a **directed graph** (digraph), or a **matrix**.

Definition 2.14 — Matrix Representation of a Relation

The **relation matrix** (or *Boolean matrix*) M_R of a relation R on $A = \{a_1, a_2, \ldots, a_n\}$ is an $n \times n$ matrix where:

$$M_R[i][j] = \begin{cases} 1 & \text{if } (a_i,\, a_j) \in R \\ 0 & \text{if } (a_i,\, a_j) \notin R \end{cases}$$

Digraph representation: Draw a vertex for each element of A. Draw a directed edge (arrow) from a_i to a_j whenever $(a_i, a_j) \in R$. A **loop** at vertex a_i represents the pair $(a_i, a_i) \in R$.

Example 1: Relation as Set Matrix and Digraph

Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$.

(a) Write R as a set of ordered pairs.

(b) Construct the relation matrix M_R.

(c) Describe the digraph.

Solution:

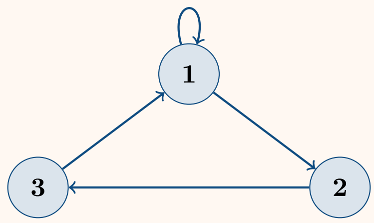
(a) $R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$ — already in set form.

(b) Relation matrix: Rows and columns ordered $1, 2, 3$.

$$M_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Entry $(i, j) = 1$ iff $(i, j) \in R$.

(c) Digraph:



Definition 2.15 — Reflexive Relation

A relation R on set A is **reflexive** if every element is related to **itself**:

$$R \text{ is reflexive} \iff \forall a \in A,\ (a, a) \in R$$

Recognition Tips:

- In the **matrix**: all diagonal entries ($M[i][i]$) are **1**.
- In the **digraph**: every vertex has a **loop**.
- To **disprove**: find any $a \in A$ with $(a, a) \notin R$.

Definition 2.16 — Symmetric Relation

A relation R on set A is **symmetric** if whenever $(a, b) \in R$, then $(b, a) \in R$ as well:

$$R \text{ is symmetric} \iff \forall a, b \in A,\ [(a, b) \in R \to (b, a) \in R]$$

Recognition Tips:

- In the **matrix**: M is **symmetric** ($M = M^T$), i.e. $M[i][j] = M[j][i]$ for all i, j.
- In the **digraph**: for every directed edge $a \to b$, there is also $b \to a$ (edges come in **pairs**).
- The empty relation $\emptyset$ is symmetric (vacuously).

Definition 2.17 — Antisymmetric Relation

A relation R on set A is **antisymmetric** if whenever both $(a, b) \in R$ and $(b, a) \in R$, then $a = b$:

$$R \text{ is antisymmetric} \iff \forall a, b \in A,\ [(a, b) \in R \land (b, a) \in R \to a = b]$$

Key Points:

- Equivalently: if $a \neq b$ and $(a, b) \in R$, then $(b, a) \notin R$.

- **Antisymmetric ≠ not symmetric.** A relation can be both symmetric and antisymmetric (e.g. the equality relation on a single element).
- In the **matrix**: for $i \neq j$, $M[i][j]$ and $M[j][i]$ cannot *both* be 1.
- Example: "$\leq$" on integers is antisymmetric ($a \leq b$ and $b \leq a$ implies $a = b$).

Definition 2.18 — Transitive Relation

A relation R on set A is **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$:

$$R \text{ is transitive} \iff \forall a, b, c \in A,\ [(a, b) \in R \wedge (b, c) \in R \to (a, c) \in R]$$

Recognition Tips:

- In the **digraph**: if there is a path $a \to b \to c$, there must also be a direct edge $a \to c$.
- To **disprove**: find a, b, c with $(a, b), (b, c) \in R$ but $(a, c) \notin R$.
- **Careful:** check *all* pairs systematically — one missed pair makes it non-transitive.

Theorem 2.4 — Detecting Properties from the Relation Matrix

Let R be a relation on $A = \{a_1, \dots, a_n\}$ with matrix M_R. Then:

Property	**Matrix Condition**
Reflexive	All diagonal entries are 1: $M[i][i] = 1$ for all i
Irreflexive	All diagonal entries are 0: $M[i][i] = 0$ for all i
Symmetric	$M = M^T$, i.e. $M[i][j] = M[j][i]$ for all i, j
Antisymmetric	$M[i][j] = 1$ and $i \neq j \Rightarrow M[j][i] = 0$
Transitive	$M_R^2 \leq M_R$ (Boolean matrix product: if $(M_R^2)[i][j] = 1$ then $M_R[i][j] = 1$)

Example 2: Four Relations Analysed — Past Paper 2020 Q3

For each relation on $\{3, 4, 5, 6\}$, determine whether it is reflexive, symmetric, antisymmetric, and transitive.

(a) $R_1 = \{(3, 3), (3, 4), (3, 6), (5, 4), (5, 5), (5, 6)\}$

Solution:

Reflexive? Need $(3, 3), (4, 4), (5, 5), (6, 6) \in R_1$. $(4, 4) \notin R_1$ and $(6, 6) \notin R_1$. × Not reflexive.

Symmetric? $(3, 4) \in R_1$ but $(4, 3) \notin R_1$. × Not symmetric.

Antisymmetric? Check all pairs: no pair (a, b) and (b, a) with $a \neq b$ exist. ✓ Antisymmetric.

Transitive? Check: $(3, 4) \in R_1$ — need $(4, ?)$ pairs. No $(4, x) \in R_1$, so no violation from $(3, 4)$. $(3, 6) \in R_1$ — no $(6, x)$ pairs. $(5, 4), (5, 6)$ — no $(4, x)$ or $(6, x)$. $(3, 3) \in R_1$: $(3, 3) + (3, 4) \Rightarrow$ need $(3, 4)$ ✓; $(3, 3) + (3, 6) \Rightarrow$ need $(3, 6)$ ✓. $(5, 5) + (5, 4) \Rightarrow$ need $(5, 4)$ ✓. $(5, 5) + (5, 6) \Rightarrow$ need $(5, 6)$ ✓. ✓ Transitive.

(b) $R_2 = \{(3,3),(3,4),(4,3),(4,4),(5,5),(6,6)\}$

Reflexive? $(3,3),(4,4),(5,5),(6,6) \in R_2$. ✓ Reflexive.
Symmetric? $(3,4) \in R_2$ and $(4,3) \in R_2$. All other non-diagonal pairs absent. ✓ Symmetric.
Antisymmetric? $(3,4) \in R_2$ and $(4,3) \in R_2$ with $3 \neq 4$. × Not antisymmetric.
Transitive? $(3,4)+(4,3) \Rightarrow$ need $(3,3)$ ✓; $(4,3)+(3,4) \Rightarrow$ need $(4,4)$ ✓; $(3,4)+(4,4) \Rightarrow$ need $(3,4)$ ✓; $(4,3)+(3,3) \Rightarrow$ need $(4,3)$ ✓. ✓ Transitive.

(c) $R_3 = \{(3,4),(4,5),(5,6)\}$

Reflexive? $(3,3) \notin R_3$. × Not reflexive.
Symmetric? $(3,4) \in R_3$ but $(4,3) \notin R_3$. × Not symmetric.
Antisymmetric? No pair (a,b) and (b,a) with $a \neq b$ both present. ✓ Antisymmetric.
Transitive? $(3,4)+(4,5) \Rightarrow$ need $(3,5)$. $(3,5) \notin R_3$. × Not transitive.

(d) $R_4 = \{(3,5),(3,6),(4,5),(4,6),(5,3),(5,5)\}$

Reflexive? $(3,3) \notin R_4$. × Not reflexive.
Symmetric? $(3,5) \in R_4$ and $(5,3) \in R_4$ ✓. But $(3,6) \in R_4$ and $(6,3) \notin R_4$. × Not symmetric.
Antisymmetric? $(3,5) \in R_4$ and $(5,3) \in R_4$ with $3 \neq 5$. × Not antisymmetric.
Transitive? $(5,3)+(3,5) \Rightarrow$ need $(5,5)$ ✓. $(5,3)+(3,6) \Rightarrow$ need $(5,6)$. $(5,6) \notin R_4$. × Not transitive.

Summary Table:

Relation	Reflexive	Symmetric	Antisymmetric	Transitive
R_1	No	No	Yes	Yes
R_2	Yes	Yes	No	Yes
R_3	No	No	Yes	No
R_4	No	No	No	No

Example 3: Relations — Past Paper 2021 Q4

For each relation on $\{1,2,3,4\}$, determine which properties hold: reflexive, symmetric, transitive.

(i) $R_1 = \{(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)\}$

Solution:
Reflexive? $(1,1) \notin R_1$ and $(4,4) \notin R_1$. × Not reflexive.
Symmetric? $(2,4) \in R_1$ but $(4,2) \notin R_1$. × Not symmetric.
Transitive? $(3,2)+(2,3) \Rightarrow (3,3)$ ✓; $(3,2)+(2,4) \Rightarrow (3,4)$ ✓; $(2,3)+(3,2) \Rightarrow (2,2)$ ✓; $(2,3)+(3,4) \Rightarrow (2,4)$ ✓; $(2,2)+(2,3) \Rightarrow (2,3)$ ✓; $(3,3)+(3,4) \Rightarrow (3,4)$ ✓. ✓ Transitive.

(ii) $R_2 = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$
Reflexive? All of $(1,1),(2,2),(3,3),(4,4) \in R_2$. ✓ Reflexive.
Symmetric? $(1,2) \in R_2$ and $(2,1) \in R_2$. All others symmetric. ✓ Symmetric.
Transitive? $(1,2)+(2,1) \Rightarrow (1,1)$ ✓; $(2,1)+(1,2) \Rightarrow (2,2)$ ✓; $(1,2)+(2,2) \Rightarrow (1,2)$ ✓. ✓ Transitive.

(iii) $R_3 = \emptyset$ (empty relation)

Reflexive? $(1,1) \notin \emptyset$. × Not reflexive.

Symmetric? Vacuously true — there are no pairs $(a,b) \in R_3$ to check. ✓ Symmetric (vacuously).

Transitive? Vacuously true. ✓ Transitive (vacuously).

(iv) $R_4 = \{(1,1),(2,2),(3,3),(4,4)\}$ (equality relation)

Reflexive? All $(a,a) \in R_4$. ✓ Reflexive.

Symmetric? Only pairs of form (a,a) — symmetric trivially. ✓ Symmetric.

Transitive? $(a,a)+(a,a) \Rightarrow (a,a)$ ✓. ✓ Transitive.

Relation	Reflexive	Symmetric	Transitive
R_1	No	No	Yes
R_2	Yes	Yes	Yes
$R_3 = \emptyset$	No	Yes	Yes
R_4 (equality)	Yes	Yes	Yes

Example 4: Three Relations Analysed — Past Paper 2022 Q2

Let $A = \{0,1,2,5\}$. Analyse each of R, S, T:

$R = \{(0,0),(0,1),(0,5),(1,0),(1,1),(2,2),(5,0),(5,5)\}$

$S = \{(0,0),(0,2),(0,5),(2,5)\}$

$T = \{(0,1),(2,5)\}$

Solution:

Relation R:

Reflexive? $(0,0),(1,1),(2,2),(5,5) \in R$. ✓ Reflexive.

Symmetric? $(0,1) \in R$ and $(1,0) \in R$ ✓; $(0,5) \in R$ and $(5,0) \in R$ ✓; all self-loops symmetric. ✓ Symmetric.

Transitive? $(1,0)+(0,1) \Rightarrow (1,1)$ ✓; $(1,0)+(0,5) \Rightarrow (1,5)$. $(1,5) \notin R$. × Not transitive.

Relation S:

Reflexive? $(1,1) \notin S$. × Not reflexive.

Symmetric? $(0,2) \in S$ but $(2,0) \notin S$. × Not symmetric.

Transitive? $(0,2)+(2,5) \Rightarrow (0,5)$ ✓; $(0,0)+(0,2) \Rightarrow (0,2)$ ✓; $(0,0)+(0,5) \Rightarrow (0,5)$ ✓. No other composable pairs. ✓ Transitive.

Relation T:

Reflexive? $(0,0) \notin T$. × Not reflexive.

Symmetric? $(0,1) \in T$ but $(1,0) \notin T$. × Not symmetric.

Transitive? No two pairs in T are composable (no x such that $(0,x),(x,?) \in T$ with both present). ✓ Transitive (vacuously).

Relation	Reflexive	Symmetric	Transitive
R	Yes	Yes	No
S	No	No	Yes
T	No	No	Yes

Example 5: Drawing Directed Graphs for Relations — Past Paper 2024 Q3

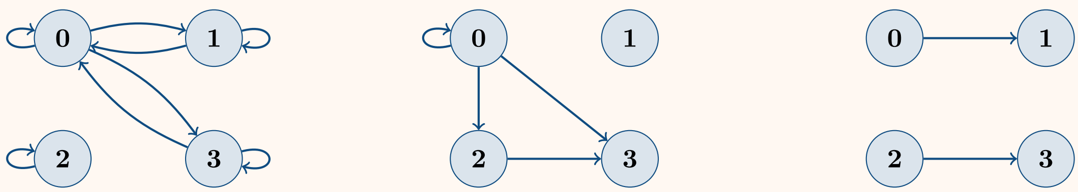
Let $A = \{0, 1, 2, 3\}$. Draw the directed graph for each relation:

$R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\}$
$S = \{(0, 0), (0, 2), (0, 3), (2, 3)\}$
$T = \{(0, 1), (2, 3)\}$

Solution:

For each relation: place vertices $0, 1, 2, 3$ and draw arrows for each ordered pair. A loop (a, a) is an arrow from a to itself.

Relation R **Relation S** **Relation T**



Observations from digraphs:

- R has loops at all vertices and bidirectional edges $\Rightarrow$ reflexive and symmetric.
- S has a loop only at 0 and all arrows point "one way" $\Rightarrow$ not reflexive, not symmetric, transitive.
- T has no loops and no reverse edges $\Rightarrow$ not reflexive, not symmetric, vacuously transitive.

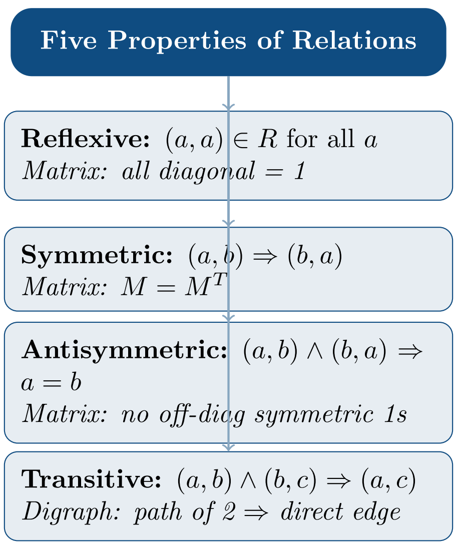


Figure 2.6: The four key properties of relations with their matrix/digraph recognition rules.

Section 2.3 Summary — Relations & Their Properties

Master Table of Properties:

Property	Definition	Matrix	Digraph
Reflexive	$(a, a) \in R\ \forall a$	Diagonal all 1s	Loop at every vertex
Irreflexive	$(a, a) \notin R\ \forall a$	Diagonal all 0s	No loops
Symmetric	$(a, b) \Rightarrow (b, a)$	$M = M^T$	Edges in pairs
Antisymmetric	$(a, b) \wedge (b, a) \Rightarrow a = b$	No sym. off-diag 1s	No 2-cycles
Transitive	$(a, b) \wedge (b, c) \Rightarrow (a, c)$	$M^2 \leq M$	Path⇒edge

Common Traps:

- **Antisymmetric $\neq$ not symmetric.** A relation can be both (e.g. $\{(1, 1), (2, 2)\}$) or neither (e.g. $\{(1, 2), (2, 1), (1, 3)\}$).
- **Empty relation** $\emptyset$ is symmetric, antisymmetric, and transitive (all vacuously), but NOT reflexive.
- **Transitivity** — always check *all* composable pairs. Missing even one pair $(a, b), (b, c)$ with $(a, c) \notin R$ breaks transitivity.
- **Vacuous truth** — if no pair (a, b) exists with $a \neq b$, the relation is automatically symmetric and antisymmetric.

Past Paper Connection:

- **2020 Q3:** Four relations on $\{3, 4, 5, 6\}$ → Example 2
- **2021 Q4:** Four relations on $\{1, 2, 3, 4\}$ → Example 3
- **2022 Q2:** Relations R, S, T on $\{0, 1, 2, 5\}$ → Example 4
- **2024 Q3:** Directed graphs for R, S, T on $\{0, 1, 2, 3\}$ → Example 5

Equivalence Relations and Partitions

Definition 2.19 — Equivalence Relation

A relation R on a set A is an **equivalence relation** if it satisfies **all three** of the following properties simultaneously:

Property	Formal Statement	Intuition
Reflexive	$\forall a \in A,\ (a, a) \in R$	Every element equals itself
Symmetric	$(a, b) \in R \Rightarrow (b, a) \in R$	Equality works both ways
Transitive	$(a, b), (b, c) \in R \Rightarrow (a, c) \in R$	Equality chains together

Key Points:

- When R is an equivalence relation, we often write $a \sim b$ instead of $(a, b) \in R$.

- **Memory aid:** Equivalence = **R**eflexive + **S**ymmetric + **T**ransitive ("RST").
- The most important example of an equivalence relation is **equality** $(=)$ itself.
- Modular congruence ("$\equiv \pmod{n}$") is the most tested example in this course.

Example 1: Equality is an Equivalence Relation

Show that the equality relation $R = \{(a, a) \mid a \in A\}$ on any set A is an equivalence relation.

Solution:

Reflexive: For every $a \in A$, $(a, a) \in R$ by definition. ✓
Symmetric: If $(a, b) \in R$ then $a = b$, so $(b, a) = (a, a) \in R$. ✓
Transitive: If $(a, b) \in R$ and $(b, c) \in R$, then $a = b$ and $b = c$, so $a = c$, giving $(a, c) \in R$. ✓
Conclusion: The equality relation is an equivalence relation. Its equivalence classes are singletons $\{a\}$ for each $a \in A$.

Definition 2.20 — Congruence Modulo n

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

The relation $R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod{n}\}$ is called **congruence modulo** n.

Key Points:

- Equivalently, $a \equiv b \pmod{n}$ iff a and b have the **same remainder** when divided by n.
- Example $(n = 3)$: $7 \equiv 1 \pmod{3}$ because $3 \mid (7 - 1) = 6$.
- Past Paper 2020 Q1(iii) asks: $(-17) \bmod 2$. Since $-17 = (-9)(2) + 1$, we get $(-17) \bmod 2 = 1$.

Theorem 2.5 — Congruence Modulo n is an Equivalence Relation

For any positive integer n, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof of Theorem 2.5

Proof:

We verify the three properties for R_n on $\mathbb{Z}$.

Step 1 — Reflexive:
For any $a \in \mathbb{Z}$: $a - a = 0 = n \cdot 0$, so $n \mid (a - a)$. Therefore $(a, a) \in R_n$ for all a. ✓

Step 2 — Symmetric:

Suppose $(a, b) \in R_n$, i.e. $n \mid (a - b)$. Then $a - b = nk$ for some integer k. So $b - a = n(-k)$, meaning $n \mid (b - a)$. Therefore $(b, a) \in R_n$. ✓

Step 3 — Transitive:

Suppose $(a, b) \in R_n$ and $(b, c) \in R_n$. Then $n \mid (a-b)$ and $n \mid (b-c)$. Write $a-b = nj$ and $b - c = nk$ for integers j, k. Then:

$$a - c = (a - b) + (b - c) = nj + nk = n(j + k)$$

So $n \mid (a - c)$, giving $(a, c) \in R_n$. ✓

Conclusion: Congruence modulo n satisfies all three properties and is therefore an equivalence relation on $\mathbb{Z}$. □

Definition 2.21 — Equivalence Class

Let R be an equivalence relation on set A. The **equivalence class** of an element $a \in A$, written $[a]$ or $\overline{a}$, is the set of all elements of A that are related to a by R:

$$[a] = \{b \in A \mid (a, b) \in R\} = \{b \in A \mid a \sim b\}$$

Key Properties:

- Every element of A belongs to **exactly one** equivalence class.
- $[a] = [b]$ if and only if $(a, b) \in R$ (i.e. $a \sim b$).
- Either $[a] = [b]$ (identical classes) or $[a] \cap [b] = \emptyset$ (completely disjoint).
- Any element of an equivalence class can serve as its **representative**.

Example 2: Equivalence Classes of Congruence Modulo 3

Find all equivalence classes of the congruence modulo 3 relation on $\mathbb{Z}$.

Solution:

When we divide any integer by 3, the remainder is 0, 1, or 2. So there are exactly **three** equivalence classes:

Class $[0]$ — integers with remainder 0:

$$[0] = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = \{n \in \mathbb{Z} \mid 3 \mid n\}$$

Class $[1]$ — integers with remainder 1:

$$[1] = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} = \{n \in \mathbb{Z} \mid n \equiv 1 \pmod 3\}$$

Class $[2]$ — integers with remainder 2:

$$[2] = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\} = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod 3\}$$

Verification:

- $[0] \cup [1] \cup [2] = \mathbb{Z}$ ✓ (every integer has a remainder)
- $[0] \cap [1] = \emptyset$, $[0] \cap [2] = \emptyset$, $[1] \cap [2] = \emptyset$ ✓ (no integer has two different remainders)
- Note: $[0] = [3] = [6] = [-3] = \dots$ (many representatives, one class)

Definition 2.22 — Partition

A **partition** of a set A is a collection of non-empty, mutually disjoint subsets $A_1, A_2, \dots, A_k$ (called **cells** or **blocks**) whose union is A:

$$A = A_1 \cup A_2 \cup \cdots \cup A_k \quad \text{where} \quad A_i \neq \emptyset \quad \text{and} \quad A_i \cap A_j = \emptyset \text{ for } i \neq j$$

Key Points:

- Every partition of A defines an equivalence relation on A: $a \sim b$ iff a and b are in the **same cell**.
- Conversely, every equivalence relation on A induces a partition of A (the cells are the equivalence classes).
- This is the **Fundamental Theorem of Equivalence Relations** (Theorem 2.6 below).
- The set of all equivalence classes is called the **quotient set**, written A/R.

Theorem 2.6 — Fundamental Theorem of Equivalence Relations

Let R be an equivalence relation on a non-empty set A. Then:

(i) The equivalence classes of R form a **partition** of A.

(ii) Conversely, given any partition $\{A_1, A_2, \dots\}$ of A, the relation defined by $a \sim b \iff a$ and b are in the same cell is an equivalence relation on A.

This establishes a **one-to-one correspondence** between equivalence relations on A and partitions of A.

Example 3: Finding the Partition from an Equivalence Relation

Let $A = \{1, 2, 3, 4, 5, 6\}$ and define the relation:

$$R = \{(a, b) \mid a \equiv b \pmod 2\}$$

(i.e. a and b have the same parity).

Verify R is an equivalence relation and find the partition of A.

Solution:

Verify equivalence relation:
Reflexive: $a - a = 0 = 2 \cdot 0$, so $2 \mid (a - a)$ for all a. ✓
Symmetric: If $2 \mid (a - b)$ then $a - b = 2k$, so $b - a = 2(-k)$, giving $2 \mid (b - a)$. ✓

Transitive: If $2 \mid (a-b)$ and $2 \mid (b-c)$, then $a-c=(a-b)+(b-c)$ is divisible by 2. ✓

Equivalence classes:

$$[1] = \{1,3,5\} \quad \text{(odd numbers in } A\text{)}$$

$$[2] = \{2,4,6\} \quad \text{(even numbers in } A\text{)}$$

Partition of A:

$$\boxed{A = \{1,3,5\} \cup \{2,4,6\}}$$

Verification: $\{1,3,5\} \cap \{2,4,6\} = \emptyset$ ✓ and $\{1,3,5\} \cup \{2,4,6\} = A$ ✓

Example 4: Constructing an Equivalence Relation from a Partition

Let $A = \{1,2,3,4,5\}$ with partition: $P_1 = \{1,3\}$, $P_2 = \{2,4\}$, $P_3 = \{5\}$.
Find the equivalence relation R induced by this partition.

Solution:

Two elements are related iff they are in the **same cell**.
From $P_1 = \{1,3\}$: $(1,1),(1,3),(3,1),(3,3) \in R$
From $P_2 = \{2,4\}$: $(2,2),(2,4),(4,2),(4,4) \in R$
From $P_3 = \{5\}$: $(5,5) \in R$

$$\boxed{R = \{(1,1),(1,3),(3,1),(3,3),(2,2),(2,4),(4,2),(4,4),(5,5)\}}$$

Verify RST:
Reflexive: $(1,1),(2,2),(3,3),(4,4),(5,5) \in R$. ✓
Symmetric: $(1,3) \in R \Rightarrow (3,1) \in R$; $(2,4) \in R \Rightarrow (4,2) \in R$. ✓
Transitive: $(1,3)+(3,1) \Rightarrow (1,1)$ ✓; $(3,1)+(1,3) \Rightarrow (3,3)$ ✓. ✓

Example 5: Is This an Equivalence Relation?

Determine whether each of the following relations on $\mathbb{Z}$ is an equivalence relation. If yes, describe the equivalence classes. If no, state which property fails.

(a) $R = \{(a,b) \mid a \le b\}$

(b) $S = \{(a,b) \mid a+b \text{ is even}\}$

(c) $T = \{(a,b) \mid 3 \mid (a+2b)\}$

Solution:

(a) R: "$\le$" on $\mathbb{Z}$.
Reflexive: $a \le a$ always. ✓
Symmetric: $1 \le 2$ but $2 \not\le 1$. × Fails.
Conclusion: Not an equivalence relation (fails symmetry).

(b) S: $a+b$ is even.

Reflexive: $a + a = 2a$ is even. ✓

Symmetric: $a + b$ even $\Rightarrow b + a$ even (addition commutes). ✓

Transitive: If $a + b$ even and $b + c$ even, then both a, b same parity and b, c same parity, so a, c same parity, giving $a + c$ even. ✓

Equivalence classes: $[\text{even}] = \{0, \pm 2, \pm 4, \dots\}$ and $[\text{odd}] = \{\pm 1, \pm 3, \pm 5, \dots\}$.

Conclusion: Equivalence relation. Partition: even integers $\cup$ odd integers.

(c) T: $3 \mid (a + 2b)$.

Reflexive: $a + 2a = 3a$, so $3 \mid 3a$. ✓

Symmetric: If $3 \mid (a + 2b)$, note $b + 2a = (a + 2b) + (a - b + b - b)$; more directly: $b + 2a = 3a + 3b - (a + 2b)$. Since $3 \mid (a + 2b)$ and $3 \mid 3(a + b)$, we get $3 \mid (b + 2a)$. ✓

Transitive: If $3 \mid (a + 2b)$ and $3 \mid (b + 2c)$, then adding: $3 \mid (a + 2b + b + 2c) = 3 \mid (a + 3b + 2c)$. Since $3 \mid 3b$, we get $3 \mid (a + 2c)$. ✓

Conclusion: Equivalence relation. The classes turn out to be the same as congruence mod 3.

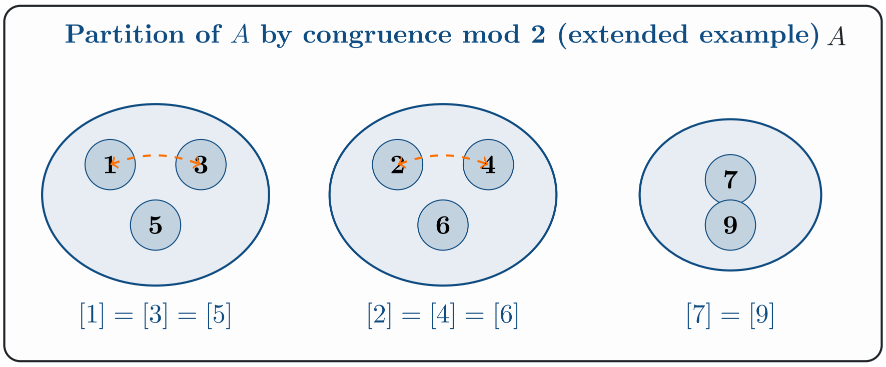


Figure 2.7: An equivalence relation partitions the set A into disjoint, non-empty equivalence classes (cells).

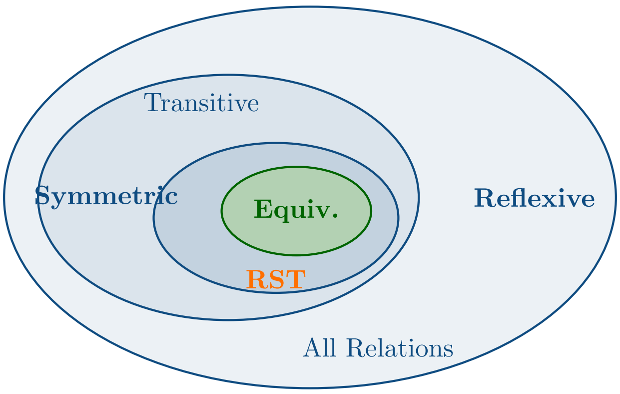


Figure 2.8: An equivalence relation lies in the intersection of reflexive, symmetric, and transitive relations.

Section 2.4 Summary — Equivalence Relations & Partitions

The Big Picture:

Concept	Key Fact
Equivalence relation	Must be Reflexive + Symmetric + Transitive
Equivalence class $[a]$	All elements related to a; $a \in [a]$ always
$[a] = [b]$	iff $(a, b) \in R$
$[a] \cap [b]$	Either $= [a] = [b]$ or $= \emptyset$
Partition	Disjoint, non-empty subsets covering A
Correspondence	Equivalence relations $\longleftrightarrow$ Partitions
Congruence mod n	Gives n equivalence classes: $[0], [1], \ldots, [n - 1]$

Step-by-Step: Analysing an Equivalence Relation

1. Check **reflexive**: is $(a, a) \in R$ for every $a \in A$?
2. Check **symmetric**: for every $(a, b) \in R$, is $(b, a) \in R$?
3. Check **transitive**: for every $(a, b), (b, c) \in R$, is $(a, c) \in R$?
4. If all three hold: find the equivalence classes by grouping related elements.
5. Verify: classes are disjoint and cover A.

Past Paper Connection:

- **2020 Q1(iii):** $(-17) \bmod 2 = 1 \to$ Definition 2.20
- **2020 Q3, 2021 Q4, 2022 Q2:** All test RST $\to$ builds directly on Section 2.3 and this section
- Relations R_2 in 2020 Q3 and R_2/R_4 in 2021 Q4 are equivalence relations $\to$ Examples 3, 4

Partial Orderings

Definition 2.23 — Partial Order (Partial Ordering)

A relation R on a set A is a **partial order** (or *partial ordering*) if it is:

Property	Formal Condition	Example with $\leq$
Reflexive	$(a, a) \in R \; \forall a \in A$	$a \leq a$
Antisymmetric	$(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$	$a \leq b \wedge b \leq a \Rightarrow a = b$
Transitive	$(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$	$a \leq b \wedge b \leq c \Rightarrow a \leq c$

Key Points:

- **Memory aid:** Partial Order = **R**eflexive + **A**ntisymmetric + **T**ransitive ("RAT").
- Compare with equivalence relation (RST): partial order replaces *symmetric* with *antisymmetric*.
- A set A together with a partial order R is called a **partially ordered set** or **poset**, written (A, R).

- We often use the symbol $\preceq$ to denote a generic partial order, writing $a \preceq b$ instead of $(a, b) \in R$.
- Two elements a and b in a poset are **comparable** if $a \preceq b$ or $b \preceq a$; otherwise they are **incomparable**.

Example 1: Common Partial Orders

Verify that each of the following is a partial order.

(a) The relation $\leq$ (less than or equal to) on $\mathbb{Z}$.

(b) The relation $|$ (divides) on $\mathbb{Z}^+$.

(c) The relation $\subseteq$ (subset) on $\mathcal{P}(A)$ for any set A.

Solution:

(a) $(\mathbb{Z}, \leq)$:
Reflexive: $a \leq a$ for all $a \in \mathbb{Z}$. ✓
Antisymmetric: $a \leq b$ and $b \leq a \Rightarrow a = b$. ✓
Transitive: $a \leq b$ and $b \leq c \Rightarrow a \leq c$. ✓

(b) $(\mathbb{Z}^+, |)$:
Reflexive: $a \mid a$ since $a = a \cdot 1$. ✓
Antisymmetric: If $a \mid b$ and $b \mid a$ then $b = ka$ and $a = mb$, giving $a = mka$, so $mk = 1$. Since $m, k \in \mathbb{Z}^+$, we get $m = k = 1$, thus $a = b$. ✓
Transitive: If $a \mid b$ and $b \mid c$, then $b = ka$ and $c = lb$, so $c = l(ka) = (lk)a$, giving $a \mid c$. ✓

(c) $(\mathcal{P}(A), \subseteq)$:
Reflexive: $A \subseteq A$ for every set. ✓
Antisymmetric: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$. ✓
Transitive: $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$. ✓

Relation	Reflexive	Antisymmetric	Transitive
$(\mathbb{Z}, \leq)$	✓	✓	✓
$(\mathbb{Z}^+, \vert)$	✓	✓	✓
$(\mathcal{P}(A), \subseteq)$	✓	✓	✓

Definition 2.24 — Total Order (Linear Order)

A partial order $(A, \preceq)$ is a **total order** (or *linear order* or *chain*) if **every** pair of elements is comparable:

$$\forall a, b \in A,\ a \preceq b \ \text{ or } \ b \preceq a$$

Key Points:

- $(\mathbb{Z}, \leq)$ is a **total order** — any two integers are comparable.
- $(\mathbb{Z}^+, |)$ is **not** a total order — for example, 2 and 3 are incomparable (neither $2 \mid 3$ nor $3 \mid 2$).

- $(\mathcal{P}(A), \subseteq)$ is **not** a total order in general — $\{1\}$ and $\{2\}$ are incomparable subsets.

Definition 2.25 — Hasse Diagram

A **Hasse diagram** is a simplified visual representation of a finite poset $(A, \preceq)$ obtained from its directed graph by:

Rule 1: **Remove all loops** (reflexivity is understood).

Rule 2: **Remove all edges implied by transitivity.** If $a \preceq b$ and $b \preceq c$, remove the direct edge $a \to c$.

Rule 3: **Orient edges upward.** Place b above a whenever $a \prec b$ (proper ordering), then drop all arrowheads.

Reading a Hasse Diagram:

- $a \preceq b$ iff you can travel from a **upward** to b along the edges.
- Elements with no element below them are **minimal elements**.
- Elements with no element above them are **maximal elements**.

Definition 2.26 — Special Elements in a Poset

Element	Definition	Key Fact
Maximal	No element strictly above it	May not be unique
Minimal	No element strictly below it	May not be unique
Greatest	Above *every* element	Unique if exists
Least	Below *every* element	Unique if exists
Upper bound of B	Above every element of $B \subseteq A$	May not exist
Lower bound of B	Below every element of $B \subseteq A$	May not exist
LUB / sup of B	Least among all upper bounds of B	Unique if exists
GLB / inf of B	Greatest among all lower bounds of B	Unique if exists

Critical Distinction:

- A **maximal** element has nothing above it *in the poset.* A **greatest** element is above *every other* element.
- A poset can have many maximal elements but at most **one** greatest element.

Theorem 2.7 — Uniqueness of Greatest and Least Elements

In a poset $(A, \preceq)$, if a greatest element exists, it is **unique**. Similarly, if a least element exists, it is unique.

Example 2: Hasse Diagram

Draw the Hasse diagram for the divisibility partial order on the set $S = \{1, 2, 3, 4, 6, 12\}$.

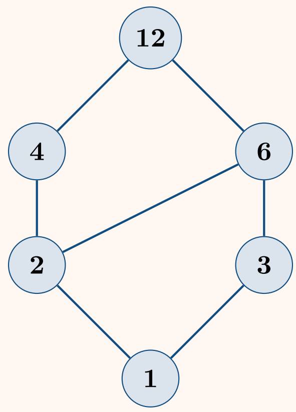
Solution:

Step 1: List all divisibility pairs ($a \mid b$ with $a \neq b$):

$$1 \mid 2,\ 1 \mid 3,\ 1 \mid 4,\ 1 \mid 6,\ 1 \mid 12,\ 2 \mid 4,\ 2 \mid 6,\ 2 \mid 12,\ 3 \mid 6,\ 3 \mid 12,\ 4 \mid 12,\ 6 \mid 12$$

Step 2: Remove transitive edges. $1 \mid 4$ is implied by $1 \mid 2$ and $2 \mid 4$, so remove direct $1 \to 4$. Similarly remove $1 \to 6$, $1 \to 12$, $2 \to 12$, $3 \to 12$.

Step 3: Draw upward edges only (no arrows, no loops).



Reading the diagram:

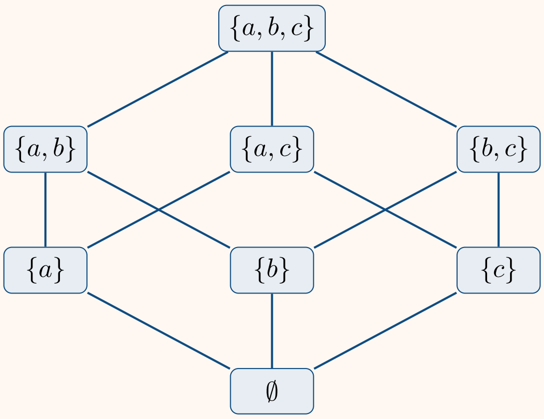
- **Least element:** 1 (below everything). ✓
- **Greatest element:** 12 (above everything). ✓
- **Minimal element:** 1 (same as least here).
- **Maximal element:** 12 (same as greatest here).
- **Comparable pairs:** e.g. 2 and 4 ($2 \mid 4$).
- **Incomparable pairs:** e.g. 4 and 6 (neither $4 \mid 6$ nor $6 \mid 4$).

Example 3: Hasse Diagram for Power Set

Draw the Hasse diagram for the power set of $\{a, b, c\}$ ordered by $\subseteq$.

Solution:

The elements are the 8 subsets of $\{a, b, c\}$, ordered by inclusion. We connect A to B (with B above A) whenever $A \subset B$ and there is no C with $A \subset C \subset B$.

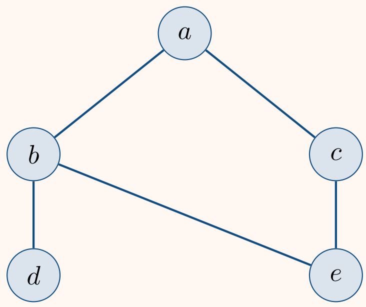


Reading the diagram:

- **Least element:** $\emptyset$.
- **Greatest element:** $\{a, b, c\}$.
- **Incomparable:** $\{a\}$ and $\{b\}$ (neither is a subset of the other).
- **LUB of $\{a\}$ and $\{b\}$:** $\{a, b\}$.
- **GLB of $\{a, b\}$ and $\{b, c\}$:** $\{b\}$.

Example 4: Identifying Special Elements from a Hasse Diagram

The Hasse diagram of a poset $(A, \preceq)$ is given below:



Find: maximal, minimal, greatest, and least elements. Also find upper and lower bounds of $\{b, c\}$.

Solution:

Concept	Elements	Reason
Maximal	a	Nothing is above a
Minimal	d, e	Nothing is below d or e
Greatest	a	a is above all elements
Least	Does not exist	No element is below both d and e
Upper bounds of $\{b, c\}$	a	a is above both b and c
LUB of $\{b, c\}$	a	Least (only) upper bound
Lower bounds of $\{b, c\}$	e	e is below both b and c
GLB of $\{b, c\}$	e	Greatest (only) lower bound

Example 5: Comparing Partial and Total Orders

Let $S = \{2, 3, 6, 12, 24, 36\}$ with the divisibility relation $|$.

(a) Is $(S, |)$ a partial order?

(b) Is it a total order?

(c) Find all incomparable pairs.

(d) Find maximal and minimal elements.

Solution:

(a) We verified in Example 1 that divisibility is reflexive, antisymmetric, and transitive. So $(S, |)$ **is a partial order**. ✓

(b) Check comparability: $2 \mid 3$? No. $3 \mid 2$? No. So 2 and 3 are **incomparable**. Therefore $(S, |)$ **is not a total order**. ×

(c) Incomparable pairs:

Pair	Reason
$(2, 3)$	$2 \nmid 3$ and $3 \nmid 2$
$(3, 12)$	$3 \mid 12$ — *comparable*
$(12, 36)$	$12 \mid 36$ — *comparable*
$(24, 36)$	$24 \nmid 36$ and $36 \nmid 24$
$(12, 24)$	$12 \mid 24$ — *comparable*

Truly incomparable pairs: $(2, 3)$ and $(24, 36)$.

(d) From the divisibility structure:

- **Minimal elements:** 2 and 3 (nothing in S divides 2 or 3 except themselves).
- **Maximal elements:** 24 and 36 (neither 24 nor 36 divides the other, and nothing in S is divisible by both).
- **Least element:** Does not exist (2 and 3 are incomparable).
- **Greatest element:** Does not exist (24 and 36 are incomparable).

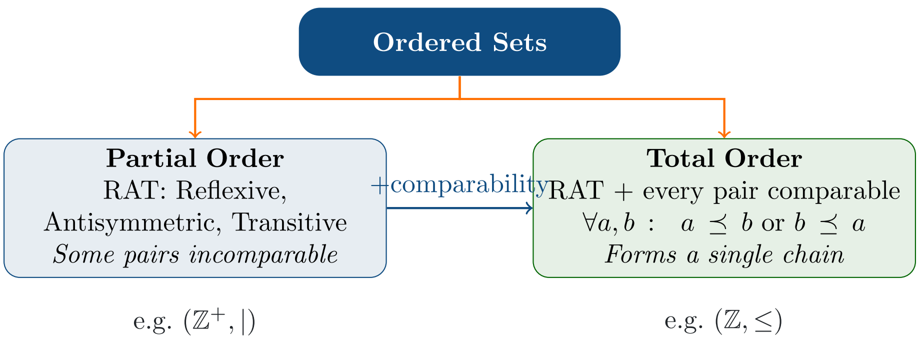


Figure 2.9: Relationship between partial orders and total orders.

Section 2.5 Summary — Partial Orderings

Equivalence vs Partial Order:

Property	Equivalence Relation	Partial Order
Reflexive	✓	✓
Symmetric	✓	×
Antisymmetric	×	✓
Transitive	✓	✓
Acronym	**RST**	**RAT**

Special Elements Quick Reference:

Element	One-line definition
Maximal	Nothing strictly above it
Minimal	Nothing strictly below it
Greatest	Above everything (unique if exists)
Least	Below everything (unique if exists)
LUB of B	Least of all upper bounds of B
GLB of B	Greatest of all lower bounds of B

Hasse Diagram Construction Rules:

1. Remove all loops.
2. Remove all edges implied by transitivity.
3. Place larger elements higher; drop all arrowheads.

Past Paper Connection:

- Partial orderings connect to **tree structures** (Chapter 5 — rooted trees use a partial order on nodes by depth).
- The divisibility poset $(\mathbb{Z}^+, |)$ appears in **Number Theory** (Chapter 3) for GCD and LCM calculations, where $\gcd(a, b) = \text{GLB}$ and $\text{lcm}(a, b) = \text{LUB}$.

Practice Exercises

Q1. Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Write each of the following sets using the roster method and find their cardinality:

(i) $\{x \in A \mid x \text{ is even}\}$
(ii) $\{x \in A \mid x \text{ is prime}\}$
(iii) $\{x \in A \mid x^2 \in A\}$
(iv) $\{x \in A \mid x \text{ is divisible by 3 or 5}\}$

Q2. Let $A = \{a, b\}$, $B = \{b, c, d\}$, and $C = \{a, c\}$.

(i) Find $A \times B$, $B \times A$, and $A \times C$.
(ii) Is $A \times B = B \times A$? Justify.
(iii) How many elements does $(A \times B) \times C$ have?
(iv) List all elements of $A \times A$.

Q3. Find the power set of each of the following sets. State the cardinality of each power set.

(i) $\{0\}$
(ii) $\{a, b\}$
(iii) $\{1, 2, 3\}$
(iv) $\{\emptyset, \{1\}\}$

Q4. Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{2, 3, 5, 7\}$, $B = \{1, 2, 3, 4, 5\}$, and $C = \{3, 5, 7, 9\}$. Find each of the following:

(i) $A \cup B$, $A \cap B$, $A - B$, $B - A$
(ii) $\overline{A}$, $\overline{B}$, $\overline{A} \cap \overline{B}$
(iii) $A \oplus B$ and $A \oplus C$
(iv) $\overline{A \cup C}$ and $\overline{A} \cap \overline{C}$ (verify De Morgan's Law)

Q5. Use set-builder notation and logical equivalences to prove De Morgan's Second Law for sets:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Then verify it numerically using $A = \{1, 3, 5\}$, $B = \{5, 6, 7\}$, $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Q6. Draw Venn diagrams to represent each of the following. Shade the region corresponding to the given expression:

(i) $(A \cup B) \cap C$
(ii) $(A - B) \cup (B - A)$
(iii) $A \cap \overline{B} \cap C$
(iv) $\overline{A \cap B \cap C}$

Q7. In a survey of 100 students: 60 study Mathematics, 45 study Physics, 30 study Chemistry, 20 study both Mathematics and Physics, 15 study both Mathematics and Chemistry, 10 study both Physics and Chemistry, and 5 study all three subjects.

(i) How many students study at least one subject?
(ii) How many study exactly one subject?
(iii) How many study none of the three?

Q8. Simplify each expression using the laws of set theory. Name every law you apply at each step.

(i) $(A \cup B) \cap \overline{A}$
(ii) $A \cup (A \cap B)$
(iii) $(A \cap B) \cup (A \cap \overline{B})$
(iv) $\overline{(\overline{A} \cup B)} \cup \overline{(\overline{A} \cup \overline{B})}$

Q9. For each of the following relations on $\{1, 2, 3, 4, 5\}$, determine which of the properties — reflexive, symmetric, antisymmetric, transitive — hold. Construct a summary table.

(i) $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 2), (2, 1)\}$
(ii) $\{(1, 2), (2, 3), (1, 3)\}$
(iii) $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (3, 5), (1, 5)\}$
(iv) $\{(1, 2), (2, 3), (3, 4), (4, 5)\}$

Q10. Let $A = \{0, 1, 2, 3\}$. For each relation below, determine all four properties (reflexive, symmetric, antisymmetric, transitive). Then draw its directed graph.

(i) $R = \{(0, 0), (1, 1), (2, 2), (3, 3), (0, 1), (1, 0), (2, 3), (3, 2)\}$
(ii) $S = \{(0, 1), (1, 2), (2, 3), (0, 2), (1, 3), (0, 3)\}$
(iii) $T = \{(0, 0), (1, 1), (2, 2), (3, 3)\}$

Q11. Write the relation matrix M_R for each of the following relations on $\{1, 2, 3, 4\}$. Then use the matrix to determine whether the relation is reflexive, symmetric, and antisymmetric.

(i) $R = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$
(ii) $S = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (3, 1)\}$
(iii) $T = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$

Q12. Determine whether each relation on $\mathbb{Z}$ is an equivalence relation. If yes, describe the equivalence classes. If no, state which property fails with a counterexample.

(i) $R = \{(a, b) \mid a - b \text{ is divisible by } 4\}$
(ii) $S = \{(a, b) \mid ab > 0\}$
(iii) $T = \{(a, b) \mid |a - b| \leq 1\}$
(iv) $U = \{(a, b) \mid a^2 = b^2\}$

Q13. Find the equivalence classes generated by congruence modulo 5 on $\mathbb{Z}$. List at least five elements in each class. Then determine which class each of the following integers belongs to: -13, -1, 0, 7, 23, 100.

Q14. Let $A = \{1, 2, 3, 4, 6, 8, 12, 24\}$ with the divisibility relation.

(i) Verify this is a partial order.

(ii) Draw the Hasse diagram.

(iii) Identify the least and greatest elements (if they exist).

(iv) Find all maximal and minimal elements.

(v) Find the LUB and GLB of $\{2, 4, 6\}$.

Q15. Given the partition $\{P_1, P_2, P_3\}$ of $A = \{a, b, c, d, e, f\}$ where $P_1 = \{a, b\}$, $P_2 = \{c, d, e\}$, $P_3 = \{f\}$:

(i) Write out the equivalence relation R induced by this partition.

(ii) Verify that R is reflexive, symmetric, and transitive.

(iii) What are the equivalence classes of R?

(iv) How many ordered pairs does R contain?

Q16. Consider the poset $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.

(i) Draw the Hasse diagram.

(ii) Find the least and greatest elements.

(iii) Are $\{1, 2\}$ and $\{2, 3\}$ comparable? Explain.

(iv) Find the LUB and GLB of $\{\{1, 2\}, \{2, 3\}\}$.

(v) Find all maximal chains (sequences of comparable elements from least to greatest).

Q17. Determine whether each relation on $\{a, b, c, d\}$ is a partial order. If yes, draw its Hasse diagram. If no, state which RAT property fails.

(i) $\{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c)\}$

(ii) $\{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a)\}$

(iii) $\{(a, a), (b, b), (c, c), (d, d), (a, c), (b, c), (a, d), (b, d)\}$

Q18. Prove or disprove each of the following statements:

(i) The intersection of two equivalence relations on a set A is also an equivalence relation on A.

(ii) The union of two equivalence relations on a set A is always an equivalence relation on A.

(iii) If R is both an equivalence relation and a partial order on A, then R must be the equality relation.

Q19. A relation R on $\mathbb{R}$ is defined by: $x\,R\,y$ if and only if $x - y \in \mathbb{Z}$ (i.e. $x - y$ is an integer).

(i) Show R is an equivalence relation.

(ii) Describe the equivalence class of 0.

(iii) Describe the equivalence class of $\frac{1}{2}$.

(iv) How many distinct equivalence classes does R have?

Q20. Let $A = \{2, 3, 4, 6, 9, 12, 18, 36\}$ with divisibility relation $|$.

(i) Draw the Hasse diagram for $(A, |)$.

(ii) Find all minimal and maximal elements.

(iii) Does a greatest element exist? Does a least element exist?

(iv) Find $\text{LUB}(\{4, 6\})$ and $\text{GLB}(\{12, 18\})$.

(v) Identify three pairs of incomparable elements.

Exam Preparation Tips for Chapter 2

- **Q1–Q3** cover sets and power sets — always in objective part (2 marks each).
- **Q4–Q8** cover set operations — De Morgan proofs appear almost every year as a 12-mark subjective question.
- **Q9–Q11** are the most heavily tested topic in this course — relations and their properties appear as full subjective questions in 2020, 2021, 2022, and 2024.
- **Q12–Q13** on equivalence relations are typically worth 12 marks when they appear. Always verify all three properties with clear steps.
- **Q14–Q20** on partial orders and Hasse diagrams are growing in frequency — master the construction rules and special element definitions.

Chapter 3

Functions and Number Theory

Functions: Types and Properties

Definition 3.1 — Function

A **function** f from set A to set B, written $f : A \to B$, is a relation from A to B such that **every element of** A **is assigned to exactly one element of** B.

Term	Meaning
Domain	The set A — inputs of f
Codomain	The set B — all possible outputs
Range / Image	$\{f(a) \mid a \in A\} \subseteq B$ — actual outputs
$f(a)$	The **image** of a under f; a is the **preimage** of $f(a)$

Key Points:

- Every element of A must be mapped — no element can be left out.
- Each element of A maps to **exactly one** element of B (no splitting).
- Different elements of A may map to the **same** element of B.
- The range is always a subset of the codomain: $\text{range}(f) \subseteq B$.
- A function is a special case of a relation: one that is **total** and **functional**.

Difference between Relation and Function:

- A **relation** allows an element of A to map to zero, one, or many elements of B.
- A **function** requires each element of A to map to **exactly one** element of B.

(Past Paper 2025 Q1(vi) directly asks: "Differentiate between a Function and a Relation.")

Example 1: Identifying Valid Functions

Determine which of the following are valid functions from $A = \{1, 2, 3\}$ to $B = \{a, b, c\}$:

Solution:

Mapping	Assigned pairs	Function?	Reason
f_1	$1 \mapsto a,\ 2 \mapsto b,\ 3 \mapsto c$	✓	Each input has exactly one output
f_2	$1 \mapsto a,\ 2 \mapsto a,\ 3 \mapsto b$	✓	Repetition in output is allowed
f_3	$1 \mapsto a,\ 2 \mapsto b$	×	Element 3 has no image
f_4	$1 \mapsto a,\ 1 \mapsto b,\ 2 \mapsto c,\ 3 \mapsto c$	×	Element 1 maps to two outputs

For f_1**:** domain $= \{1, 2, 3\}$, codomain $= \{a, b, c\}$, range $= \{a, b, c\}$.
For f_2**:** domain $= \{1, 2, 3\}$, codomain $= \{a, b, c\}$, range $= \{a, b\} \subsetneq B$ (proper subset of codomain).

Definition 3.2 — One-to-One Function (Injective)

A function $f : A \to B$ is **one-to-one** (or *injective*) if different elements of A always map to different elements of B:

$$f \text{ is injective} \iff \forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

Equivalently (contrapositive):

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

Key Points:

- No two distinct inputs share the same output.
- **To prove injective:** assume $f(a_1) = f(a_2)$ and show $a_1 = a_2$.
- **To disprove:** find $a_1 \neq a_2$ with $f(a_1) = f(a_2)$.
- In a function diagram: no two arrows point to the same output.
- Requires $|A| \leq |B|$ for a finite injective function to exist.

Definition 3.3 — Onto Function (Surjective)

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

$$f \text{ is surjective} \iff \forall b \in B,\ \exists a \in A \text{ such that } f(a) = b$$

Key Points:

- The **range equals the codomain**: $\text{range}(f) = B$.

- **To prove surjective:** for an arbitrary $b \in B$, find (construct) an $a \in A$ with $f(a) = b$.
- **To disprove:** find a $b \in B$ with no preimage in A.
- Requires $|A| \geq |B|$ for a finite surjective function to exist.

Definition 3.4 — Into Function

A function $f : A \to B$ is called an **into** function if it is **not onto**, i.e., there exists at least one element $b \in B$ that is **not** in the range of f:

$$\text{range}(f) \subsetneq B \quad \text{(range is a proper subset of codomain)}$$

Note: Every function is either onto or into. "Into" simply means the function does not cover the entire codomain. *(Past Paper 2025 Q3 directly asks to describe and give examples of one-to-one, onto, into, and bijective functions.)*

Definition 3.5 — Bijective Function (One-to-One Correspondence)

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

Injective	Surjective	Bijective?
✓	✓	✓ Yes
✓	×	× No
×	✓	× No
×	×	× No

Key Points:

- A bijection establishes a **perfect pairing** between A and B.
- For finite sets: $f : A \to B$ is bijective iff $|A| = |B|$ and f is injective (or surjective — either one implies the other when $|A| = |B|$).
- A function has an inverse if and only if it is **bijective**.
- Past Papers 2021 Q6, 2022 Q6(b), 2024 Q1(x): all test bijectivity.

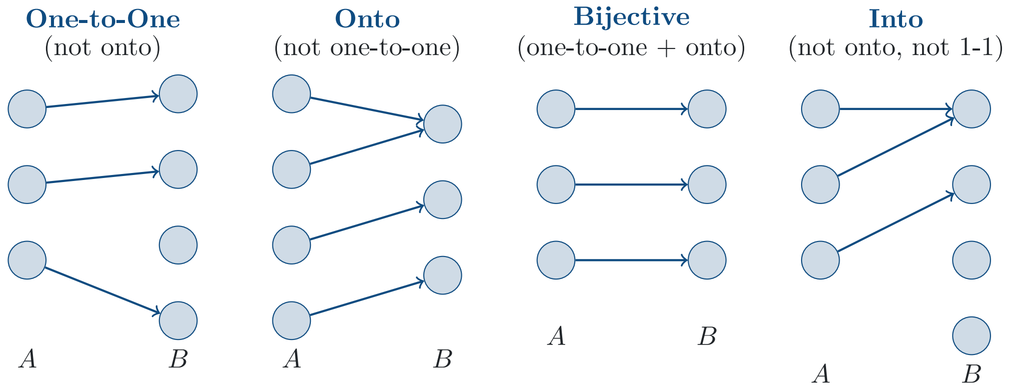


Figure 3.1: The four types of functions. Bijective has a perfect pairing; into leaves some outputs unreached.

Theorem 3.1 — Bijection and Equal Cardinality

For finite sets A and B, a bijection $f : A \to B$ exists if and only if $|A| = |B|$.

Moreover, for a function $f : A \to B$ with $|A| = |B|$:

$$f \text{ is injective} \iff f \text{ is surjective} \iff f \text{ is bijective}$$

Example 2: Testing Bijectivity — Past Paper 2021 Q6

Determine whether the following functions are bijective from $\mathbb{R}$ to $\mathbb{R}$:

(a) $f(x) = -3x + 4$

(b) $f(x) = -3x^2 + 7$

(c) $f(x) = \dfrac{x+1}{x+2}$

(d) $f(x) = x^3 + 1$

Solution:

(a) $f(x) = -3x + 4$
Injective: Suppose $f(x_1) = f(x_2)$.

$$-3x_1 + 4 = -3x_2 + 4 \implies -3x_1 = -3x_2 \implies x_1 = x_2$$

✓ Injective.

Surjective: For any $y \in \mathbb{R}$, solve $-3x + 4 = y$: $x = \dfrac{4-y}{3} \in \mathbb{R}$. ✓ Surjective.
Bijective.

(b) $f(x) = -3x^2 + 7$
Injective? $f(1) = -3+7 = 4$ and $f(-1) = -3+7 = 4$. So $f(1) = f(-1)$ but $1 \neq -1$.
× Not injective.

Surjective? The range of $-3x^2 + 7$ is $(-\infty, 7]$ since $-3x^2 \leq 0$. So $y = 8$ has no preimage. × Not surjective.

Not bijective. (Neither injective nor surjective.)

(c) $f(x) = \dfrac{x+1}{x+2}$

Domain issue: f is undefined at $x = -2$, so the domain is not all of $\mathbb{R}$. Therefore $f : \mathbb{R} \to \mathbb{R}$ as stated is **not a valid function**. **Not bijective.**

(d) $f(x) = x^3 + 1$

Injective: Suppose $f(x_1) = f(x_2)$.

$$x_1^3 + 1 = x_2^3 + 1 \implies x_1^3 = x_2^3 \implies x_1 = x_2$$

(cube root is unique over $\mathbb{R}$). ✓ Injective.

Surjective: For any $y \in \mathbb{R}$, set $x = \sqrt[3]{y-1} \in \mathbb{R}$. Then $f(x) = (y-1)+1 = y$. ✓ Surjective.

Bijective.

Example 3: Invertible — Past Paper 2020 Q5(b)

Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$. Is f invertible?

Solution:

A function is invertible if and only if it is **bijective**. We check both conditions.

Injective? $f(2) = 4$ and $f(-2) = 4$, but $2 \neq -2$. × Not injective.

Surjective? For $y = -1$: we need $x^2 = -1$, which has no real solution. × Not surjective.

Since f is **neither injective nor surjective** over $\mathbb{R}$, it is **not bijective**.

Conclusion:

$$\boxed{f(x) = x^2 \text{ is } \textbf{NOT} \text{ invertible as } f : \mathbb{R} \to \mathbb{R}}$$

Note: If we restrict the domain to $\mathbb{R}^+$ and codomain to $\mathbb{R}^+$, then $f(x) = x^2$ *becomes* bijective and its inverse is $f^{-1}(y) = \sqrt{y}$.

Example 4: Finite Function-Bijection Check - Past Paper 2022 Q4(b) & Q6(b)

(a) Let $f : \{a, b, c\} \to \{1, 2, 3\}$ with $f(a) = 2$, $f(b) = 3$, $f(c) = 1$. Is f invertible? If yes, find f^{-1}.

(b) Let $f : \{w, x, y, z\} \to \{0, 1, 2, 3\}$ with $f(w) = 3$, $f(x) = 1$, $f(y) = 0$, $f(z) = 2$. Is f a bijection?

Solution:

(a) Check injection and surjection:
$f(a) = 2$, $f(b) = 3$, $f(c) = 1$ — all outputs are distinct. ✓ Injective.
Range $= \{1, 2, 3\} =$ codomain. ✓ Surjective.
Bijective and therefore invertible.
Inverse: swap inputs and outputs.

$$f^{-1}(1) = c, \quad f^{-1}(2) = a, \quad f^{-1}(3) = b$$

$$\boxed{f^{-1} : \{1, 2, 3\} \to \{a, b, c\}}$$

(b) $|domain| = 4 = |codomain|$.
All outputs: $\{3, 1, 0, 2\} = \{0, 1, 2, 3\}$ = codomain. ✓ Surjective.
All outputs are distinct. ✓ Injective.
f is a bijection. ✓

Example 5: Define & Give Examples of All Types — Past Paper 2025 Q3

Define a function. Describe one-to-one, onto, into and bijective functions. Give an example of each with a diagram.

Solution:

Function: A rule assigning each element of domain A to exactly one element of codomain B.

Type	Condition	Example ($\mathbb{Z} \to \mathbb{Z}$)
One-to-one	$f(a) = f(b) \Rightarrow a = b$	$f(x) = 2x$
Onto	range = codomain	$f(x) = x - 1$
Into	range $\subsetneq$ codomain	$f(x) = x^2$ (range: $\mathbb{Z}^+ \cup \{0\}$)
Bijective	one-to-one AND onto	$f(x) = x + 5$

Verification of $f(x) = 2x$ (one-to-one, not onto):
Injective: $2x_1 = 2x_2 \Rightarrow x_1 = x_2$. ✓
Not surjective: $y = 1$ has no preimage since $2x = 1 \Rightarrow x = \frac{1}{2} \notin \mathbb{Z}$. ×

Verification of $f(x) = x + 5$ (bijective):
Injective: $x_1 + 5 = x_2 + 5 \Rightarrow x_1 = x_2$. ✓
Surjective: For any $y \in \mathbb{Z}$, $x = y - 5 \in \mathbb{Z}$ and $f(x) = y$. ✓

Section 3.1 Summary — Functions: Types & Properties

Four Types at a Glance:

Type	Condition	Range vs Codomain	Requires
Injective	No two inputs share output	range $\subseteq B$	$|A| \leq |B|$
Surjective	Every output is reached	range $= B$	$|A| \geq |B|$
Bijective	Both above	range $= B$, 1-1	$|A| = |B|$
Into	Some outputs unreached	range $\subsetneq B$	$|A| < |B|$ typical

Proof Strategy:

- **To prove injective:** Assume $f(a_1) = f(a_2)$. Derive $a_1 = a_2$.
- **To prove surjective:** Take arbitrary $b \in B$. Construct a with $f(a) = b$.
- **To disprove injective:** Give a concrete $a_1 \neq a_2$ with $f(a_1) = f(a_2)$.
- **To disprove surjective:** Give a concrete $b \in B$ with no preimage.

Past Paper Connection:

- **2020 Q5(b):** $f(x) = x^2$ invertible? $\to$ Example 3
- **2021 Q6:** Bijective from $\mathbb{R}$ to $\mathbb{R}$ $\to$ Example 2
- **2022 Q4(b) & Q6(b):** Finite function invertibility $\to$ Example 4
- **2024 Q1(x),(xi):** Define bijection; inverse of one-to-one $\to$ Definitions 3.2–3.5
- **2025 Q1(vi) & Q3:** Relation vs function; all four types $\to$ Definitions 3.1–3.5, Example 5

Composition and Inverse Functions

Definition 3.6 — Composition of Functions

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

$$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in A$$

Key Points:

- **Order matters:** $g \circ f$ means apply f *first*, then g. Read right to left.
- $g \circ f \neq f \circ g$ in general (composition is **not commutative**).
- Composition **is associative:** $(h \circ g) \circ f = h \circ (g \circ f)$.
- The **range of** f must be a subset of the **domain of** g for $g \circ f$ to be defined.
- Composition of two injective functions is injective.
- Composition of two surjective functions is surjective.
- Composition of two bijections is a bijection.

Example 1: Computing Function Compositions

Let $f, g, h : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 3$, $g(x) = x^2 - 1$, $h(x) = \sqrt{x + 4}$.
Find: (a) $(g \circ f)(x)$ (b) $(f \circ g)(x)$ (c) $(g \circ f)(2)$ (d) $(h \circ g)(x)$ (e) $(f \circ f)(x)$

Solution:

(a) $(g \circ f)(x) = g(f(x)) = g(2x + 3) = (2x + 3)^2 - 1$

$$= 4x^2 + 12x + 9 - 1 = \boxed{4x^2 + 12x + 8}$$

(b) $(f \circ g)(x) = f(g(x)) = f(x^2 - 1) = 2(x^2 - 1) + 3$

$$= 2x^2 - 2 + 3 = \boxed{2x^2 + 1}$$

Note: $(g \circ f)(x) \neq (f \circ g)(x)$ — composition is **not commutative**.

(c) $(g \circ f)(2) = 4(4) + 12(2) + 8 = 16 + 24 + 8 = \boxed{48}$
Verification: $f(2) = 7$, then $g(7) = 49 - 1 = 48$. ✓

(d) $(h \circ g)(x) = h(g(x)) = h(x^2 - 1) = \sqrt{(x^2 - 1) + 4} = \boxed{\sqrt{x^2 + 3}}$

(e) $(f \circ f)(x) = f(f(x)) = f(2x + 3) = 2(2x + 3) + 3 = 4x + 6 + 3 = \boxed{4x + 9}$

Example 2: Compositions of Finite Functions — Past Paper 2021 Q3

Let $A = \{1, 2, 3, 4\}$, $f : A \to A$ and $g : A \to A$ defined by:

$$f = \{(1, 3), (2, 1), (3, 2), (4, 4)\} \qquad g = \{(1, 2), (2, 4), (3, 1), (4, 3)\}$$

Find: (a) $g \circ f$ (b) $f \circ g$ (c) $f \circ f$

Solution:

(a) $g \circ f$: apply f first, then g.

x	$f(x)$	$g(f(x))$	$(g \circ f)(x)$
1	3	$g(3) = 1$	1
2	1	$g(1) = 2$	2
3	2	$g(2) = 4$	4
4	4	$g(4) = 3$	3

$$g \circ f = \{(1, 1), (2, 2), (3, 4), (4, 3)\}$$

(b) $f \circ g$: apply g first, then f.

x	$g(x)$	$f(g(x))$	$(f \circ g)(x)$
1	2	$f(2) = 1$	1
2	4	$f(4) = 4$	4
3	1	$f(1) = 3$	3
4	3	$f(3) = 2$	2

$$f \circ g = \{(1, 1), (2, 4), (3, 3), (4, 2)\}$$

(c) $f \circ f$: apply f twice.

x	$f(x)$	$f(f(x))$	$(f \circ f)(x)$
1	3	$f(3) = 2$	2
2	1	$f(1) = 3$	3
3	2	$f(2) = 1$	1
4	4	$f(4) = 4$	4

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

Observation: $g \circ f \neq f \circ g$. Composition is **not commutative**.

Definition 3.7 — Identity Function

The **identity function** on a set A, written I_A or id_A, is the function that maps every element to itself:

$$I_A : A \to A, \qquad I_A(x) = x \quad \text{for all } x \in A$$

Key Properties:

- $f \circ I_A = f$ and $I_B \circ f = f$ for any $f : A \to B$.
- The identity function is always bijective.
- It plays the same role in function composition that 1 plays in multiplication.

Definition 3.8 — Inverse Function

Let $f : A \to B$ be a **bijective** function. The **inverse** of f, written $f^{-1} : B \to A$, is the unique function defined by:

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

Equivalently, f^{-1} satisfies:

$$f^{-1} \circ f = I_A \qquad \text{and} \qquad f \circ f^{-1} = I_B$$

Key Points:

- A function has an inverse **if and only if** it is bijective.
- f^{-1} is obtained by **swapping** the roles of input and output.
- $(f^{-1})^{-1} = f$ — the inverse of the inverse is the original.
- $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ — reverse order for compositions.
- **Do not confuse** $f^{-1}(x)$ (inverse function) with $[f(x)]^{-1} = \dfrac{1}{f(x)}$ (reciprocal).

Theorem 3.2 — The Inverse of a Bijection is a Bijection

If $f : A \to B$ is bijective, then $f^{-1} : B \to A$ exists and is also bijective.

Example 3: Finding the Inverse — Past Paper 2024 Q1(xi)

Find the inverse of $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = 3x - 7$.
Verify that $f \circ f^{-1} = I$ and $f^{-1} \circ f = I$.

Solution:

Step 1: Verify f is bijective.
Injective: $3x_1 - 7 = 3x_2 - 7 \Rightarrow x_1 = x_2$. ✓

Surjective: For any $y \in \mathbb{R}$, set $x = \dfrac{y+7}{3}$. Then $f(x) = y$. ✓

Step 2: Find f^{-1}.
Set $y = f(x) = 3x - 7$. Solve for x:

$$y = 3x - 7 \implies y + 7 = 3x \implies x = \frac{y+7}{3}$$

$$\boxed{f^{-1}(x) = \frac{x+7}{3}}$$

Step 3: Verify.
$(f \circ f^{-1})(x) = f\left(\dfrac{x+7}{3}\right) = 3 \cdot \dfrac{x+7}{3} - 7 = x + 7 - 7 = x = I(x)$ ✓
$(f^{-1} \circ f)(x) = f^{-1}(3x-7) = \dfrac{(3x-7)+7}{3} = \dfrac{3x}{3} = x = I(x)$ ✓

Example 4: Inverse of a Finite Function — Past Paper 2023 Q3

Let $f : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ be given by:

$$f = \{(1,3),\ (2,5),\ (3,4),\ (4,1),\ (5,2)\}$$

(a) Show that f is a bijection.

(b) Find f^{-1}.

(c) Compute $f^{-1} \circ f^{-1}$.

Solution:

(a) All outputs $\{3,5,4,1,2\} = \{1,2,3,4,5\}$ are distinct and cover the codomain. Bijection. ✓

(b) Swap inputs and outputs:

$$f^{-1} = \{(3,1),\ (5,2),\ (4,3),\ (1,4),\ (2,5)\}$$

(c) $f^{-1} \circ f^{-1}$: apply f^{-1} twice.

x	$f^{-1}(x)$	$f^{-1}(f^{-1}(x))$	$(f^{-1} \circ f^{-1})(x)$
1	4	$f^{-1}(4) = 3$	3
2	5	$f^{-1}(5) = 2$	2
3	1	$f^{-1}(1) = 4$	4
4	3	$f^{-1}(3) = 1$	1
5	2	$f^{-1}(2) = 5$	5

$$f^{-1} \circ f^{-1} = \{(1,3),(2,2),(3,4),(4,1),(5,5)\}$$

Example 5: Composition of Bijections — Past Paper 2022 Q4(b)

Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x - 1$ and $g : \mathbb{R} \to \mathbb{R}$ with $g(x) = x + 4$.

(a) Find $g \circ f$ and $f \circ g$.

(b) Are $g \circ f$ and $f \circ g$ bijective?

(c) Find $(g \circ f)^{-1}$ and verify using $f^{-1} \circ g^{-1}$.

Solution:

(a)

$$(g \circ f)(x) = g(2x - 1) = (2x - 1) + 4 = \boxed{2x + 3}$$
$$(f \circ g)(x) = f(x + 4) = 2(x + 4) - 1 = \boxed{2x + 7}$$

(b) Both f and g are linear with non-zero slope, hence bijective. Composition of bijections is bijective. ✓ Both $g \circ f$ and $f \circ g$ are bijective.

(c) Find $(g \circ f)^{-1}$ directly:
Set $y = 2x + 3$, solve for x:

$$x = \frac{y - 3}{2} \implies \boxed{(g \circ f)^{-1}(x) = \frac{x - 3}{2}}$$

Verify via $f^{-1} \circ g^{-1}$:
$f(x) = 2x - 1 \Rightarrow f^{-1}(x) = \dfrac{x + 1}{2}$
$g(x) = x + 4 \Rightarrow g^{-1}(x) = x - 4$
$(f^{-1} \circ g^{-1})(x) = f^{-1}(g^{-1}(x)) = f^{-1}(x - 4) = \dfrac{(x - 4) + 1}{2} = \dfrac{x - 3}{2}$ ✓
The formula $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ is confirmed.

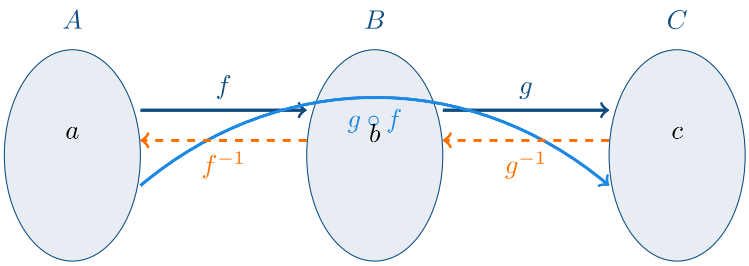


Figure 3.2: Composition $g \circ f : A \to C$ applies f then g. Inverses reverse the arrows: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Section 3.2 Summary — Composition & Inverse Functions

Composition Rules:

- $(g \circ f)(x) = g(f(x))$ — apply f first, then g.
- **Not commutative:** $g \circ f \neq f \circ g$ in general.

- **Associative:** $(h \circ g) \circ f = h \circ (g \circ f)$.
- Composition of injections is injective; surjections is surjective; bijections is bijective.

Inverse Function Rules:

- f^{-1} exists $\iff$ f is bijective.
- To find f^{-1}: set $y = f(x)$, solve for x, write $f^{-1}(y) = x$.
- $(f^{-1})^{-1} = f$.
- $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (reverse order!).
- $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_B$.

Step-by-Step: Finding an Inverse

1. Verify f is bijective.
2. Write $y = f(x)$.
3. Solve algebraically for x in terms of y.
4. Write $f^{-1}(y) = x$ (or replace y with x for standard notation).
5. Verify: $f(f^{-1}(x)) = x$ and $f^{-1}(f(x)) = x$.

Past Paper Connection:

- **2021 Q3:** Composition of finite functions $\to$ Example 2
- **2022 Q4(b):** Composition of linear functions + inverse $\to$ Example 5
- **2023 Q3:** Inverse of finite bijection + $f^{-1} \circ f^{-1}$ $\to$ Example 4
- **2024 Q1(xi):** Find f^{-1} and verify $\to$ Example 3

Recursive Functions and Recurrence Relations

Definition 3.9 — Recursive (Inductive) Definition

A **recursive definition** of a function f on non-negative integers consists of two parts:

1. **Base Case:** The value of f is explicitly stated for the smallest input(s), e.g. $f(0)$ or $f(1)$.
2. **Recursive Step:** A rule expressing $f(n)$ in terms of f at smaller values, e.g. $f(n) =$ expression involving $f(n-1)$.

Key Points:

- Every recursive definition must **terminate** — the recursion must eventually reach the base case.

- Recursive definitions are equivalent to definitions by induction.
- The base case prevents infinite recursion.
- Recursion is the foundation of many algorithms: merge sort, binary search, tree traversals, dynamic programming.

Example 1: Recursive Definition of Factorial

Give a recursive definition of $n!$ (n factorial) and compute $5!$.

Solution:

Recursive definition:

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{if } n \geq 1 \end{cases}$$

Computation of $5!$:

$$\begin{aligned} 5! &= 5 \cdot 4! \\ 4! &= 4 \cdot 3! \\ 3! &= 3 \cdot 2! \\ 2! &= 2 \cdot 1! \\ 1! &= 1 \cdot 0! = 1 \cdot 1 = 1 \end{aligned}$$

Substituting back:

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = \boxed{120}$$

Note: $0! = 1$ is the base case by definition — it is not zero. This is necessary for the formula $\binom{n}{r} = \dfrac{n!}{r!(n-r)!}$ to work when $r = 0$ or $r = n$.

Example 2: Fibonacci Sequence

The Fibonacci sequence is defined recursively as:

$$F(0) = 0, \quad F(1) = 1, \quad F(n) = F(n-1) + F(n-2) \quad \text{for } n \geq 2$$

List the first 10 Fibonacci numbers and compute $F(10)$.

Solution:

n	0	1	2	3	4	5	6	7	8	9	10
$F(n)$	0	1	1	2	3	5	8	13	21	34	55

Sample computations:

$$\begin{aligned} F(2) &= F(1) + F(0) = 1 + 0 = 1 \\ F(5) &= F(4) + F(3) = 3 + 2 = 5 \\ F(10) &= F(9) + F(8) = 34 + 21 = \boxed{55} \end{aligned}$$

Property: Each Fibonacci number is the sum of the two preceding ones. The sequence appears in nature: flower petals, spiral shells, and phyllotaxis all follow Fibonacci numbers.

Definition 3.10 — Recurrence Relation

A **recurrence relation** for a sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of its predecessors $a_{n-1}, a_{n-2}, \ldots$

Order of a recurrence: the difference between the highest and lowest subscripts, e.g. $a_n = a_{n-1} + a_{n-2}$ has **order 2**.

Linear recurrence with constant coefficients:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

where $c_1, c_2, \ldots, c_k$ are constants. If there is also a non-recursive term $f(n)$, it is called **non-homogeneous**; otherwise **homogeneous**.

Solving recurrences:

- **Iteration (unrolling):** expand the recurrence step by step until a pattern emerges, then prove by induction.
- **Characteristic equation:** for linear homogeneous recurrences.
- **Direct substitution:** verify a given closed-form solution.

Definition 3.11 — Solving Recurrences by Iteration

To solve $a_n = f(a_{n-1}, a_{n-2}, \ldots)$ by **iteration**:

Step 1: **Expand** the recurrence repeatedly: $a_n \to a_{n-1} \to \cdots \to a_0$.

Step 2: **Identify** the pattern after k expansions.

Step 3: **Substitute** $k = n$ to get the closed form.

Step 4: **Verify** the closed form satisfies the original recurrence and initial conditions.

Example 3: Solve by Iteration — Past Paper 2020 Q6 (Related)

Solve the recurrence relation $a_n = 2a_{n-1} + 1$ with $a_0 = 3$.

Solution:

Step 1: Expand (iterate) the recurrence.

$$\begin{aligned} a_n &= 2a_{n-1} + 1 \\ &= 2(2a_{n-2} + 1) + 1 = 2^2 a_{n-2} + 2 + 1 \\ &= 2^2(2a_{n-3} + 1) + 2 + 1 = 2^3 a_{n-3} + 4 + 2 + 1 \\ &\vdots \\ &= 2^k a_{n-k} + 2^{k-1} + 2^{k-2} + \cdots + 2 + 1 \\ &= 2^k a_{n-k} + (2^k - 1) \end{aligned}$$

Step 2: Substitute $k = n$.

$$a_n = 2^n a_0 + (2^n - 1) = 2^n \cdot 3 + 2^n - 1 = 3 \cdot 2^n + 2^n - 1$$

$$\boxed{a_n = 4 \cdot 2^n - 1 = 2^{n+2} - 1}$$

Step 3: Verify.
$a_0 = 2^2 - 1 = 3$ ✓
$a_1 = 2a_0 + 1 = 7;$ formula: $a_1 = 2^3 - 1 = 7$ ✓
$a_2 = 2a_1 + 1 = 15;$ formula: $a_2 = 2^4 - 1 = 15$ ✓

Example 4: Towers of Hanoi

The Towers of Hanoi with n disks satisfies:

$$H(1) = 1, \qquad H(n) = 2H(n-1) + 1 \quad \text{for } n \geq 2$$

Find a closed-form solution and compute $H(5)$.

Solution:

Iteration:

$$\begin{aligned} H(n) &= 2H(n-1) + 1 \\ &= 2[2H(n-2) + 1] + 1 = 2^2 H(n-2) + 2 + 1 \\ &= 2^3 H(n-3) + 2^2 + 2 + 1 \\ &\vdots \\ &= 2^{n-1} H(1) + 2^{n-2} + \cdots + 2 + 1 \\ &= 2^{n-1} + (2^{n-1} - 1) \qquad \left(\text{geometric series: } \sum_{i=0}^{n-2} 2^i = 2^{n-1} - 1\right) \\ &= 2 \cdot 2^{n-1} - 1 \end{aligned}$$

$$\boxed{H(n) = 2^n - 1}$$

Computation:

n	$H(n) = 2^n - 1$	Verification
1	1	$H(1) = 1$ ✓
2	3	$2(1) + 1 = 3$ ✓
3	7	$2(3) + 1 = 7$ ✓
4	15	$2(7) + 1 = 15$ ✓
5	**31**	$2(15) + 1 = 31$ ✓

$$\boxed{H(5) = 2^5 - 1 = 31 \text{ moves}}$$

Insight: Even with just 64 disks, $H(64) = 2^{64} - 1 \approx 1.8 \times 10^{19}$ moves are needed — more moves than seconds since the Big Bang!

Example 5: Verify a Closed-Form Solution

Show that $a_n = 3^n$ is a solution to the recurrence $a_n = 3a_{n-1}$ with $a_0 = 1$.
Also solve $b_n = 2b_{n-1} + 3$ with $b_0 = 2$ by iteration.

Solution:

Part 1: Verify $a_n = 3^n$.
Check initial condition: $a_0 = 3^0 = 1$. ✓
Check recurrence: $3a_{n-1} = 3 \cdot 3^{n-1} = 3^n = a_n$. ✓
Therefore $a_n = 3^n$ is indeed the solution.

Part 2: Solve $b_n = 2b_{n-1} + 3$, $b_0 = 2$.
Iteration:

$$\begin{aligned}
b_n &= 2b_{n-1} + 3 \\
&= 2(2b_{n-2} + 3) + 3 = 2^2 b_{n-2} + 3 \cdot 2 + 3 \\
&= 2^3 b_{n-3} + 3 \cdot 2^2 + 3 \cdot 2 + 3 \\
&\vdots \\
&= 2^n b_0 + 3(2^{n-1} + 2^{n-2} + \cdots + 1) \\
&= 2^n \cdot 2 + 3 \cdot \frac{2^n - 1}{2 - 1} \\
&= 2^{n+1} + 3(2^n - 1) \\
&= 2^{n+1} + 3 \cdot 2^n - 3
\end{aligned}$$

$$\boxed{b_n = 2^{n+1} + 3 \cdot 2^n - 3 = 5 \cdot 2^n - 3}$$

Verify: $b_0 = 5 \cdot 1 - 3 = 2$ ✓; $b_1 = 2(2) + 3 = 7$; formula: $5 \cdot 2 - 3 = 7$ ✓

Example 6: Sum Recurrence — Past Paper 2023 Q1(xi)Related

A sequence is defined by $a_1 = 2$ and $a_n = a_{n-1} + 4$ for $n \geq 2$.
Find a_n in closed form and compute a_{10}.

Solution:

Iteration:

$$\begin{aligned}
a_n &= a_{n-1} + 4 \\
&= (a_{n-2} + 4) + 4 = a_{n-2} + 2 \cdot 4 \\
&= a_{n-3} + 3 \cdot 4 \\
&\vdots \\
&= a_1 + (n-1) \cdot 4 \\
&= 2 + 4(n-1)
\end{aligned}$$

$$\boxed{a_n = 4n - 2}$$

Verify: $a_1 = 4(1) - 2 = 2$ ✓; $a_2 = a_1 + 4 = 6$; formula: $4(2) - 2 = 6$ ✓

$$a_{10} = 4(10) - 2 = \boxed{38}$$

Note: This is an **arithmetic sequence** with first term 2 and common difference 4. The closed form $a_n = a_1 + (n-1)d = 2 + (n-1)(4) = 4n - 2$.

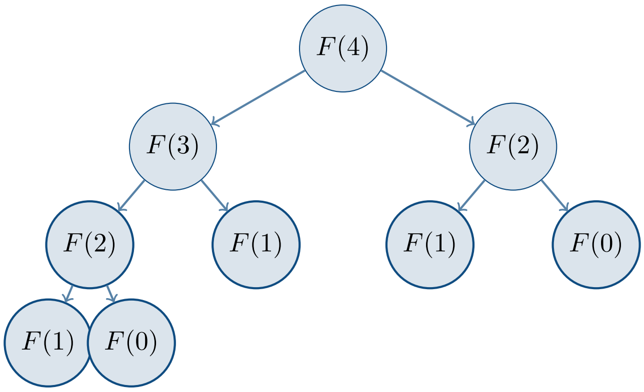


Figure 3.3: Recursion tree for $F(4)$. Each node splits into two subproblems. $F(4) = F(3) + F(2) = 3$.

Section 3.3 Summary — Recursive Functions & Recurrence Relations

Common Recurrences and Their Solutions:

Recurrence	Type	Closed Form
$a_n = a_{n-1} + d$, $a_1 = a$	Arithmetic	$a_n = a + (n-1)d$
$a_n = r \cdot a_{n-1}$, $a_0 = a$	Geometric	$a_n = a \cdot r^n$
$a_n = 2a_{n-1} + 1$, $a_0 = 3$	Linear	$a_n = 2^{n+2} - 1$
$H(n) = 2H(n-1) + 1$, $H(1) = 1$	Hanoi	$H(n) = 2^n - 1$
$F(n) = F(n-1) + F(n-2)$	Fibonacci	No simple closed form

Iteration Method Steps:

1. Write a_n in terms of a_{n-1}, substitute again for a_{n-1} in terms of a_{n-2}, and so on.
2. After k steps, identify the pattern: $a_n = 2^k a_{n-k} +$ (sum terms).

3. Set $k = n$ (or $k = n - 1$) to reach the base case.
4. Simplify the geometric series: $\sum_{i=0}^{k-1} r^i = \frac{r^k - 1}{r - 1}$ for $r \neq 1$.
5. Verify both the initial condition and one step of the recurrence.

Algorithm Complexity and Big-O Notation

Definition 3.12 — Big-O Notation

Let f and g be functions from $\mathbb{Z}^+$ (or $\mathbb{R}^+$) to $\mathbb{R}$. We say $f(n)$ is **Big-O of** $g(n)$, written $f(n) = O(g(n))$, if there exist positive constants C and k such that:

$$|f(n)| \leq C \cdot |g(n)| \quad \text{for all } n > k$$

Key Points:

- C is called the **witness constant** and k is the **threshold**. We only need these to exist — we do not need the smallest possible values.
- $f(n) = O(g(n))$ means f grows **no faster** than g (up to a constant factor) for large n.
- Big-O gives an **upper bound** on the growth rate of f.
- We always choose the **simplest** and **tightest** Big-O expression: e.g. prefer $O(n)$ over $O(n^2)$ if both hold.
- **Drop lower-order terms** and **constant coefficients**: $7n^3 + 5n^2 + 100 = O(n^3)$.

Definition 3.13 — Big-Ω and Big-Θ Notation

Big-Ω (lower bound): $f(n) = \Omega(g(n))$ if there exist positive constants C and k such that:

$$|f(n)| \geq C \cdot |g(n)| \quad \text{for all } n > k$$

f grows **at least as fast** as g.

Big-Θ (tight bound): $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$ **and** $f(n) = \Omega(g(n))$, i.e. there exist positive constants C_1, C_2, and k such that:

$$C_1 \cdot |g(n)| \leq |f(n)| \leq C_2 \cdot |g(n)| \quad \text{for all } n > k$$

f and g have **exactly the same** growth rate (up to constants).

Notation	Meaning	Bound Type
$O(g)$	f grows at most as fast as g	Upper bound
$\Omega(g)$	f grows at least as fast as g	Lower bound
$\Theta(g)$	f and g grow at the same rate	Tight bound

Theorem 3.3 — Growth Rate Hierarchy

The following ordering holds for large n (each class grows strictly faster than the previous):

$$O(1) \subset O(\log n) \subset O(n) \subset O(n \log n) \subset O(n^2) \subset O(n^3) \subset O(2^n) \subset O(n!)$$

If $f(n) = O(g(n))$ and $g(n) = O(h(n))$, then $f(n) = O(h(n))$ (transitivity).
Also: if $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$, then:

$$f_1(n) + f_2(n) = O(\max(g_1(n), g_2(n)))$$

$$f_1(n) \cdot f_2(n) = O(g_1(n) \cdot g_2(n))$$

Example 1: Proving Big-O from the Definition

Show that $f(n) = 3n^2 + 5n + 7$ is $O(n^2)$.

Solution:

Step 1: Find witnesses C and k.
For $n \geq 1$: $n \leq n^2$ and $1 \leq n^2$, so:

$$3n^2 + 5n + 7 \leq 3n^2 + 5n^2 + 7n^2 = 15n^2$$

Step 2: State the witnesses.
Choose $C = 15$ and $k = 1$. Then for all $n > 1$:

$$|3n^2 + 5n + 7| \leq 15n^2 = C \cdot n^2$$

Step 3: Conclude.

$$\boxed{f(n) = 3n^2 + 5n + 7 = O(n^2)}$$

Note: We could also choose $C = 4$, $k = 7$ (tighter), but any valid pair works. The simplest is preferred.

Example 2: Showing n^2 is NOT $O(n)$ — Past Paper 2020 Q5(a)

Show that $f(n) = n^2$ is **not** $O(n)$.

Solution:

Proof by contradiction (see also Section 1.6, Example 8):
Assume for contradiction that $n^2 = O(n)$. Then there exist positive constants C and k such that for all $n > k$:

$$n^2 \leq C \cdot n$$

Dividing both sides by n (valid since $n > 0$):

$$n \leq C \quad \text{for all } n > k$$

But this is impossible — n grows without bound and cannot be bounded above by any constant C. For example, choose $n = \lfloor C \rfloor + k + 1$; then $n > k$ yet $n > C$, giving a contradiction.

Conclusion: $n^2 \neq O(n)$. □

Example 3: Big-O of Polynomial and Logarithm

Find the Big-O classification of each function. Provide witnesses C and k.

(a) $f(n) = 5n^3 + 3n^2 + 100$

(b) $f(n) = 2^n + n^{100}$

(c) $f(n) = \log_2(n^3) + n$

(d) $f(n) = (n+1)!$

Solution:

(a) $f(n) = 5n^3 + 3n^2 + 100$
For $n \geq 10$: $n^2 \leq n^3$ and $100 \leq n^3$:

$$5n^3 + 3n^2 + 100 \leq 5n^3 + 3n^3 + n^3 = 9n^3$$

Witnesses: $C = 9$, $k = 10$. $\boxed{f(n) = O(n^3)}$

(b) $f(n) = 2^n + n^{100}$
For large n, exponentials dominate polynomials: $n^{100} \leq 2^n$ for $n \geq N$ (for some large N). So $2^n + n^{100} \leq 2 \cdot 2^n$.
Witnesses: $C = 2$, $k = N$. $\boxed{f(n) = O(2^n)}$

(c) $f(n) = \log_2(n^3) + n = 3\log_2 n + n$
Since $\log_2 n \leq n$ for all $n \geq 1$: $3\log_2 n + n \leq 3n + n = 4n$.
Witnesses: $C = 4$, $k = 1$. $\boxed{f(n) = O(n)}$

(d) $f(n) = (n+1)! = (n+1) \cdot n!$
$(n+1)! \leq (n+1) \cdot n! \leq n \cdot n!$ is wrong; note $(n+1)! = (n+1) \cdot n!$. Since $n + 1 \leq 2n$ for $n \geq 1$: $(n+1)! \leq 2n \cdot n!$.
$\boxed{f(n) = O(n \cdot n!)}$

Or simply: $(n+1)! \leq (n+1)^{n+1}$ and grows faster than any $O(n^k)$ or $O(c^n)$, so the tightest standard class is $O((n+1)!)$ itself.

Example 4: Complexity of Algorithms

Determine the time complexity of each algorithm segment. Express your answer in Big-O notation.

(a) Linear search:

```
for i = 1 to n:
    if A[i] == target:
        return i
```

```
return -1
```

(b) Nested loops:

```
for i = 1 to n:
    for j = 1 to n:
        sum = sum + A[i][j]
```

(c) Binary search:

```
while low <= high:
    mid = (low + high) / 2
    if A[mid] == target: return mid
    elif A[mid] < target: low = mid + 1
    else: high = mid - 1
```

Solution:

(a) Linear search:
The loop runs at most n times, with $O(1)$ work per iteration.
Complexity: $O(n)$

(b) Nested loops:
Outer loop runs n times. For each iteration of the outer loop, the inner loop also runs n times. Total operations $= n \times n = n^2$.
Complexity: $O(n^2)$

(c) Binary search:
Each iteration halves the search space. Starting with n elements: after k iterations, $\lfloor n/2^k \rfloor$ elements remain. The loop ends when $n/2^k \leq 1$, i.e. $k \geq \log_2 n$.
Complexity: $O(\log n)$

Algorithm	Complexity	Reason
Linear search	$O(n)$	One loop over n elements
Nested loops	$O(n^2)$	Two nested loops
Binary search	$O(\log n)$	Halving at each step

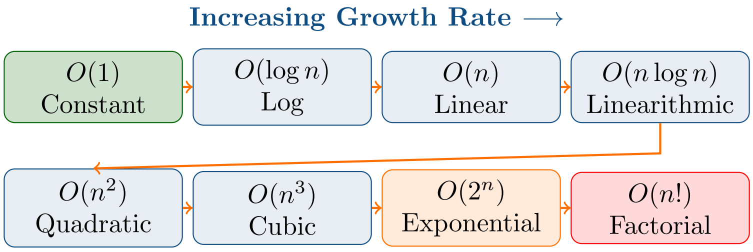


Figure 3.4: Big-O growth rate hierarchy. Green = efficient, red = infeasible for large n.

Section 3.4 Summary — Algorithm Complexity & Big-O

Big-O Proof Template:

To show $f(n) = O(g(n))$:

1. Choose a threshold k (usually small: 1, 2, 7, 10, ...).
2. For $n > k$, bound each sub-term: replace $1 \le n$, $n \le n^2$, etc.
3. Add up to get $f(n) \le C \cdot g(n)$ for an explicit constant C.
4. State: "By definition of Big-O, $f(n) = O(g(n))$ with witnesses $C = \ldots$ and $k = \ldots$"

Common Algorithm Complexities:

Algorithm	Big-O	Pattern
Single loop	$O(n)$	1 loop, $O(1)$ body
Two nested loops	$O(n^2)$	Loop inside loop
Three nested loops	$O(n^3)$	Triple nesting
Divide and halve	$O(\log n)$	Binary search pattern
Divide + merge	$O(n \log n)$	Merge sort pattern
Recursive branching	$O(2^n)$	Fibonacci, subsets

Key Rules (no proof needed):

- Drop constants: $5n = O(n)$, not $O(5n)$.
- Drop lower terms: $n^2 + n = O(n^2)$.
- Sum rule: $O(f) + O(g) = O(\max(f, g))$.
- Product rule: $O(f) \cdot O(g) = O(f \cdot g)$.
- Polynomial: $a_d n^d + \cdots + a_0 = O(n^d)$.

Number Theory

Definition 3.14 — Divisibility

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say a **divides** b, written $a \mid b$, if there exists an integer k such that:

$$b = a \cdot k$$

We also say b is **divisible by** a, or a is a **factor** of b. If a does not divide b, we write $a \nmid b$.

Key Properties:

- $a \mid a$ for all $a \neq 0$ (reflexive on $\mathbb{Z}^+$)
- If $a \mid b$ and $b \mid c$ then $a \mid c$ (transitive)
- If $a \mid b$ and $a \mid c$ then $a \mid (bm + cn)$ for all $m, n \in \mathbb{Z}$
- $1 \mid b$ for all b; $b \mid 0$ for all $b \neq 0$
- If $a \mid b$ and $b \mid a$ then $|a| = |b|$

Definition 3.15 — The Division Algorithm

For any integer a and positive integer d, there exist **unique** integers q (quotient) and r (remainder) with $0 \leq r < d$ such that:

$$a = d \cdot q + r$$

We write $q = a$ **div** d and $r = a$ **mod** d.

Examples:

a	d	$q = a \div d$	$r = a \bmod d$	Check: $dq + r$
17	5	3	2	$5(3) + 2 = 17$ ✓
-11	3	-4	1	$3(-4) + 1 = -11$ ✓
0	7	0	0	$7(0) + 0 = 0$ ✓
100	13	7	9	$13(7) + 9 = 100$ ✓

Key Rule for Negatives: The remainder r must always satisfy $0 \leq r < d$. So for $a = -11$, $d = 3$: $q = -4$ (not -3) because $-3 \cdot (-4) + 1 = 12 - 11 = 1 \geq 0$. *(Past Paper 2020 Q1(iii): $(-17) \bmod 2 = 1$.)*

Definition 3.16 — Modular Arithmetic

For a positive integer m called the **modulus**, integers a and b are **congruent modulo** m, written $a \equiv b \pmod{m}$, if $m \mid (a - b)$.

Arithmetic operations modulo m:

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

$$(a-b) \bmod m = ((a \bmod m) - (b \bmod m) + m) \bmod m$$

Key Properties of Congruence:

- If $a \equiv b$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- Congruence mod m is an equivalence relation (proved in Section 2.4)

Example 1: Modular Arithmetic — Past Paper 2020 Q1(iii)

Compute each of the following:

(a) $(-17) \bmod 2$

(b) $(2^{100}) \bmod 3$

(c) $(7^{50}) \bmod 4$

(d) $(11 \cdot 13) \bmod 7$

Solution:

(a) $(-17) \bmod 2$:
$-17 = 2 \cdot (-9) + 1$. Since $r = 1 \geq 0$: $\boxed{(-17) \bmod 2 = 1}$

(b) $(2^{100}) \bmod 3$:
$2 \equiv -1 \pmod{3}$, so $2^{100} \equiv (-1)^{100} = 1 \pmod{3}$.
$\boxed{2^{100} \bmod 3 = 1}$

(c) $(7^{50}) \bmod 4$:
$7 \equiv 3 \equiv -1 \pmod{4}$, so $7^{50} \equiv (-1)^{50} = 1 \pmod{4}$.
$\boxed{7^{50} \bmod 4 = 1}$

(d) $(11 \cdot 13) \bmod 7$:
$11 \bmod 7 = 4, \quad 13 \bmod 7 = 6$.
$(4 \cdot 6) \bmod 7 = 24 \bmod 7 = 3$.
$\boxed{(11 \cdot 13) \bmod 7 = 3}$
Verification: $11 \times 13 = 143$; $143 = 7 \times 20 + 3$. ✓

Definition 3.17 — Greatest Common Divisor (GCD)

The **greatest common divisor** of two non-zero integers a and b, written $\gcd(a, b)$, is the largest positive integer that divides both a and b:

$$\gcd(a, b) = \max\{d \in \mathbb{Z}^+ \mid d \mid a \text{ and } d \mid b\}$$

Least Common Multiple:

$$\text{lcm}(a, b) = \frac{|a \cdot b|}{\gcd(a, b)}$$

Key Facts:

- $\gcd(a, b) = \gcd(b, a \bmod b)$ (used in the Euclidean Algorithm)
- $\gcd(a, 0) = a$ (base case of Euclidean Algorithm)
- If $\gcd(a, b) = 1$, then a and b are **relatively prime** (coprime).
- $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |a \cdot b|$

Definition 3.18 — The Euclidean Algorithm

The **Euclidean Algorithm** finds $\gcd(a, b)$ by repeated application of the division algorithm:

$$\begin{array}{ll} \textbf{Step 1:} & \text{Divide } a \text{ by } b\text{: } a = bq_1 + r_1, \quad 0 \le r_1 < b \\ \textbf{Step 2:} & \text{Divide } b \text{ by } r_1\text{: } b = r_1 q_2 + r_2 \\ \textbf{Step 3:} & \text{Divide } r_1 \text{ by } r_2\text{: } r_1 = r_2 q_3 + r_3 \\ \vdots & \text{Continue until remainder} = 0 \\ \textbf{Last:} & \gcd(a, b) = \text{last } \textbf{non-zero} \text{ remainder} \end{array}$$

Why it works: $\gcd(a, b) = \gcd(b, a \bmod b)$. This reduces the problem size at each step until we reach $\gcd(d, 0) = d$.

Theorem 3.4 — Bézout's Identity

For any integers a and b (not both zero), there exist integers s and t (called **Bézout coefficients**) such that:

$$\gcd(a, b) = sa + tb$$

These coefficients can be found by the **extended Euclidean algorithm**.

Example 2: Euclidean Algorithm

Find $\gcd(252, 198)$ and $\operatorname{lcm}(252, 198)$ using the Euclidean Algorithm.

Solution:

Euclidean Algorithm:

Step	Division	Equation	Remainder
1	$252 \div 198$	$252 = 198(1) + 54$	$r_1 = 54$
2	$198 \div 54$	$198 = 54(3) + 36$	$r_2 = 36$
3	$54 \div 36$	$54 = 36(1) + 18$	$r_3 = 18$
4	$36 \div 18$	$36 = 18(2) + 0$	$r_4 = 0$ **(stop)**

Last non-zero remainder: $\boxed{\gcd(252, 198) = 18}$

LCM:

$$\operatorname{lcm}(252, 198) = \frac{252 \times 198}{18} = \frac{49896}{18} = \boxed{2772}$$

Verification: $252 = 18 \times 14$ ✓; $198 = 18 \times 11$ ✓

Example 3: GCD by Prime Factorisation

Find $\gcd(360, 504)$ and $\text{lcm}(360, 504)$ using prime factorisation.

Solution:

Prime factorisations:

$$360 = 2^3 \times 3^2 \times 5 \qquad 504 = 2^3 \times 3^2 \times 7$$

GCD: Take the **minimum** exponent of each common prime:

$$\gcd(360, 504) = 2^{\min(3,3)} \times 3^{\min(2,2)} = 2^3 \times 3^2 = 8 \times 9 = \boxed{72}$$

LCM: Take the **maximum** exponent of each prime:

$$\text{lcm}(360, 504) = 2^{\max(3,3)} \times 3^{\max(2,2)} \times 5^1 \times 7^1 = 8 \times 9 \times 5 \times 7 = \boxed{2520}$$

Verify: $\gcd \times \text{lcm} = 72 \times 2520 = 181440 = 360 \times 504$ ✓

Definition 3.19 — Prime and Composite Numbers

An integer $p > 1$ is **prime** if its only positive divisors are 1 and p. An integer $n > 1$ that is not prime is called **composite**.

Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be written as a product of primes in exactly one way (up to order):

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$$

Primality Testing: To test if n is prime, check divisibility by all primes up to $\lfloor \sqrt{n} \rfloor$. If none divides n, then n is prime.

Example 4: Extended Euclidean Algorithm

Use the extended Euclidean Algorithm to find integers s and t such that:

$$\gcd(35, 15) = 35s + 15t$$

Solution:

Step 1: Apply Euclidean Algorithm.

$$35 = 15(2) + 5$$
$$15 = 5(3) + 0$$

$\gcd(35, 15) = 5$.

Step 2: Back-substitute.
From the first equation:

$$5 = 35 - 15(2) = 35(1) + 15(-2)$$

So $s = 1$, $t = -2$.

Verification: $35(1) + 15(-2) = 35 - 30 = 5 = \gcd(35, 15)$ ✓

$$\boxed{\gcd(35, 15) = 5 = 35(1) + 15(-2)}$$

Example 5: Modular Inverse

Find the modular inverse of 7 modulo 26, i.e. find x such that $7x \equiv 1 \pmod{26}$.

Solution:

Step 1: Apply Euclidean Algorithm to find $\gcd(7, 26)$.

$$\begin{aligned} 26 &= 7(3) + 5 \\ 7 &= 5(1) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

$\gcd(7, 26) = 1$ (coprime, so the inverse exists). ✓

Step 2: Back-substitute.

$$\begin{aligned} 1 &= 5 - 2(2) \\ &= 5 - 2(7 - 5) = 3(5) - 2(7) \\ &= 3(26 - 7 \cdot 3) - 2(7) = 3(26) - 9(7) - 2(7) \\ &= 3(26) - 11(7) \end{aligned}$$

So $-11(7) \equiv 1 \pmod{26}$.
Since $-11 \equiv 15 \pmod{26}$:

$$\boxed{7^{-1} \equiv 15 \pmod{26}}$$

Verify: $7 \times 15 = 105 = 4(26) + 1 \equiv 1 \pmod{26}$ ✓
(This modular inverse is used in the Affine Cipher in Section 3.6.)

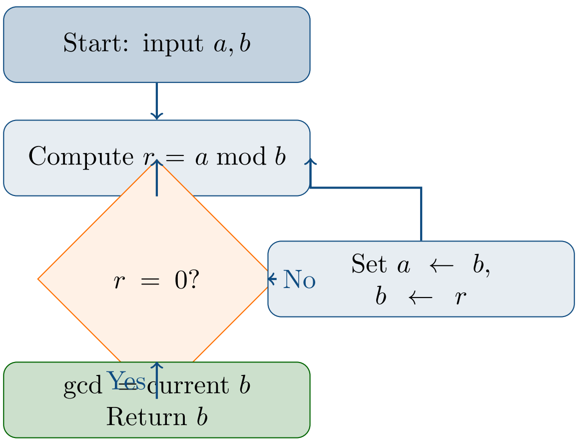


Figure 3.5: Euclidean Algorithm flowchart. At each step, replace (a, b) with $(b, a \bmod b)$ until remainder is zero.

Section 3.5 Summary — Number Theory Basics

Key Formulas:

Concept	Formula / Rule
Division Algorithm	$a = dq + r, \quad 0 \le r < d$
GCD (Euclidean)	$\gcd(a, b) = \gcd(b, a \bmod b)$
GCD via primes	Take **min** exponent of each shared prime
LCM via primes	Take **max** exponent of each prime
GCD × LCM	$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = \lvert a \cdot b\rvert$
Bézout's Identity	$\gcd(a, b) = sa + tb$ for some $s, t \in \mathbb{Z}$
Modular inverse	$x = a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$
Congruence	$a \equiv b \pmod{m} \iff m \mid (a - b)$

Euclidean Algorithm Template:

1. Divide a by b, get remainder r.
2. Replace $(a, b) \leftarrow (b, r)$.
3. Repeat until $r = 0$.
4. $\gcd =$ last non-zero r.
5. For LCM: $\operatorname{lcm} = ab/\gcd$.

Cryptography

Definition 3.20 — Cryptography Terminology

Term	Meaning
Plaintext	Original, readable message
Ciphertext	Encrypted, unreadable message
Encryption	Process of converting plaintext to ciphertext
Decryption	Process of converting ciphertext back to plaintext
Key	Secret value controlling encryption/decryption
Cipher	Algorithm for encryption and decryption
Cryptanalysis	Breaking a cipher without the key
Symmetric key	Same key used for both encryption and decryption
Public key	Two keys: one public (encrypt), one private (decrypt)

Letter-to-Number Encoding: In classical ciphers, letters are mapped to numbers using $A = 0, B = 1, C = 2, \ldots, Z = 25$. All arithmetic is performed modulo 26.

Definition 3.21 — Caesar Cipher (Shift Cipher)

The **Caesar cipher** (or *shift cipher*) with shift k encodes each letter by shifting it k positions forward in the alphabet:

Encryption: $E(p) = (p + k) \bmod 26$
Decryption: $D(c) = (c - k) \bmod 26$

where p is the plaintext letter number (0–25) and c is the ciphertext letter number. The key is $k \in \{0, 1, \ldots, 25\}$.

Key Points:

- Julius Caesar used $k = 3$: A→D, B→E, ..., Z→C.
- Only 26 possible keys — easily broken by exhaustive search.
- Decryption is the inverse: shift back by k.
- $(c - k) \bmod 26$: add 26 if the result is negative.

Example 1: Caesar Cipher Encryption and Decryption

(a) Encrypt the message `HELLO` using the Caesar cipher with $k = 3$.
(b) Decrypt the ciphertext `KHOOR` using $k = 3$.
(c) If the ciphertext is `PBZR` and the key is $k = 7$, find the plaintext.

Solution:

(a) Encrypt `HELLO`, $k = 3$:

Letter	p	$E(p) = (p + 3) \bmod 26$	Ciphertext
H	7	10	K
E	4	7	H
L	11	14	O
L	11	14	O
O	14	17	R

$\boxed{\texttt{HELLO} \xrightarrow{k=3} \texttt{KHOOR}}$

(b) Decrypt `KHOOR`, $k = 3$:

$D(c) = (c-3) \bmod 26$: K(10) → 7(H), H(7) → 4(E), O(14) → 11(L), O(14) → 11(L), R(17) → 14(O).

$\boxed{\texttt{KHOOR} \xrightarrow{k=3} \texttt{HELLO}}$ ✓

(c) Decrypt `PBZR`, $k = 7$:

Cipher	c	$D(c) = (c - 7) \bmod 26$	Plaintext
P	15	8	I
B	1	$-6 \equiv 20$	U
Z	25	18	S
R	17	10	K

$\boxed{\texttt{PBZR} \xrightarrow{k=7} \texttt{IUSK}}$

Definition 3.22 — Affine Cipher

The **affine cipher** uses two keys a and b with $\gcd(a, 26) = 1$:

Encryption: $E(p) = (ap + b) \bmod 26$
Decryption: $D(c) = a^{-1}(c - b) \bmod 26$

where a^{-1} is the **modular inverse** of a modulo 26 (i.e. $a \cdot a^{-1} \equiv 1 \pmod{26}$).

Key Points:

- a must be coprime to 26 so that a^{-1} exists and decryption is unique.
- Valid values of a: $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ — 12 values.
- When $a = 1$, the affine cipher reduces to the Caesar cipher.
- The key space has $12 \times 26 = 312$ possible key pairs (a, b).
- **Modular inverse table for mod 26:**

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Example 2: Affine Cipher

Let $a = 7$, $b = 3$. Encrypt `MATH` and decrypt `XAJP`.

Solution:

Step 1: Find $a^{-1} = 7^{-1} \bmod 26$.
From Section 3.5, Example 5: $7^{-1} \equiv 15 \pmod{26}$.

Step 2: Encryption of `MATH`: $E(p) = (7p + 3) \bmod 26$.

Letter	p	$(7p + 3) \bmod 26$	Ciphertext
M	12	$(84 + 3) \bmod 26 = 87 \bmod 26 = 9$	J
A	0	$(0 + 3) \bmod 26 = 3$	D
T	19	$(133 + 3) \bmod 26 = 136 \bmod 26 = 6$	G
H	7	$(49 + 3) \bmod 26 = 52 \bmod 26 = 0$	A

$\boxed{\texttt{MATH} \xrightarrow{a=7, b=3} \texttt{JDGA}}$

Step 3: Decryption of `XAJP`: $D(c) = 15(c - 3) \bmod 26$.

Cipher	c	$15(c - 3) \bmod 26$	Plaintext
X	23	$15(20) \bmod 26 = 300 \bmod 26 = 14$	O
A	0	$15(-3) \bmod 26 = -45 \bmod 26 = 7$	H
J	9	$15(6) \bmod 26 = 90 \bmod 26 = 12$	M
P	15	$15(12) \bmod 26 = 180 \bmod 26 = 24$	Y

$\boxed{\texttt{XAJP} \xrightarrow{a=7, b=3} \texttt{OHMY}}$

Definition 3.23 — RSA Public Key Cryptosystem

RSA (Rivest–Shamir–Adleman, 1977) is a **public key** cryptosystem based on the difficulty of factoring large integers.

Key Generation:

Step 1: Choose two large distinct primes p and q.

Step 2: Compute $n = p \cdot q$ (the **modulus**).

Step 3: Compute $\phi(n) = (p-1)(q-1)$ (Euler's totient function).

Step 4: Choose e with $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.

Step 5: Find $d = e^{-1} \bmod \phi(n)$ (using extended Euclidean).

Step 6: **Public key:** (n, e) **Private key:** (n, d)

Encryption: $C = M^e \bmod n$
Decryption: $M = C^d \bmod n$

Key Points:

- M is the plaintext (as a number with $M < n$).
- The public key (n, e) is shared openly; the private key d is secret.
- Security relies on the fact that factoring $n = pq$ for large primes is computationally infeasible.
- $(M^e)^d \equiv M^{ed} \equiv M \pmod{n}$ by Euler's theorem since $ed \equiv 1 \pmod{\phi(n)}$.

Theorem 3.5 — RSA Correctness

In the RSA scheme with $n = pq$, $\gcd(e, \phi(n)) = 1$, and $d = e^{-1} \bmod \phi(n)$, decryption correctly recovers the plaintext:

$$(M^e)^d \equiv M \pmod{n} \quad \text{for all } M \text{ with } \gcd(M, n) = 1$$

Example 3: RSA Key Generation and Encryption

Let $p = 5$, $q = 11$. Use $e = 3$.

(a) Generate the RSA public and private keys.

(b) Encrypt $M = 9$.

(c) Decrypt the ciphertext to verify.

Solution:

(a) Key Generation:
Step 1: $n = p \cdot q = 5 \times 11 = 55$
Step 2: $\phi(n) = (p-1)(q-1) = 4 \times 10 = 40$

Step 3: Verify $\gcd(e, \phi(n)) = \gcd(3, 40) = 1$ ✓
Step 4: Find $d = e^{-1} \bmod 40$:
Need $3d \equiv 1 \pmod{40}$. By inspection or extended Euclidean: $3 \times 27 = 81 = 2(40) + 1$, so $d = 27$.

Public key: $(n, e) = (55, 3)$
Private key: $(n, d) = (55, 27)$

(b) Encrypt $M = 9$:

$$C = M^e \bmod n = 9^3 \bmod 55 = 729 \bmod 55$$

$729 = 55 \times 13 + 14$, so $C = 14$.

$$\boxed{C = 14}$$

(c) Decrypt $C = 14$:

$$M = C^d \bmod n = 14^{27} \bmod 55$$

Use repeated squaring:

$$\begin{aligned}
14^1 &\equiv 14 \pmod{55} \\
14^2 &\equiv 196 \equiv 196 - 3(55) = 31 \pmod{55} \\
14^4 &\equiv 31^2 = 961 \equiv 961 - 17(55) = 26 \pmod{55} \\
14^8 &\equiv 26^2 = 676 \equiv 676 - 12(55) = 16 \pmod{55} \\
14^{16} &\equiv 16^2 = 256 \equiv 256 - 4(55) = 36 \pmod{55} \\
14^{27} &= 14^{16} \cdot 14^8 \cdot 14^2 \cdot 14^1 \\
&\equiv 36 \cdot 16 \cdot 31 \cdot 14 \pmod{55}
\end{aligned}$$

Compute step by step: $36 \times 16 = 576 \equiv 576 - 10(55) = 26 \pmod{55}$
$26 \times 31 = 806 \equiv 806 - 14(55) = 36 \pmod{55}$
$36 \times 14 = 504 \equiv 504 - 9(55) = 9 \pmod{55}$

$$\boxed{M = 14^{27} \bmod 55 = 9}$$

Decryption correctly recovers $M = 9$. ✓

Example 4: RSA with Larger Primes — Past Paper 2025 Q5 (Related)

Let $p = 7$, $q = 13$, and $e = 5$.

(a) Find n, $\phi(n)$, and the private key d.

(b) Encrypt $M = 3$.

(c) Decrypt $C = 47$.

Solution:

(a)
$n = 7 \times 13 = 91$
$\phi(n) = 6 \times 12 = 72$

$\gcd(5, 72) = 1$ ✓
Find d: $5d \equiv 1 \pmod{72}$.
Extended Euclidean on $(72, 5)$:

$$\begin{aligned} 72 &= 5(14) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

Back-substitute: $1 = 5 - 2(2) = 5 - 2(72 - 5 \cdot 14) = 29(5) - 2(72)$
So $d = 29$.
Private key: $(91, 29)$ **Public key:** $(91, 5)$

(b) Encrypt $M = 3$:

$$C = 3^5 \bmod 91 = 243 \bmod 91 = 243 - 2(91) = \boxed{61}$$

(c) Decrypt $C = 47$:

$$M = 47^{29} \bmod 91$$

Using repeated squaring (key steps):

$$\begin{aligned} 47^1 &\equiv 47 \pmod{91} \\ 47^2 &\equiv 2209 \bmod 91 = 2209 - 24(91) = 25 \pmod{91} \\ 47^4 &\equiv 25^2 = 625 \bmod 91 = 625 - 6(91) = 79 \pmod{91} \\ 47^8 &\equiv 79^2 = 6241 \bmod 91 = 6241 - 68(91) = 53 \pmod{91} \\ 47^{16} &\equiv 53^2 = 2809 \bmod 91 = 2809 - 30(91) = 79 \pmod{91} \end{aligned}$$

$47^{29} = 47^{16} \cdot 47^8 \cdot 47^4 \cdot 47^1$:
$79 \times 53 = 4187 \bmod 91 = 4187 - 46(91) = 1 \pmod{91}$
$1 \times 79 = 79 \pmod{91}$
$79 \times 47 = 3713 \bmod 91 = 3713 - 40(91) = 73 \pmod{91}$

$$\boxed{M = 47^{29} \bmod 91 = 73}$$

Note: The plaintext 73 corresponds to the letter T (if using 0-indexed letters with T=19, this would be interpreted as a number block, not a single letter).

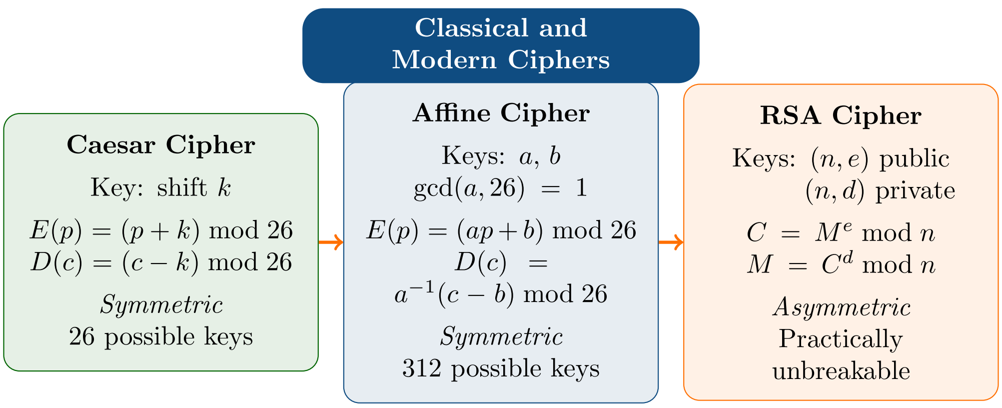


Figure 3.6: From Caesar (26 keys) to Affine (312 keys) to RSA (essentially unbreakable). Each is

stronger than the previous.

Section 3.6 Summary — Cryptography

Three Ciphers Compared:

Feature	Caesar	Affine	RSA
Type	Symmetric	Symmetric	Asymmetric
Keys	k	(a, b)	(n, e, d)
Encrypt	$p + k$	$ap + b$	M^e
Decrypt	$c - k$	$a^{-1}(c - b)$	C^d
Modulus	26	26	$n = pq$
Key space	26	312	Astronomically large
Security basis	None	None	Difficulty of factoring

RSA Step-by-Step:

1. Choose primes p, q. Compute $n = pq$.
2. Compute $\phi(n) = (p - 1)(q - 1)$.
3. Choose e with $\gcd(e, \phi(n)) = 1$.
4. Find $d = e^{-1} \bmod \phi(n)$ via extended Euclidean.
5. Encrypt: $C = M^e \bmod n$.
6. Decrypt: $M = C^d \bmod n$.

Affine Cipher Checklist:

- Always verify $\gcd(a, 26) = 1$ before proceeding.
- Find $a^{-1} \bmod 26$ using the extended Euclidean algorithm.
- For decryption: $D(c) = a^{-1}(c - b) \bmod 26$. Add 26 if the result is negative.

Practice Exercises

Q1. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d, e\}$. For each mapping below, state whether it is a valid function from A to B. If yes, classify it as injective, surjective, bijective, or into. If no, explain why not.

(i) $f = \{(1, a), (2, b), (3, a), (4, c)\}$
(ii) $g = \{(1, a), (2, b), (3, c)\}$
(iii) $h = \{(1, a), (2, b), (3, c), (4, d), (1, e)\}$
(iv) $k = \{(1, b), (2, d), (3, a), (4, c)\}$

Q2. Determine whether each function $f : \mathbb{R} \to \mathbb{R}$ is injective, surjective, both, or neither. Prove your answer in each case.

(i) $f(x) = 5x - 3$
(ii) $f(x) = x^2 + 4$
(iii) $f(x) = x^3 - 8$
(iv) $f(x) = |x|$
(v) $f(x) = \dfrac{2x}{x+1}$ (assume $x \neq -1$)

Q3. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = 2n + 1$ and $g : \mathbb{Z} \to \mathbb{Z}$ by $g(n) = n^2 - 3$.

(i) Compute $(g \circ f)(n)$ and $(f \circ g)(n)$.
(ii) Evaluate $(g \circ f)(3)$ and $(f \circ g)(-2)$.
(iii) Is $g \circ f = f \circ g$? Justify.
(iv) Find $(f \circ f)(n)$ and $(g \circ g)(n)$.

Q4. Let $A = \{1, 2, 3, 4, 5\}$ and define $f, g : A \to A$ by:

$$f = \{(1, 2), (2, 4), (3, 1), (4, 5), (5, 3)\} \qquad g = \{(1, 3), (2, 1), (3, 5), (4, 2), (5, 4)\}$$

(i) Find $g \circ f$, $f \circ g$, and $f \circ f$.
(ii) Is f a bijection? Find f^{-1}.
(iii) Is g a bijection? Find g^{-1}.
(iv) Verify $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Q5. Find the inverse of each function (if it exists). If no inverse exists, explain why. Verify each inverse using the identity $f(f^{-1}(x)) = x$.

(i) $f(x) = 4x - 9$
(ii) $f(x) = \dfrac{x+3}{2x-1}$
(iii) $f(x) = x^2 - 5$ (domain: $\mathbb{R}$)
(iv) $f(x) = \sqrt{2x+6}$ (domain: $x \geq -3$)
(v) $f(x) = e^{2x}$

Q6. A recurrence relation is defined by $a_1 = 5$ and $a_n = 3a_{n-1} - 2$ for $n \geq 2$.

(i) Compute a_2, a_3, a_4, a_5.

(ii) Solve the recurrence by iteration to find a closed-form formula for a_n.

(iii) Verify the closed form using the values from part (i).

(iv) What is a_{10}?

Q7. Solve each recurrence relation by iteration. State the closed-form solution and verify with the initial condition.

(i) $a_n = a_{n-1} + 7, \quad a_1 = 3$

(ii) $a_n = 4a_{n-1}, \quad a_0 = 2$

(iii) $a_n = 2a_{n-1} + 3, \quad a_0 = 1$

(iv) $a_n = a_{n-1} + n, \quad a_0 = 0$

Q8. The number of bacteria in a culture doubles every hour. Initially there are 100 bacteria.

(i) Write a recurrence relation for $B(n)$, the number of bacteria after n hours.

(ii) Solve the recurrence to find $B(n)$ in closed form.

(iii) How many bacteria are there after 8 hours?

(iv) After how many hours will the count exceed 1,000,000?

Q9. Prove or disprove each Big-O claim by finding explicit witnesses C and k or by providing a contradiction argument.

(i) $6n^2 + 4n + 3 = O(n^2)$

(ii) $2^n + n^5 = O(n^5)$

(iii) $n \log n + n = O(n \log n)$

(iv) $n^3 = O(n^2)$

(v) $5 = O(1)$

Q10. Determine the time complexity of each algorithm in Big-O notation. Justify your answer by counting the number of basic operations.

(i) **Sum of array:** `s = 0; for i = 1 to n:  s = s + A[i]`

(ii) **Bubble sort (worst case):** Two nested loops each running n times.

(iii) **Recursive factorial:** $T(n) = T(n-1) + O(1)$, $T(0) = O(1)$.

(iv) **Matrix multiplication:** Three nested loops each of size n.

(v) **Merge sort:** $T(n) = 2T(n/2) + O(n)$. (State the result only.)

Q11. Arrange the following functions in increasing order of their Big-O growth rate. Then state which functions are in the same complexity class.

$$3n^2, \quad 100, \quad 2^n, \quad n \log n, \quad n!, \quad \sqrt{n}, \quad 5n^3 + 2n, \quad \log_2 n$$

Q12. Compute each of the following using the properties of modular arithmetic. Show all working clearly.

(i) $(-23) \bmod 5$

(ii) $(2^{50}) \bmod 7$

(iii) $(3^{100}) \bmod 4$

(iv) $(17 \times 29) \bmod 11$

(v) $(5^{12}) \bmod 13$ (Hint: $5^2 \equiv 12 \equiv -1 \pmod{13}$)

Q13. Use the Euclidean Algorithm to find $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ for each pair. Show every step of the algorithm.

(i) $\gcd(414, 662)$

(ii) $\gcd(1001, 364)$

(iii) $\gcd(144, 89)$

(iv) $\gcd(1000, 625)$

Q14. Find integers s and t (Bézout coefficients) such that $\gcd(a, b) = sa + tb$ for each pair below. Use the extended Euclidean Algorithm.

(i) $\gcd(26, 9)$

(ii) $\gcd(55, 22)$

(iii) $\gcd(77, 13)$

Q15. Find the modular inverse of each value (if it exists). If no inverse exists, explain why.

(i) $3^{-1} \bmod 26$

(ii) $11^{-1} \bmod 26$

(iii) $4^{-1} \bmod 26$

(iv) $5^{-1} \bmod 11$

(v) $7^{-1} \bmod 40$

Q16. Encrypt the following messages using the Caesar cipher with the given key k. Then decrypt the resulting ciphertext to verify.

(i) Encrypt `DISCRETE` with $k = 4$

(ii) Encrypt `PAKISTAN` with $k = 13$

(iii) Decrypt `GXEVKZEX` with $k = 3$

(iv) Decrypt `ZHOFRPH` with $k = 3$

Q17. For the affine cipher with keys (a, b):

(i) Encrypt `LOGIC` using $a = 5$, $b = 8$.

(ii) Decrypt `RCLLA` using $a = 5$, $b = 8$.

(iii) Encrypt `MATH` using $a = 11$, $b = 7$.

(iv) Why can we not use $a = 4$ in an affine cipher over $\mathbb{Z}_{26}$?

(v) Find the decryption key for $(a, b) = (9, 4)$.

Q18. Perform RSA key generation for each set of primes and encryption key. Then encrypt the given plaintext and decrypt to verify.

(i) $p = 3$, $q = 11$, $e = 7$; encrypt $M = 5$.

(ii) $p = 5$, $q = 7$, $e = 5$; encrypt $M = 3$.

(iii) $p = 11$, $q = 13$, $e = 7$; encrypt $M = 2$.

Q19. Mixed function and cryptography: A message is encoded first using the affine cipher with $a = 3$, $b = 5$, then the result is shifted by $k = 4$ using the Caesar cipher.

(i) Write the composed encryption formula as a single affine cipher.

(ii) Encrypt `HELLO` using the composed cipher.

(iii) Find the decryption formula for the composed cipher.

(iv) Is the composition of two affine ciphers always affine? Justify.

Q20. Comprehensive problem: A company uses the RSA system with public key $(n, e) = (33, 7)$.

(i) Factor $n = 33$ to find primes p and q.

(ii) Compute $\phi(n) = (p - 1)(q - 1)$.

(iii) Find the private key $d = e^{-1} \bmod \phi(n)$.

(iv) Encrypt the messages $M = 2$, $M = 5$, and $M = 10$.

(v) Decrypt the ciphertext $C = 14$ to recover the original message.

(vi) Why would it be insecure to use $n = 33$ in a real RSA system?

Chapter 4

Counting and Combinatorics

Basic Counting Principles

Definition 4.1 — The Product Rule

If a procedure can be broken into **two successive tasks**, where task 1 can be done in n_1 ways and task 2 can be done in n_2 ways **regardless of how task 1 was done**, then the total number of ways to do the procedure is:

$$n_1 \times n_2$$

More generally, for k successive tasks with $n_1, n_2, \ldots, n_k$ ways respectively:

$$n_1 \times n_2 \times \cdots \times n_k$$

Key Points:

- Use the product rule when tasks are performed **simultaneously** or **one after the other**.
- The tasks must be **independent**: the number of ways to do task 2 does not depend on which choice was made in task 1.
- Think of it as filling **slots**: one slot per task, multiply the number of choices for each slot.

Past Paper: 2020 Q1(x), 2023 Q1(xii), 2025 Q4

Example 1: Applying the Product Rule — Past Paper 2023 Q1(xii) & 2025 Q4

(a) [**2023 Q1(xii)**] A car number plate is formed by 4 digits from $\{1, 2, \ldots, 9\}$ followed by 3 letters from the alphabet (26 letters). Neither digits nor letters are repeated. How many plates are possible?

(b) How many bit strings of length 8 are there?

Solution:

(a) Seven successive slots, no repetition within digits or within letters:

Digit 1	Digit 2	Digit 3	Digit 4	Letter 1	Letter 2	Letter 3
9	8	7	6	26	25	24

$$9 \times 8 \times 7 \times 6 \times 26 \times 25 \times 24 = 3024 \times 15600 = \boxed{47{,}174{,}400}$$

(b) Each of the 8 bits is independently 0 or 1 (2 choices):

$$\underbrace{2 \times 2 \times \cdots \times 2}_{8} = 2^8 = \boxed{256}$$

Definition 4.2 — The Sum Rule

If a task can be done either in n_1 ways **or** in n_2 ways, where the two sets of ways are **disjoint** (no overlap), then the total number of ways to do the task is:

$$n_1 + n_2$$

More generally, for k mutually exclusive alternatives:

$$n_1 + n_2 + \cdots + n_k$$

Key Points:

- Use the sum rule when you **choose one option from multiple alternatives**.
- The alternatives must be **mutually exclusive**: no outcome can satisfy more than one alternative.
- If alternatives *do* overlap, use **Inclusion-Exclusion** (Section 4.4).

Combined rule: Most counting problems use both rules together. Break the problem into tasks (product rule) and cases (sum rule).

Past Paper: 2020 Q1(x), 2025 Q4

Example 2: Sum Rule and Product Rule Combined — Past Paper 2025 Q4

How many license plates can be made using either:

- two uppercase English letters followed by four digits, **or**
- two digits followed by four uppercase English letters?

Repetition is allowed.

Solution:

The two formats are **mutually exclusive** (different structures).
Case 1 — 2 letters then 4 digits:

$$\underbrace{26 \times 26}_{\text{letters}} \times \underbrace{10 \times 10 \times 10 \times 10}_{\text{digits}} = 26^2 \times 10^4 = 676 \times 10{,}000 = 6{,}760{,}000$$

Case 2 — 2 digits then 4 letters:

$$\underbrace{10 \times 10}_{\text{digits}} \times \underbrace{26 \times 26 \times 26 \times 26}_{\text{letters}} = 10^2 \times 26^4 = 100 \times 456{,}976 = 45{,}697{,}600$$

By Sum Rule (two disjoint cases):

$$6{,}760{,}000 + 45{,}697{,}600 = \boxed{52{,}457{,}600}$$

Definition 4.3 — The Subtraction Rule (Complementary Counting)

If a task can be done in N total ways and n_{bad} of those ways violate a constraint, then the number of **valid** ways is:

$$N - n_{\text{bad}}$$

This is called **complementary counting**: it is often easier to count what you do **not** want and subtract.

When to use:

- Keywords: **"at least one"**, **"not all"**, **"except"**, **"other than"**.
- When counting valid outcomes directly is harder than counting invalid ones.

Example 3: Subtraction Rule — Past Paper 2022 Q1(viii)

(a) [**2022 Q1(viii)**] Let A be the set of odd positive integers less than 10. Find $|A|$.
(b) How many 4-digit passwords using digits 0–9 contain **at least one** 7?
(c) How many bit strings of length 8 start with 1 or end with 00?

Solution:

(a) Odd positive integers less than 10: $A = \{1, 3, 5, 7, 9\} \Rightarrow |A| = \boxed{5}$
(b) Complementary counting:
Total 4-digit passwords: $10^4 = 10{,}000$.
Passwords with **no 7**: each digit has 9 choices $\Rightarrow 9^4 = 6{,}561$.
At least one 7:

$$10{,}000 - 6{,}561 = \boxed{3{,}439}$$

(c) Let A = strings starting with 1, B = strings ending with 00.
$|A| = 2^7 = 128$; $|B| = 2^6 = 64$; $|A \cap B| = 2^5 = 32$ (starts with 1 AND ends with 00).
$|A \cup B| = 128 + 64 - 32 = \boxed{160}$

Definition 4.4 — The Division Rule

If a counting method counts each distinct object exactly d times, the number of distinct objects is:

$$\frac{\text{total count}}{d}$$

Key application: The **Handshaking Lemma** is a direct application. Each edge is counted twice in the degree sum (once for each endpoint):

$$\sum_{v\in V} \deg(v) = 2|E| \quad \Rightarrow \quad |E| = \frac{\sum \deg(v)}{2}$$

Past Paper: 2021 Q1(vii) — "How many edges in a graph with 10 vertices each of degree 6?"

Example 4: Division Rule — Past Paper 2021 Q1(vii)

(a) [**2021 Q1(vii)**] How many edges are there in a graph with 10 vertices each of degree 6?

(b) How many ways can 6 people sit around a round table?

(c) A class has 30 students. How many handshakes occur if every student shakes hands with every other student exactly once?

Solution:

(a) Division rule via Handshaking Lemma:

$$\sum \deg(v) = 10 \times 6 = 60 = 2|E| \implies |E| = \frac{60}{2} = \boxed{30}$$

(b) Linear arrangements: $6! = 720$. Each circular arrangement is counted 6 times (one per rotation). Apply division rule:

$$\frac{6!}{6} = \frac{720}{6} = (6-1)! = 5! = \boxed{120}$$

(c) Each pair of students shakes hands once. Total ordered pairs: $30 \times 29 = 870$. Division rule (each handshake counted twice):

$$\frac{30 \times 29}{2} = \binom{30}{2} = \boxed{435}$$

Example 5: Mixed Counting — Exam-Style

(a) How many 3-digit numbers can be formed from $\{1, 2, 3, 4, 5\}$ with no repeated digits? How many of these are even?

(b) A committee of 2 is chosen from 4 men and 3 women. How many committees have **at least one woman**?

(c) How many 4-character passwords use letters A–Z and digits 0–9 and contain **at least one digit**?

Solution:

(a) No repetition, 3 digits from 5:

$$5 \times 4 \times 3 = \boxed{60}$$

Even means last digit $\in \{2, 4\}$ (2 choices). Fix last digit (2 choices), then first two slots get 4 and 3 choices:

$$4 \times 3 \times 2 = \boxed{24}$$

(b) Total committees of 2 from 7: $\binom{7}{2} = 21$.
All-male committees: $\binom{4}{2} = 6$.
At least one woman:

$$21 - 6 = \boxed{15}$$

(c) Each position: $26 + 10 = 36$ choices. Total $= 36^4 = 1{,}679{,}616$.
No digit (all letters): $26^4 = 456{,}976$.
At least one digit:

$$1{,}679{,}616 - 456{,}976 = \boxed{1{,}222{,}640}$$

Product Rule

Task 1 **AND** Task 2

$n_1 \times n_2$

Tasks are **independent**

Keywords: sequential, simultaneous, slots

Example: $26^2 \times 10^4$

vs

Sum Rule

Case 1 **OR** Case 2

$n_1 + n_2$

Cases are **disjoint**

Keywords: or, either, alternative, format

Example: 6.76M + 45.7M

Figure 4.1: Product Rule (AND) vs Sum Rule (OR). Most problems combine both.

Section 4.1 Summary — Basic Counting Principles

Four Rules:

Rule	When to use	Formula
Product	Do task 1 AND task 2	$n_1 \times n_2$
Sum	Choose case 1 OR case 2 (disjoint)	$n_1 + n_2$
Subtraction	Count complement, subtract	$N - n_{\text{bad}}$
Division	Each object counted d times	total $\div\, d$

Quick Decision Guide:

- **"and"** / sequential tasks → **multiply**
- **"or"** / separate cases → **add**
- **"at least"** / **"at most"** → complement: total − opposite
- **No repetition** → choices decrease: $n, n{-}1, n{-}2, \ldots$
- **With repetition** → choices constant: n^k

Past Paper Connection:

- **2020 Q1(x):** Name the basic counting principles → Definitions 4.1 & 4.2
- **2021 Q1(vii):** Edges in a 10-vertex degree-6 graph → Example 4(a) (division rule)

- **2022 Q1(viii):** $|A|$ where A = odd integers $< 10 \rightarrow$ Example 3(a)
- **2023 Q1(xii):** Car plates, no repetition $\rightarrow$ Example 1(a)
- **2025 Q4:** License plates, two formats, sum + product $\rightarrow$ Example 2

Permutations and Combinations

Definition 4.5 — Factorial

The **factorial** of a non-negative integer n, written $n!$, is:

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 \qquad \text{with } 0! = 1$$

Common values:

n	0	1	2	3	4	5	6
$n!$	1	1	2	6	24	120	720

Key identity: $n! = n \times (n-1)!$ (useful for simplifying expressions)

Past Paper: Used throughout 2023 Q3

Definition 4.6 — Permutation

A **permutation** is an **ordered** arrangement of objects.

Permutation of n distinct objects taken r at a time:

$$P(n,r) = \frac{n!}{(n-r)!} = n \times (n-1) \times \cdots \times (n-r+1) \qquad (0 \leq r \leq n)$$

Permutation of all n objects:

$$P(n,n) = n!$$

Key Properties:

- **Order matters**: arrangement AB is different from BA.
- Each object can be used **at most once** (no repetition).
- Think of filling r ordered slots: first slot has n choices, second has $n-1$, and so on.

Quick reference:

Expression	Expanded	Value
$P(5,2)$	5×4	20
$P(6,3)$	$6 \times 5 \times 4$	120
$P(7,7)$	$7!$	5040
$P(7,1)$	7	7

Past Paper: 2023 Q3 (all 6 parts use permutation logic), 2023 Q1(xii), 2025 Q4

Example 1: Basic Permutations

(a) How many ways can 5 students be arranged in a row?

(b) How many 3-letter arrangements can be made from MATH (no repetition)?

(c) A president, vice-president, and secretary are chosen from 10 candidates. How many ways?

Solution:

(a) Arrange all 5 students in order:

$$P(5,5) = 5! = \boxed{120}$$

(b) Choose 3 from 4 letters {M,A,T,H}, order matters:

$$P(4,3) = \frac{4!}{(4-3)!} = \frac{24}{1} = 4 \times 3 \times 2 = \boxed{24}$$

(c) Three distinct roles from 10 candidates, order matters:

$$P(10,3) = 10 \times 9 \times 8 = \boxed{720}$$

Definition 4.7 — Permutations with Repeated Elements

The number of distinct permutations of n objects where object 1 appears n_1 times, object 2 appears n_2 times, …, object k appears n_k times (with $n_1 + n_2 + \cdots + n_k = n$) is:

$$\frac{n!}{n_1!\, n_2!\, \cdots\, n_k!}$$

Examples:

- Arrangements of **AABB** (4 letters: A×2, B×2): $\dfrac{4!}{2!\,2!} = 6$
- Arrangements of **MISSISSIPPI** (11 letters: M×1, I×4, S×4, P×2): $\dfrac{11!}{1!\,4!\,4!\,2!} =$ 34,650

Past Paper: 2023 Q3 — required strings treated as single repeated units.

Definition 4.8 — Permutations Containing a Fixed String

To count permutations of n objects that **must contain a specific consecutive substring**:

1. **Glue** all letters of the required string into one single block.
2. Count the total objects to arrange: $(n - s + 1)$ where s is the length of the glued string.
3. Total permutations $= (n - s + 1)!$

Multiple required strings: Glue each required string into its own block, then count arrangements of all blocks and remaining letters.

Overlapping strings: If two required strings **share a letter at the joining point**, merge them into one combined block. If two strings share a letter but the overlap is **incompatible** (the letter must occupy two different positions), the answer is **0**.

Past Paper: 2023 Q3 (all 6 parts)

Example 2: Permutations of ABCDEFG with Strings — Past Paper 2023 Q3

How many permutations of **ABCDEFG** ($n = 7$ distinct letters) contain the following strings?

i) BCD **ii)** CFGA **iii)** BA and GF **iv)** ABC and DE **v)** ABC and CDE **vi)** CBA and BED

Solution:

i) String BCD (length 3):

Glue $\{B, C, D\}$ into block $[BCD]$. Remaining letters: A, E, F, G. Total objects: $[BCD], A, E, F, G = 5$.

$$5! = \boxed{120}$$

ii) String CFGA (length 4):

Glue $\{C, F, G, A\}$ into block $[CFGA]$. Remaining: B, D, E.
Total objects: $[CFGA], B, D, E = 4$.

$$4! = \boxed{24}$$

iii) Strings BA and GF (two separate blocks):

Glue $B, A \to [BA]$. Glue $G, F \to [GF]$. Total objects: $[BA], [GF], C, D, E = 5$.

$$5! = \boxed{120}$$

iv) Strings ABC and DE (two non-overlapping blocks):

Glue $A, B, C \to [ABC]$. Glue $D, E \to [DE]$. Total objects: $[ABC], [DE], F, G = 4$.

$$4! = \boxed{24}$$

v) Strings ABC and CDE (overlapping at C):

ABC ends in C; CDE starts with C. For both substrings to appear, C must be simultaneously the 3rd letter of ABC and the 1st letter of CDE, forcing the combined block $[ABCDE]$. Total objects: $[ABCDE], F, G = 3$.

$$3! = \boxed{6}$$

vi) Strings CBA and BED (B appears in both):

CBA contains B at position 2; BED starts with B. Since B is a single letter appearing once in ABCDEFG, it cannot simultaneously be in two different positions required by CBA and BED.

$$\text{Answer} = \boxed{0}$$

Definition 4.9 — Combination

A **combination** is an **unordered** selection of objects.

Number of ways to choose r objects from n distinct objects (order does not matter):

$$C(n,r) = \binom{n}{r} = \frac{n!}{r!\,(n-r)!} \qquad (0 \le r \le n)$$

Key Properties:

- **Order does not matter**: $\{A,B\} = \{B,A\}$.
- $\binom{n}{r} = \binom{n}{n-r}$ (symmetry)
- $\binom{n}{0} = \binom{n}{n} = 1$; $\binom{n}{1} = n$
- **Link to permutation:** $P(n,r) = \binom{n}{r} \times r!$

Quick reference:

Expression	Expanded	Value
$\binom{5}{2}$	$\frac{5\times 4}{2!}$	10
$\binom{6}{3}$	$\frac{6\times 5\times 4}{3!}$	20
$\binom{7}{4}$	$\frac{7\times 6\times 5\times 4}{4!}$	35
$\binom{10}{5}$	$\frac{10!}{5!\,5!}$	252

Past Paper: Selection / committee problems appear in exam-style 4.2 questions.

Example 3: Applying Combinations

(a) How many ways can a committee of 3 be chosen from 10 people?

(b) A class has 12 boys and 8 girls. How many committees of 5 contain exactly 3 boys and 2 girls?

(c) How many ways can you choose at least one book from a shelf of 4 different books?

Solution:

(a) Order does not matter (committee):

$$\binom{10}{3} = \frac{10\times 9\times 8}{3!} = \frac{720}{6} = \boxed{120}$$

(b) Choose boys AND choose girls (product rule with combinations):

$$\binom{12}{3} \times \binom{8}{2} = \frac{12\times 11\times 10}{6} \times \frac{8\times 7}{2} = 220 \times 28 = \boxed{6{,}160}$$

(c) Each book independently chosen or not $\Rightarrow 2^4$ total subsets. At least one book = total − empty set:

$$2^4 - 1 = 16 - 1 = \boxed{15}$$

Definition 4.10 — Permutation vs Combination: How to Decide

Feature	**Permutation**	**Combination**
Order	Matters ($AB \neq BA$)	Does not matter ($AB = BA$)
Formula	$\dfrac{n!}{(n-r)!}$	$\dfrac{n!}{r!\,(n-r)!}$
Keywords	arrange, rank, seat, schedule, order	choose, select, committee, group, team, subset
Example	Top-3 finishers in race	3 members from a club
Relation	$P(n,r) = C(n,r) \times r!$	

Quick test: Ask *"Does swapping two chosen items give a different result?"* Yes $\rightarrow$ Permutation. No $\rightarrow$ Combination.

Example 4: Permutation vs Combination Mixed

Identify whether each uses P or C, then solve.

(a) 8 runners compete; how many ways can gold, silver, and bronze medals be awarded?

(b) A team of 4 is chosen from 9 players. How many teams?

(c) How many 4-digit PIN codes use digits 0–9 with no repeated digit?

(d) From 5 men and 4 women, how many committees of 4 contain **at least 2 women**?

Solution:

(a) Different medals $\Rightarrow$ order matters. **Permutation.**

$$P(8,3) = 8 \times 7 \times 6 = \boxed{336}$$

(b) Team membership, no roles $\Rightarrow$ order does not matter. **Combination.**

$$\binom{9}{4} = \frac{9 \times 8 \times 7 \times 6}{4!} = \boxed{126}$$

(c) 4 ordered positions, no repetition. **Permutation.**

$$P(10,4) = 10 \times 9 \times 8 \times 7 = \boxed{5040}$$

(d) At least 2 women: split into cases.

Women	Men	Ways	Count
2	2	$\binom{4}{2} \times \binom{5}{2}$	$6 \times 10 = 60$
3	1	$\binom{4}{3} \times \binom{5}{1}$	$4 \times 5 = 20$
4	0	$\binom{4}{4} \times \binom{5}{0}$	$1 \times 1 = 1$
		Total	**81**

Example 5: License Plates Analysis — Past Paper 2023 Q1(xii) & 2025 Q4

(a) [**2023 Q1(xii)**] A car plate: 4 digits from $\{1, \ldots, 9\}$ then 3 letters from 26, no repetition within each group.

(b) [**2025 Q4**] License plates: 2 letters + 4 digits OR 2 digits + 4 letters, repetition allowed.

(c) Compare: choose 3 letters for a code where order matters vs order does not matter.

Solution:

(a) Different positions are distinct, no repetition. This is a **permutation** calculation.
Digits in order: $P(9,4) = 9 \times 8 \times 7 \times 6 = 3024$
Letters in order: $P(26,3) = 26 \times 25 \times 24 = 15{,}600$
Total (product rule):

$$3024 \times 15{,}600 = \boxed{47{,}174{,}400}$$

(b) Repetition allowed $\Rightarrow$ not a pure permutation; use product rule with independent slots.
Case 1 (2L + 4D): $26^2 \times 10^4 = 676 \times 10{,}000 = 6{,}760{,}000$
Case 2 (2D + 4L): $10^2 \times 26^4 = 100 \times 456{,}976 = 45{,}697{,}600$
By sum rule (disjoint formats):

$$6{,}760{,}000 + 45{,}697{,}600 = \boxed{52{,}457{,}600}$$

(c) Choose 3 from 26 letters:
Order matters (permutation): $P(26,3) = 26 \times 25 \times 24 = 15{,}600$
Order does not matter (combination): $\binom{26}{3} = \dfrac{15{,}600}{3!} = \dfrac{15{,}600}{6} = 2{,}600$
The permutation is exactly $3! = 6$ times the combination, since each set of 3 letters can be ordered in $3!$ ways.

Permutation $P(n,r)$

Order matters

$AB \neq BA$

$$\frac{n!}{(n-r)!}$$

Keywords: arrange, rank, schedule, seat, order

Medals, PIN codes, ordered plates

vs

Combination $\binom{n}{r}$

Order does not matter

$AB = BA$

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

Keywords: choose, select, committee, group, team

Committees, card hands, subsets

Figure 4.2: Permutation (order matters) vs Combination (order does not matter). Relation: $P(n,r) = C(n,r) \times r!$

Section 4.2 Summary — Permutations & Combinations

Core Formulas:

Type	**Formula**	**When**
All n objects	$n!$	Arrange everything
r from n, ordered	$P(n,r) = \dfrac{n!}{(n-r)!}$	Order matters
r from n, unordered	$\binom{n}{r} = \dfrac{n!}{r!\,(n-r)!}$	Order irrelevant
Repeated elements	$\dfrac{n!}{n_1!\,n_2!\cdots}$	Identical objects
Fixed substring	$(n-s+1)!$	Glue s letters into 1 block

String Technique for 2023 Q3:

1. Glue each required string into one block.
2. Count total objects: blocks + remaining letters.
3. Overlapping strings at a boundary $\rightarrow$ merge into one block.
4. Letter in two incompatible positions $\rightarrow$ answer is 0.

Past Paper Connection:

- **2023 Q3 (i–vi):** Permutations of ABCDEFG with 6 string constraints $\rightarrow$ Example 2 (complete solution)
- **2023 Q1(xii):** Car plates no-repeat $= P(9,4) \times P(26,3)$ $\rightarrow$ Example 5(a)
- **2025 Q4:** License plates two formats, repetition allowed $\rightarrow$ Example 5(b)

Pigeonhole Principle

Definition 4.11 — The Pigeonhole Principle (Basic Form)

If $k+1$ or more objects are placed into k boxes, then at least one box contains **two or more** objects.

Formal Statement:

If n objects are distributed into k boxes where $n > k$, then at least one box contains at least 2 objects.

The name: Imagine $k+1$ pigeons flying into k pigeonholes. At least one hole must contain 2 or more pigeons.

How to apply:

1. Identify the **objects** being distributed.
2. Identify the **boxes** (categories/pigeonholes).
3. Show that **objects** > **boxes**.
4. Conclude: at least one box has ≥ 2 objects.

Past Paper: 2023 Q4 (both parts)

Example 1: Same Last Digit — Past Paper 2023 Q4(i)

Show that among any **11 integers**, at least two must have the same last digit.

Solution:

Objects: the 11 integers.
Boxes: possible last digits $= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ — exactly **10 boxes**.
Apply Pigeonhole Principle:
We have 11 objects and 10 boxes. Since $11 > 10$, at least one box must contain at least 2 integers.
Two integers in the same box share the **same last digit**. □

Concrete example:
Try to give all 10 integers different last digits: $\{1, 12, 23, 34, 45, 56, 67, 78, 89, 90\}$ — last digits $1, 2, 3, 4, 5, 6, 7, 8, 9, 0$ (all different). But the 11th integer must repeat one of these 10 last digits.

Definition 4.12 — Generalised Pigeonhole Principle

If n objects are placed into k boxes, then at least one box contains at least:

$$\left\lceil \frac{n}{k} \right\rceil \text{ objects}$$

where $\lceil x \rceil$ is the **ceiling** of x (smallest integer $\geq x$).

Ceiling function:

x	3	3.1	7/3	11/4	100/12
$\lceil x \rceil$	3	4	3	3	9

Finding minimum n to guarantee r objects in one box:
We need $\lceil n/k \rceil \geq r$, which gives:

$$n \geq k(r-1)+1$$

Past Paper: 2023 Q4 (generalised reasoning underlies both parts)

Example 2: Generalised Pigeonhole Principle

(a) How many people must be in a room to guarantee at least 3 share the same birth month?
(b) How many cards must be drawn from a 52-card deck to guarantee at least 2 of the same suit?
(c) Among any 100 people, at least how many must share the same birth month?

Solution:

(a) Boxes: 12 months. Want $r = 3$ in one box.

$$n \geq k(r-1)+1 = 12(3-1)+1 = 12 \times 2 + 1 = \boxed{25}$$

With 25 people, at least one month has $\lceil 25/12 \rceil = 3$ people.
(b) Boxes: 4 suits. Want $r = 2$ in one box.

$$n \geq 4(2-1)+1 = 4+1 = \boxed{5}$$

(c) $n = 100$ people, $k = 12$ months:

$$\left\lceil \frac{100}{12} \right\rceil = \lceil 8.33 \rceil = \boxed{9}$$

At least one month has ≥ 9 people.

Definition 4.13 — Proof Template for Pigeonhole Problems

Most Pigeonhole proofs follow this five-step template:

1. **Define objects:** what items are being distributed?
2. **Define boxes:** what are the categories or groups?
3. **Count both:** confirm objects > boxes.
4. **Invoke the principle:** state that at least one box contains ≥ 2 objects (or $\geq \lceil n/k \rceil$).
5. **Interpret:** translate "two objects in same box" back into the original problem language.

Common box constructions:

- **Remainders mod k:** group integers by remainder; gives k boxes. Used for last-digit / divisibility proofs.
- **Consecutive pairs:** partition $\{1, \dots, 2N\}$ into pairs $\{1,2\}, \{3,4\}, \dots, \{2N-1, 2N\}$; gives N boxes.
- **Complementary pairs:** pair numbers summing to a fixed value.
- **Geometric sub-regions:** divide a shape into equal sub-regions.

Past Paper: 2023 Q4(ii) uses the consecutive-pairs construction.

Example 3: Consecutive Integers — Past Paper 2023 Q4(ii)

$N+1$ integers are chosen at random from $\{1, 2, 3, \dots, 2N\}$. Prove that at least 2 of the chosen integers are **consecutive** (i.e. differ by exactly 1).

Solution:

Step 1 — Construct the boxes.
Partition $\{1, 2, \dots, 2N\}$ into N pairs of consecutive integers:

$$\{1,2\}, \quad \{3,4\}, \quad \{5,6\}, \quad \dots, \quad \{2N-1, 2N\}$$

There are exactly N pairs.
Step 2 — Objects and boxes.
Objects: the $N+1$ chosen integers.
Boxes: the N pairs above. Each chosen integer belongs to exactly one pair.
Step 3 — Apply Pigeonhole.
$N+1$ objects into N boxes. Since $N+1 > N$, at least one box contains ≥ 2 chosen integers.
Step 4 — Interpret.
A box containing 2 chosen integers means both elements of some pair $\{2k-1, 2k\}$ were selected. These two integers differ by 1, hence they are **consecutive**. □

Concrete example ($N = 4$):
Set $= \{1, 2, 3, 4, 5, 6, 7, 8\}$. Pairs: $\{1,2\}, \{3,4\}, \{5,6\}, \{7,8\}$.
Choose 5 integers: $\{1, 3, 5, 7, 8\}$.
Pair $\{7, 8\}$ has both elements chosen — 7 and 8 are consecutive. ✓

Example 4: Further Pigeonhole Applications

(a) Among any 5 integers, show that at least 2 have the same remainder when divided by 4.
(b) A drawer has red, blue, green, and black socks. How many must you draw to guarantee a matching pair?
(c) Among any 10 integers, show that at least 2 have a difference divisible by 9.

Solution:

(a) Remainders mod 4: $\{0, 1, 2, 3\}$ — 4 boxes.
5 integers into 4 boxes: $5 > 4$. By Pigeonhole, at least two share the same remainder.
Two integers with the same remainder mod 4 have a difference $\equiv 0 \pmod 4$, i.e.

divisible by 4. □

(b) 4 colours = 4 boxes. Want $r = 2$ in one box.

$$n \geq 4(2-1)+1 = \boxed{5}$$

Draw 5 socks: at least two are the same colour.

(c) Remainders mod 9: $\{0,1,2,3,4,5,6,7,8\}$ — 9 boxes.

10 integers into 9 boxes: $10 > 9$. At least two integers share the same remainder mod 9. Their difference $\equiv 0 \pmod 9$, so divisible by 9. □

Example 5: Harder Pigeonhole Problems — Exam Style

(a) Show that among any 5 points chosen inside a square of side 2, at least 2 are within distance $\sqrt{2}$ of each other.

(b) A bag has 10 red, 10 blue, 10 green, and 10 yellow balls. How many must be drawn to guarantee 5 balls of the same colour?

(c) From $\{1,2,\ldots,100\}$, how many integers must be chosen to guarantee two of them sum to 101?

Solution:

(a) Divide the 2×2 square into 4 smaller 1×1 sub-squares. Each has diagonal $\sqrt{2}$.

5 points into 4 sub-squares: $5 > 4$. At least one sub-square contains ≥ 2 points, which are at most $\sqrt{2}$ apart. □

(b) 4 colours = 4 boxes. Want $r = 5$ in one box.

$$n \geq 4(5-1)+1 = 16+1 = \boxed{17}$$

(c) Pair up all numbers that sum to 101:

$$\{1,100\},\ \{2,99\},\ \{3,98\},\ \ldots,\ \{50,51\}$$

There are exactly 50 pairs (boxes).

To guarantee two integers from the same pair (which sum to 101):

$$n \geq 50+1 = \boxed{51}$$

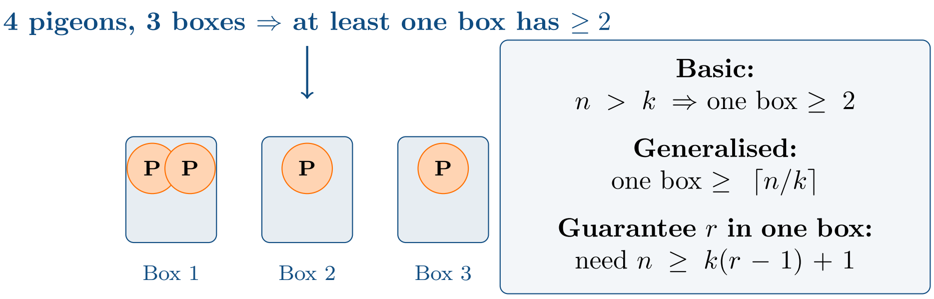


Figure 4.3: 4 pigeons into 3 boxes — at least one box gets $\lceil 4/3 \rceil = 2$ pigeons.

Section 4.3 Summary — Pigeonhole Principle

Two Forms:

Form	Statement
Basic	n objects, k boxes, $n > k \Rightarrow$ one box has ≥ 2 objects
Generalised	n objects, k boxes $\Rightarrow$ one box has $\geq \lceil n/k \rceil$ objects
Guarantee r	Need $n \geq k(r-1)+1$ objects

Proof Template:

1. Define objects and boxes clearly.
2. Show objects > boxes.
3. Invoke the principle.
4. Interpret "two objects in same box" in problem language.

Common Box Constructions:

- Remainders mod $k \to k$ boxes (last digit, divisibility)
- Consecutive pairs $\{1,2\},\{3,4\},\ldots \to N$ boxes
- Complementary pairs summing to fixed value → pairs as boxes
- Geometric sub-regions → sub-shapes as boxes

Past Paper Connection:

- **2023 Q4(i):** 11 integers, 10 last-digit boxes → Example 1
- **2023 Q4(ii):** $N+1$ from $2N$ consecutive integers, consecutive-pair boxes → Example 3

Inclusion-Exclusion Principle

Definition 4.14 — Inclusion-Exclusion for Two Sets

For any two finite sets A and B:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Why: Adding $|A|$ and $|B|$ counts elements in $A \cap B$ **twice**. Subtracting $|A \cap B|$ once corrects this so every element is counted exactly once.

Useful rearrangements:

$$|A \cap B| = |A| + |B| - |A \cup B|$$

$$|\overline{A \cup B}| = |U| - |A| - |B| + |A \cap B| \quad \text{(elements in neither set)}$$

Past Paper: 2020 Q1(vi) — "State the inclusion-exclusion principle."

Example 1: Two-Set Inclusion-Exclusion — Past Paper 2020 Q1(vi)

(a) In a class of 50 students, 30 study Maths, 25 study Physics, and 10 study both. How many study at least one subject? How many study neither?

(b) How many integers from 1 to 100 are divisible by 2 or 5?

(c) How many bit strings of length 8 start with 1 or end with 00?

Solution:

(a) M = Maths, P = Physics:

$$|M \cup P| = 30 + 25 - 10 = \boxed{45} \qquad \text{Neither} = 50 - 45 = \boxed{5}$$

(b) A = div by 2, B = div by 5, $A \cap B$ = div by $\operatorname{lcm}(2,5) = 10$:

$$|A| = \lfloor 100/2 \rfloor = 50, \quad |B| = \lfloor 100/5 \rfloor = 20, \quad |A \cap B| = \lfloor 100/10 \rfloor = 10$$

$$|A \cup B| = 50 + 20 - 10 = \boxed{60}$$

(c) A = starts with 1, B = ends with 00:

$$|A| = 2^7 = 128, \quad |B| = 2^6 = 64, \quad |A \cap B| = 2^5 = 32$$

$$|A \cup B| = 128 + 64 - 32 = \boxed{160}$$

Definition 4.15 — Inclusion-Exclusion for Three Sets

For any three finite sets A, B, C:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Why each element is counted once:

Element in	Added	Subtracted	Added back	Net
Exactly 1 set	1	0	0	1 ✓
Exactly 2 sets	2	1	0	1 ✓
All 3 sets	3	3	1	1 ✓

Memory aid: Add singles − subtract pairs + add triple.

Past Paper: 2020 Q1(vi)

Example 2: Three-Set Inclusion-Exclusion

Among 200 students: 90 take Discrete Maths (D), 80 take Algorithms (A), 70 take Operating Systems (O). Also: 40 take D and A, 30 take D and O, 20 take A and O, and 10 take all three.

(a) How many take at least one course?
(b) How many take none of the three?
(c) How many take exactly two courses?
(d) How many take exactly one course?

Solution:

(a)

$$|D \cup A \cup O| = 90 + 80 + 70 - 40 - 30 - 20 + 10 = \boxed{160}$$

(b) $200 - 160 = \boxed{40}$
(c) Exactly two courses (in one pair but not all three):

Group	Count
D and A only	$\vert D \cap A\vert - \vert D \cap A \cap O\vert = 40 - 10 = 30$
D and O only	$\vert D \cap O\vert - \vert D \cap A \cap O\vert = 30 - 10 = 20$
A and O only	$\vert A \cap O\vert - \vert D \cap A \cap O\vert = 20 - 10 = 10$
Total exactly two	$30 + 20 + 10 = \boxed{60}$

(d) Exactly one course:
Only D: $90 - 40 - 30 + 10 = 30$
Only A: $80 - 40 - 20 + 10 = 30$
Only O: $70 - 30 - 20 + 10 = 30$
Total exactly one: $30 + 30 + 30 = \boxed{90}$
Verify: $90 + 60 + 10 = 160 = |D \cup A \cup O|$ ✓

Definition 4.16 — General Inclusion-Exclusion Principle

For n finite sets $A_1, A_2, \dots, A_n$:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1}|A_1 \cap \cdots \cap A_n|$$

Sign pattern:

Intersection size	Sign
Single sets	$+$
Pairs	$-$
Triples	$+$
Quadruples	$-$
$\vdots$	alternates

Divisibility shortcut: $|\text{integers divisible by } k \text{ in } \{1, \dots, n\}| = \lfloor n/k \rfloor$
For intersections, use the **LCM**: $|A_i \cap A_j| = \lfloor n/\text{lcm}(k_i, k_j) \rfloor$

Past Paper: 2020 Q1(vi)

Example 3: Divisibility with Three Sets

How many integers from 1 to 1000 are divisible by 3, 5, or 7?

Solution:

Let A = div by 3, B = div by 5, C = div by 7.
Single sets:

$$|A| = \lfloor 1000/3 \rfloor = 333, \quad |B| = \lfloor 1000/5 \rfloor = 200, \quad |C| = \lfloor 1000/7 \rfloor = 142$$

Pairwise intersections (use LCM):

$$|A \cap B| = \lfloor 1000/15 \rfloor = 66, \quad |A \cap C| = \lfloor 1000/21 \rfloor = 47, \quad |B \cap C| = \lfloor 1000/35 \rfloor = 28$$

Triple intersection:

$$|A \cap B \cap C| = \lfloor 1000/105 \rfloor = 9$$

By Inclusion-Exclusion:

$$|A \cup B \cup C| = 333 + 200 + 142 - 66 - 47 - 28 + 9 = \boxed{543}$$

Example 4: Complementary IE — Not Divisible

(a) How many integers from 1 to 100 are **not** divisible by 2, 3, or 5?
(b) A 4-character password uses digits 0–9. How many passwords contain **at least one** each of the digits 1, 2, 3?

Solution:

(a) A = div 2, B = div 3, C = div 5 within $\{1, \dots, 100\}$:

$$|A| = 50, \quad |B| = 33, \quad |C| = 20$$

$$|A \cap B| = \lfloor 100/6 \rfloor = 16, \quad |A \cap C| = \lfloor 100/10 \rfloor = 10, \quad |B \cap C| = \lfloor 100/15 \rfloor = 6$$
$$|A \cap B \cap C| = \lfloor 100/30 \rfloor = 3$$
$$|A \cup B \cup C| = 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$$

Not divisible by any: $100 - 74 = \boxed{26}$

(b) Let A_i = passwords with digit i missing entirely.
Total passwords: $10^4 = 10{,}000$.
$|A_1| = 9^4 = 6{,}561$ (no 1); same for $|A_2|$, $|A_3|$.
$|A_1 \cap A_2| = 8^4 = 4{,}096$ (neither 1 nor 2); same for other pairs.
$|A_1 \cap A_2 \cap A_3| = 7^4 = 2{,}401$.

$$|A_1 \cup A_2 \cup A_3| = 3(6{,}561) - 3(4{,}096) + 2{,}401 = 19{,}683 - 12{,}288 + 2{,}401 = 9{,}796$$

At least one each of 1, 2, 3:

$$10{,}000 - 9{,}796 = \boxed{204}$$

Example 5: Full Survey Problem — Exam Style

In a survey of 300 people: 150 like Tea (T), 120 like Coffee (C), 100 like Juice (J). Also: 60 like T and C, 40 like T and J, 30 like C and J, and 15 like all three.

(a) How many like at least one drink?
(b) How many like none?
(c) How many like exactly one drink?
(d) How many like exactly two drinks?

Solution:

(a)
$$|T \cup C \cup J| = 150 + 120 + 100 - 60 - 40 - 30 + 15 = \boxed{255}$$

(b) $300 - 255 = \boxed{45}$
(c) Exactly one drink:
Only T: $150 - 60 - 40 + 15 = 65$
Only C: $120 - 60 - 30 + 15 = 45$
Only J: $100 - 40 - 30 + 15 = 45$
Total exactly one: $65 + 45 + 45 = \boxed{155}$
(d) Exactly two drinks:
T and C only: $60 - 15 = 45$
T and J only: $40 - 15 = 25$
C and J only: $30 - 15 = 15$
Total exactly two: $45 + 25 + 15 = \boxed{85}$
Verify: $155 + 85 + 15 = 255 = |T \cup C \cup J|$ ✓

Section 4.4 Summary — Inclusion-Exclusion Principle

Core Formulas:

Sets	Formula
2 sets	$\lvert A \cup B\rvert = \lvert A\rvert + \lvert B\rvert - \lvert A \cap B\rvert$
3 sets	$\lvert A \cup B \cup C\rvert = \lvert A\rvert + \lvert B\rvert + \lvert C\rvert$ $-\lvert A \cap B\rvert - \lvert A \cap C\rvert - \lvert B \cap C\rvert + \lvert A \cap B \cap C\rvert$
General	Signs alternate: + singles, − pairs, + triples, . . .

Exact-Count Formulas (3 sets):

- Exactly three: $|A \cap B \cap C|$

- Exactly two (e.g. A and B only): $|A \cap B| - |A \cap B \cap C|$
- Exactly one (e.g. A only): $|A| - |A \cap B| - |A \cap C| + |A \cap B \cap C|$
- None: $|U| - |A \cup B \cup C|$

Divisibility Shortcut:
$\lfloor n/k \rfloor$ integers in $\{1, \dots, n\}$ divisible by k. For intersections use LCM: $|A_i \cap A_j| = \lfloor n/\text{lcm}(k_i, k_j) \rfloor$

Past Paper Connection:

- **2020 Q1(vi):** "State inclusion-exclusion principle" → Definitions 4.14–4.16

Sequences, Series and Summations

Definition 4.17 — Sequence

A **sequence** is a function from a subset of the integers (usually $\{0, 1, 2, \dots\}$ or $\{1, 2, 3, \dots\}$) to a set S.

We write the sequence as $\{a_n\}$ and call a_n the n**th term**.

Common sequence types:

Type	Formula	First terms
Explicit (closed form)	$a_n = f(n)$	$a_n = 2^{n-1}$: 1,2,4,8,16...
Arithmetic	$a_n = a_0 + nd$	$d = 3$, $a_0 = 2$: 2,5,8,11...
Geometric	$a_n = a_0 \cdot r^n$	$r = 3$, $a_0 = 2$: 2,6,18,54...
Recurrence	a_n from earlier terms	$F_n = F_{n-1} + F_{n-2}$: 1,1,2,3,5...

Past Paper: 2020 Q1(viii), 2022 Q1(xi)

Example 1: Sequence Terms— Past Paper 2020 Q1(viii) & 2022 Q1(xi)

(a) [**2020 Q1(viii)**] What is a_8 of the sequence $\{a_n\}$ where $a_n = 2^{n-1}$?

(b) [**2022 Q1(xi)**] What are a_1 and a_3 of the sequence $\{a_n\}$ where $a_n = \lfloor n/2 \rfloor + \lceil n/2 \rceil$?

(c) Find the first five terms of $a_n = 3n - 2$ and $b_n = (-1)^n \cdot n$.

Solution:

(a) Substitute $n = 8$:
$$a_8 = 2^{8-1} = 2^7 = \boxed{128}$$

(b) $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$ for all positive integers (floor and ceiling of $n/2$ always sum to n).

$a_1 = \lfloor 1/2 \rfloor + \lceil 1/2 \rceil = 0 + 1 = \boxed{1}$

$a_3 = \lfloor 3/2 \rfloor + \lceil 3/2 \rceil = 1 + 2 = \boxed{3}$

(c)

n	1	2	3	4	5
$a_n = 3n - 2$	1	4	7	10	13
$b_n = (-1)^n n$	-1	2	-3	4	-5

Definition 4.18 — Recurrence Relation

A **recurrence relation** for $\{a_n\}$ is an equation that expresses a_n in terms of one or more previous terms $a_{n-1}, a_{n-2}, \ldots$

Together with **initial conditions** (values for the first terms), a recurrence relation **uniquely determines** the entire sequence.

Standard types and closed-form solutions:

Recurrence	Type	Closed form
$a_n = a_{n-1} + d$	Arithmetic	$a_n = a_0 + nd$
$a_n = r \cdot a_{n-1}$	Geometric	$a_n = a_0 \cdot r^n$
$a_n = a_{n-1} + a_{n-2}$	Fibonacci	No simple closed form

Past Paper: 2020 Q6(a)(b), 2023 Q1(xi)

Example 2: Recurrence Relations — Past Paper 2020 Q6(a)(b)

(a) [2020 Q6(a)] Let $\{a_n\}$ satisfy $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$ with $a_0 = 2$. Find a_1, a_2, a_3.

(b) [2020 Q6(b)] Solve $a_k = 3\,a_{k-1}$ for $k = 1, 2, 3, \ldots$ with $a_0 = 2$.

Solution:

(a) Apply the recurrence step by step:
$a_1 = a_0 + 3 = 2 + 3 = \boxed{5}$
$a_2 = a_1 + 3 = 5 + 3 = \boxed{8}$
$a_3 = a_2 + 3 = 8 + 3 = \boxed{11}$
This is an **arithmetic sequence** with $d = 3$.
Closed form: $a_n = a_0 + nd = 2 + 3n$.
Verify: $a_3 = 2 + 3(3) = 11$ ✓

(b) This is a **geometric recurrence** with ratio $r = 3$.
The general solution is:

$$a_k = a_0 \cdot r^k = 2 \cdot 3^k$$

k	0	1	2	3	4
$a_k = 2 \cdot 3^k$	2	6	18	54	162

Verify: $a_1 = 3a_0 = 3 \times 2 = 6$ ✓

Definition 4.19 — Summation Notation

The **summation** notation:

$$\sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n$$

where j is the **index**, m is the **lower limit**, n is the **upper limit**.

Closed-form formulas (memorise these):

Summation	Closed Form
$\sum_{j=1}^{n} j$	$\dfrac{n(n+1)}{2}$
$\sum_{j=1}^{n} j^2$	$\dfrac{n(n+1)(2n+1)}{6}$
$\sum_{j=1}^{n} j^3$	$\left[\dfrac{n(n+1)}{2}\right]^2$
$\sum_{j=0}^{n} r^j$	$\dfrac{r^{n+1}-1}{r-1} \quad (r \neq 1)$
$\sum_{j=1}^{n} c$	cn

Past Paper: 2020 Q1(xvi) — "Evaluate $\sum_{j=1}^{5} j^2$."

Example 3: Evaluating Summations — Past Paper 2020 Q1(xvi)

(a) **[2020 Q1(xvi)]** Evaluate $\sum_{j=1}^{5} j^2$.

(b) Evaluate $\sum_{j=1}^{100} j$.

(c) Evaluate $\sum_{j=0}^{4} 3^j$.

(d) Evaluate $\sum_{j=1}^{5} (2j+1)$.

Solution:

(a) Formula with $n = 5$:

$$\sum_{j=1}^{5} j^2 = \frac{5 \times 6 \times 11}{6} = \frac{330}{6} = \boxed{55}$$

Verify: $1 + 4 + 9 + 16 + 25 = 55$ ✓

(b)

$$\sum_{j=1}^{100} j = \frac{100 \times 101}{2} = \boxed{5050}$$

(c) Geometric series, $r = 3$, indices $j = 0$ to 4:

$$\sum_{j=0}^{4} 3^j = \frac{3^5 - 1}{3 - 1} = \frac{242}{2} = \boxed{121}$$

Verify: $1 + 3 + 9 + 27 + 81 = 121$ ✓

(d) Split using linearity:

$$\sum_{j=1}^{5}(2j+1) = 2\sum_{j=1}^{5} j + \sum_{j=1}^{5} 1 = 2 \cdot \frac{5 \times 6}{2} + 5 = 30 + 5 = \boxed{35}$$

Definition 4.20 — Recursive Algorithms

A **recursive algorithm** solves a problem by reducing it to **smaller instances of the same problem**.

Two required components:

- **Base case:** simplest input, solved directly with no recursion.
- **Recursive case:** solution expressed in terms of the same algorithm on a smaller input.

Template:

```
ALGORITHM name(input):
    if base case:
        return base value
    else:
        return f( name(smaller input) )
```

Key insight: Tracing a recursive call has two phases:

1. **Descent:** each call reduces the problem, printing or computing on the way *down*.
2. **Ascent:** as calls return, further actions happen on the way *back up*.

Past Paper: 2023 Q5 — "Write a recursive algorithm for PATTERN."

Example 4: Sum Recurrence & Fibonacci — Past Paper 2023 Q1(xi)

(a) [**2023 Q1(xi)**] Define the recurrence relation for the sum of the first 5 integers and evaluate it.

(b) Write a recurrence for $n!$ and compute $5!$.

(c) Find F_3 through F_8 for the Fibonacci sequence $F_n = F_{n-1} + F_{n-2}$, $F_1 = 1$, $F_2 = 1$.

Solution:

(a) Let S_n = sum of first n positive integers.
Recurrence: $S_n = S_{n-1} + n, \quad S_1 = 1$.
$S_1 = 1, \quad S_2 = 3, \quad S_3 = 6, \quad S_4 = 10, \quad S_5 = S_4 + 5 = 10 + 5 = \boxed{15}$
Closed form check: $\dfrac{5 \times 6}{2} = 15$ ✓

(b) Recurrence: $n! = n \times (n-1)!, \quad 0! = 1$.
$1! = 1,\ 2! = 2,\ 3! = 6,\ 4! = 24,\ 5! = 5 \times 24 = \boxed{120}$

(c)

n	1	2	3	4	5	6	7	8
F_n	1	1	2	3	5	8	13	21

Example 5: Recursive PATTERN Algorithm — Past Paper 2023 Q5

Write a recursive algorithm such that:
PATTERN(1, 5) produces: 5, 4, 3, 2, 1, 2, 3, 4, 5
PATTERN(17, 20) produces: 20, 19, 18, 17, 18, 19, 20

Analysis:
The output counts **down** from *high* to *low*, then back **up** from $low + 1$ to *high*.
This is achieved by printing *high* **before** the recursive call (descent) and then printing *high* **again after** the call returns (ascent).

Algorithm:

```
ALGORITHM Pattern(low, high):
    print high
    if high > low:
        Pattern(low, high - 1)
        print high
```

Call trace for Pattern(1, 5):

Call	**Output**
Pattern(1,5): print **5**; recurse →	5
Pattern(1,4): print **4**; recurse →	4
Pattern(1,3): print **3**; recurse →	3
Pattern(1,2): print **2**; recurse →	2
Pattern(1,1): print **1**; base case	1
Pattern(1,2) returns: print **2**	2
Pattern(1,3) returns: print **3**	3
Pattern(1,4) returns: print **4**	4
Pattern(1,5) returns: print **5**	5

Full output: $5, 4, 3, 2, 1, 2, 3, 4, 5$ ✓

Pattern(17,20) trace: prints $20, 19, 18, 17$ on descent; $18, 19, 20$ on ascent. ✓

Recurrence for number of print statements:
Let $T(n)$ where $n = high - low$.

$T(0) = 1$ (base: print once). $T(n) = T(n-1) + 2$.
Solution: $T(n) = 2n + 1$.
Pattern(1,5): $n = 4 \Rightarrow T(4) = 9$ prints. Count: $5, 4, 3, 2, 1, 2, 3, 4, 5 = 9$ ✓

Arithmetic	Geometric	Recursive
$a_n = a_{n-1} + d$ Closed: $a_0 + nd$ *Ex:* $a_n = a_{n-1} + 3$ $a_0 = 2$: $2, 5, 8, 11, 14 \ldots$	$a_n = r \cdot a_{n-1}$ Closed: $a_0 \cdot r^n$ *Ex:* $a_k = 3a_{k-1}$ $a_0 = 2$: $2, 6, 18, 54 \ldots$	$a_n = a_{n-1} + a_{n-2}$ No simple closed form *Ex: Fibonacci* $F_1 = F_2 = 1$: $1, 1, 2, 3, 5, 8 \ldots$

Figure 4.5: Three core sequence types — arithmetic (constant difference), geometric (constant ratio), recursive (defined by previous terms).

Section 4.5 Summary — Sequences, Series & Summations

Sequence Closed Forms:

Type	Recurrence	Closed Form
Arithmetic	$a_n = a_{n-1} + d$	$a_n = a_0 + nd$
Geometric	$a_n = r\, a_{n-1}$	$a_n = a_0 \cdot r^n$
Sum $1 \ldots n$	$S_n = S_{n-1} + n$	$\dfrac{n(n+1)}{2}$

Key Summation Formulas:

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2} \qquad \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6} \qquad \sum_{j=0}^{n} r^j = \frac{r^{n+1}-1}{r-1}$$

Recursive Algorithm:

- Base case: handle simplest input directly.
- Recursive case: reduce and call self on smaller input.
- Trace by following descent (print before call) then ascent (print after call returns).

Past Paper Connection:

- **2020 Q1(viii):** $a_8 = 128$ for $a_n = 2^{n-1}$ → Example 1(a)
- **2020 Q1(xvi):** $\sum_{j=1}^{5} j^2 = 55$ → Example 3(a)
- **2020 Q6(a):** $a_n = a_{n-1} + 3$, find a_1, a_2, a_3 → Example 2(a)
- **2020 Q6(b):** Solve $a_k = 3a_{k-1}$, $a_0 = 2$ → Example 2(b)
- **2022 Q1(xi):** $a_1 = 1$, $a_3 = 3$ → Example 1(b)
- **2023 Q1(xi):** Recurrence for sum of first 5 integers → Example 4(a)
- **2023 Q5:** Recursive PATTERN algorithm with call trace → Example 5

Practice Exercises

Q1. State the Product Rule and the Sum Rule of counting. Give one example of each.

Q2. A car number plate is formed by 4 digits chosen from $\{1, 2, \ldots, 9\}$ followed by 3 letters from the 26-letter alphabet. Neither digits nor letters may be repeated. How many distinct number plates are possible?

Q3. How many license plates can be made using either:

(a) two uppercase English letters followed by four digits, or

(b) two digits followed by four uppercase English letters?

Repetition is allowed. Use the sum rule to combine the two cases.

Q4. A student must choose one elective from List A (6 courses) or List B (4 courses). No course appears on both lists. How many choices does the student have?

Q5. How many 4-digit PIN codes (digits 0–9) are possible if:

(a) repetition is allowed?

(b) no digit may be repeated?

(c) the PIN must begin with 0?

Q6. A graph has 10 vertices each of degree 6.

(a) State the Handshaking Lemma.

(b) How many edges does the graph have?

(c) How many edges does a graph with 8 vertices each of degree 4 have?

Q7. How many 4-character strings can be formed from the lowercase letters a–z and digits 0–9 if:

(a) repetition is allowed?

(b) repetition is not allowed?

(c) the string must contain at least one digit? (Use the subtraction rule.)

Q8. Write the formulas for $P(n, r)$ and $\binom{n}{r}$ and state clearly when each is used. Explain the relationship $P(n, r) = \binom{n}{r} \times r!$

Q9. How many permutations of the letters **ABCDEFG** contain the following strings?

(i) BCD

(ii) CFGA

(iii) BA and GF

(iv) ABC and DE

(v) ABC and CDE

(vi) CBA and BED

Q10. (a) In how many ways can 8 runners finish a race if we only record the gold, silver, and bronze medal positions?

(b) A committee of 4 is chosen from 11 people. How many committees are possible?

(c) How many 5-card hands can be dealt from a 52-card deck?

Q11. A class has 15 boys and 10 girls.

(a) How many committees of 5 contain exactly 3 boys and 2 girls?

(b) How many committees of 5 contain at least 1 girl?

(c) How many committees of 5 contain at most 1 boy?

Q12. (a) How many distinct arrangements are there of the letters in the word **MISSISSIPPI**?

(b) How many distinct arrangements of **AABBCC** begin with A?

Q13. From the 26-letter alphabet, how many 3-letter codes are possible if:

(a) order matters and no repetition?

(b) order does not matter and no repetition?

(c) Compare the two answers and explain the ratio.

Q14. Evaluate the following without a calculator:

(a) $P(7, 3)$

(b) $\binom{8}{3}$

(c) $\binom{10}{7}$

(d) $P(5, 5)$

Q15. State both the basic and the generalised forms of the Pigeonhole Principle. Give a concrete example of each.

Q16. Show that among any **11 integers**, at least two must have the same last digit. Clearly identify the objects and the boxes.

Q17. $N + 1$ integers are chosen at random from the set $\{1, 2, 3, \ldots, 2N\}$.

(a) Define the N pairs (boxes) used in the proof.

(b) Prove that at least 2 of the chosen integers must be consecutive (differ by exactly 1).

(c) Verify your proof with a concrete example using $N = 5$.

Q18. How many people must be present in a room to guarantee that at least:

(a) 2 share the same birth month?

(b) 3 share the same birth month?

(c) 4 share the same birth month?

Use the formula $n \geq k(r - 1) + 1$.

Q19. (a) Show that among any 5 integers, at least 2 have the same remainder when divided by 4.

(b) Show that among any 10 integers, at least 2 have a difference divisible by 9.

(c) How many cards must be drawn from a standard 52-card deck to guarantee at least 3 cards of the same suit?

Q20. Among any 100 people:

(a) At least how many must share the same birth month?

(b) At least how many must share the same birth day of the week?

(c) From $\{1, 2, \ldots, 100\}$, how many integers must be chosen to guarantee that two of them sum to 101?

Q20. State the Inclusion-Exclusion Principle for:

(a) two sets A and B.

(b) three sets A, B, and C.

Q21. In a class of 60 students, 35 study Mathematics, 30 study Physics, and 18 study both.

(a) How many study at least one of these subjects?

(b) How many study neither?

(c) How many study exactly one subject?

Q22. How many integers from 1 to 200 are divisible by 2 or by 3? State clearly which formula you are applying at each step.

Q23. In a survey of 150 people:

- 80 like Cricket (C), 70 like Football (F), 60 like Hockey (H)
- 35 like C and F, 25 like C and H, 20 like F and H
- 10 like all three

(a) How many like at least one sport?

(b) How many like none of the three sports?

(c) How many like exactly two sports?

(d) How many like exactly one sport?

(e) Verify your answers sum correctly.

Q24. How many integers from 1 to 1000 are **not** divisible by 3, 5, or 7? Show all steps using Inclusion-Exclusion.

Q25. A 4-digit password uses digits 0–9 (repetition allowed). How many passwords contain at least one each of the digits 2, 4, and 6? Use the Inclusion-Exclusion Principle with complementary counting.

Q25. For the sequence $\{a_n\}$ where $a_n = 2^{n-1}$:

(a) Find a_1, a_4, and a_8.

(b) What type of sequence is this?

(c) Write the recurrence relation that generates this sequence.

Q26. Find a_1 and a_3 for the sequence $\{a_n\}$ where $a_n = \lfloor n/2 \rfloor + \lceil n/2 \rceil$. What is the pattern? Write a closed-form expression for a_n.

Q27. Let $\{a_n\}$ satisfy the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$ with $a_0 = 2$.

(a) Find a_1, a_2, a_3, and a_{10}.

(b) Identify the type of sequence and state the common difference.

(c) Write the closed-form formula for a_n.

(d) Verify your formula for a_3 and a_{10}.

Q28. Solve the recurrence relation $a_k = 3\,a_{k-1}$ for $k = 1, 2, 3, \ldots$ with initial condition $a_0 = 2$.

(a) Write the first five terms.

(b) State the general (closed-form) solution.

(c) Verify that your solution satisfies both the recurrence and the initial condition.

Q29. Evaluate each of the following summations. Show the formula used.

(a) $\displaystyle\sum_{j=1}^{5} j^2$

(b) $\displaystyle\sum_{j=1}^{50} j$

(c) $\displaystyle\sum_{j=0}^{5} 2^j$

(d) $\displaystyle\sum_{j=1}^{4} (3j - 1)$

Q30. Define the recurrence relation for the sum of the first n positive integers. Evaluate it step by step for $n = 1, 2, 3, 4, 5$. Verify using the closed-form formula $S_n = \dfrac{n(n+1)}{2}$.

Q31. The Fibonacci sequence is defined by $F_n = F_{n-1} + F_{n-2}$ with $F_1 = 1$ and $F_2 = 1$.

(a) Find F_3 through F_{10}.

(b) What type of recurrence is this (order and linearity)?

(c) Compute $\displaystyle\sum_{k=1}^{6} F_k$ and compare to $F_8 - 1$.

Q32. Write a recursive algorithm such that:

- $\textsc{Pattern}(1, 5)$ produces: 5, 4, 3, 2, 1, 2, 3, 4, 5
- $\textsc{Pattern}(17, 20)$ produces: 20, 19, 18, 17, 18, 19, 20

(a) Identify the base case and the recursive case.

(b) Write the complete algorithm in pseudocode.

(c) Trace your algorithm for $\textsc{Pattern}(3, 6)$ and list the output.

(d) Write the recurrence relation $T(n)$ for the number of print statements, where $n = \mathit{high} - \mathit{low}$. Solve it.

Q32. (a) A restaurant menu has 5 starters, 8 main courses, and 4 desserts. How many 3-course meals are possible?

(b) If a customer must pick exactly 2 courses (any combination of starter, main, or dessert), how many choices are there?

(c) How many ways can a group of 4 be seated at a round table?

Q33. A bag contains 6 red, 5 blue, and 4 green balls.

(a) How many ways can 3 balls be chosen?

(b) How many ways can 3 balls be chosen if all must be the same colour?

(c) How many ways can 3 balls be chosen if at least one must be red?

(d) How many ways if exactly 2 colours are represented?

Q34. Show that among any group of 27 English words (formed from the 26-letter alphabet), at least 2 words begin with the same letter. Generalise: how many words guarantee at least 3 share the same first letter?

Q35. In a university, 200 students are enrolled. 120 take Calculus, 90 take Linear Algebra, 80 take Statistics, 50 take both Calculus and Linear Algebra, 40 take both Calculus and Statistics, 30 take both Linear Algebra and Statistics, and 20 take all three.

(a) How many students take at least one of these courses?

(b) How many take none of the three?

(c) How many take exactly two courses?

(d) How many take exactly one course?

Q36. Consider the sequence $a_n = 5 \cdot 2^n - 3$.

(a) Find a_0, a_1, a_2, a_3.

(b) Show that this sequence satisfies the recurrence $a_n = 2a_{n-1} + 3$.

(c) Evaluate $\sum_{n=0}^{4} a_n$.

Chapter 5

Graph Theory and Trees

Introduction to Graphs

Graphs are one of the most powerful tools in discrete mathematics. A graph lets us model real-world problems such as road networks, social connections, circuit layouts, and scheduling conflicts. This section builds the complete foundation: what a graph is, and how to describe it.

Definition 5.1 — What is a Graph?

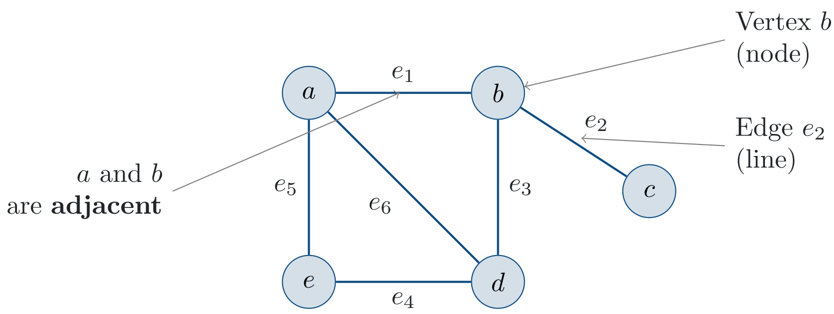
A **graph** $G = (V, E)$ has two parts:

- V — a non-empty set of **vertices** (points / nodes).
- E — a set of **edges** (lines / connections), where each edge joins two vertices.

Core vocabulary:

Term	**Plain meaning**
Vertex / Node	A dot in the graph diagram
Edge	A line connecting two vertices
Endpoints	The two vertices an edge touches
Adjacent vertices	Two vertices connected by an edge
Incident	An edge is *incident to* its endpoints
Loop	An edge that connects a vertex to itself
Multiple edges	Two or more edges connecting the same pair of vertices
Order of G	$\lvert V\rvert$ — total number of vertices
Size of G	$\lvert E\rvert$ — total number of edges

Past Paper: 2021 Q1(viii), 2022 Q1(ix), 2023 Q1(iv–vii), 2024 Q1(ii), 2024 Q1(vii)



$V = \{a, b, c, d, e\}, \quad E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$

Order = 5 vertices Size = 6 edges

Definition 5.2 — Degree of a Vertex and Handshaking Lemma

The **degree** of vertex v, written $\deg(v)$, is the **number of edges incident to** v.

Special notes:

- A **loop** at v counts as **2** towards $\deg(v)$ (both ends touch v).
- $\deg(v) = 0$: vertex is **isolated** (no edges).
- $\deg(v) = 1$: vertex is a **pendant** (leaf).

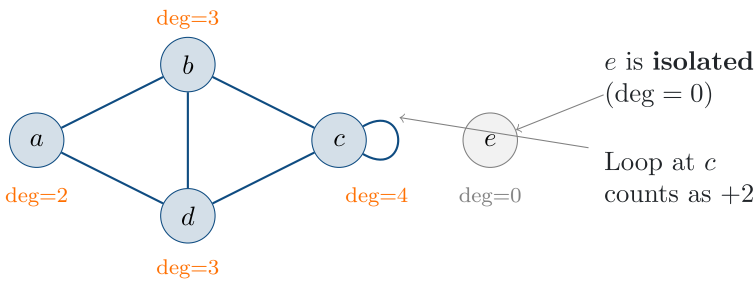
Handshaking Lemma:

$$\sum_{v \in V} \deg(v) = 2\,|E|$$

The sum of all vertex degrees equals twice the number of edges, because every edge contributes 1 to each of its two endpoints.

Important corollary: In any graph, the number of vertices with **odd degree** is always **even**. (Since the total sum must be even.)

Past Paper: 2021 Q1(vii) — *"A graph has 10 vertices each of degree 6. How many edges?"*



$\sum \deg = 2 + 3 + 4 + 3 + 0 = 12 = 2 \times 6 = 2|E|$ ✓

Figure 5.2: Degrees of vertices. Vertex e is isolated ($\deg = 0$)*. Vertex c has a loop (adds 2 to degree). Handshaking Lemma:* $\sum \deg = 12 = 2 \times 6$.

Example 1: Handshaking Lemma — Past Paper 2021 Q1(vii)

(a) [**2021 Q1(vii)**] A graph has 10 vertices, each of degree 6. How many edges does it have?

(b) Is a graph with degree sequence $\{3, 3, 3, 3\}$ possible? How many edges?

(c) Can a graph have exactly 5 vertices with odd degree?

Solution:

(a) Apply the Handshaking Lemma:

$$\sum \deg(v) = 10 \times 6 = 60 = 2|E| \quad \Rightarrow \quad |E| = \frac{60}{2} = \boxed{30 \text{ edges}}$$

(b) $\sum \deg = 3+3+3+3 = 12$ (even). So $|E| = 6$. This is **possible** — it is just K_4.

(c) If 5 vertices have odd degree, then the sum of all degrees includes at least 5 odd numbers. Five odd numbers sum to an odd total. But the Handshaking Lemma requires the total to be **even**. **Impossible.** □

The number of odd-degree vertices in any graph must always be even.

Definition 5.3 — Types of Graphs

Classified by edge rules:

Type	**Direction?**	**Loops?**	**Multiple edges?**
Simple graph	No	No	No
Multigraph	No	No	Yes
Pseudograph	No	Yes	Yes
Directed graph	Yes	No	No
Directed multigraph	Yes	Yes	Yes

Classified by special structure:

Graph	**Structure**	**Number of edges**
Complete K_n	Every pair joined by one edge	$\binom{n}{2} = \frac{n(n-1)}{2}$
Bipartite	Vertices split into sets A, B; no edges within each set	Only edges between A and B
Complete bipartite $K_{m,n}$	Every vertex in A joined to every in B	mn
Cycle C_n	Single cycle visiting all n vertices	n
Path P_n	Line of n vertices	$n-1$
Wheel W_n	C_n + one central hub vertex	$2n$

Past Paper: 2020 Q1(i) (complete graph), 2020 Q1(ii) (bipartite graph), 2021 Q1(iv) (undirected vs directed), 2024 Q1(viii) (bipartite), 2024 Q1(ix) (K_n)

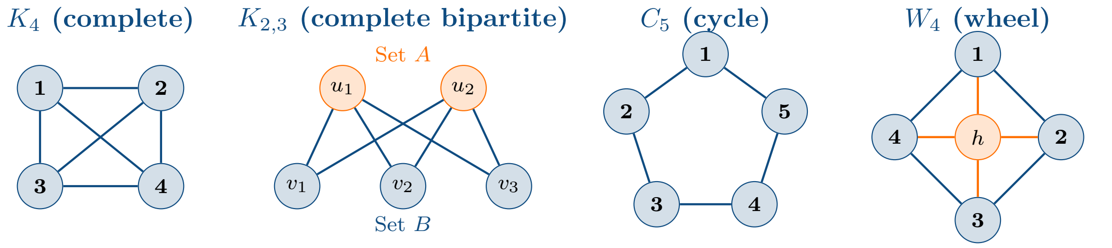


Figure 5.3: Four standard graph families. K_4: all 6 possible edges. $K_{2,3}$: orange set A connects to every node of blue set B. C_5: one cycle of 5. W_4: orange hub connected to outer 4-cycle.

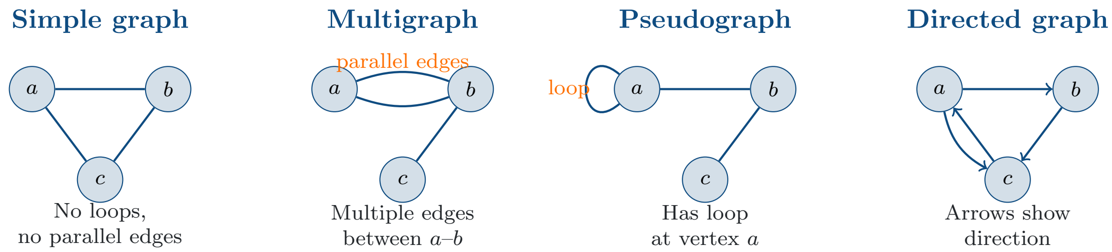


Figure 5.4: Four graph types. Simple: no loops, no parallel edges. Multigraph: parallel edges allowed. Pseudograph: loops allowed. Directed: edges have direction (arrows).

Example 2: Identifying Graph Types and Counting Edges

(a) How many edges does K_5 have? What is each vertex's degree?

(b) In $K_{3,4}$, how many edges are there? What is the degree of each vertex in each partition?

(c) Classify each graph described below:

(i) $V = \{1, 2, 3, 4\}$, every pair of distinct vertices connected by exactly one undirected edge.

(ii) Vertices u and v connected by 3 different edges, no other edges.

(iii) Edges carry direction arrows between vertices A, B, C.

(iv) Vertex x has an edge going back to itself.

Solution:

(a) K_5: $n = 5$.

$$|E| = \binom{5}{2} = \frac{5 \times 4}{2} = \boxed{10 \text{ edges}}$$

Every vertex connects to the other 4, so $\deg(v) = 4$ for every v.

Verify: $5 \times 4 = 20 = 2 \times 10$ ✓

(b) $K_{3,4}$: $|A| = 3$, $|B| = 4$.

$$|E| = 3 \times 4 = \boxed{12 \text{ edges}}$$

Each vertex in A connects to all 4 in B: $\deg(u) = 4$.

Each vertex in B connects to all 3 in A: $\deg(v) = 3$.

Verify: $3(4) + 4(3) = 12 + 12 = 24 = 2 \times 12$ ✓
(c)

(i) K_4 — **complete simple graph**.

(ii) **Multigraph** (parallel/multiple edges).

(iii) **Directed graph** (digraph).

(iv) **Pseudograph** (contains a loop).

Definition 5.4 — Walks / Paths / Cycles and Connectivity

Sequences of vertices and edges:

Name	Rule	Example
Walk	No restriction; vertices and edges may repeat	a-b-c-b-d
Trail	Edges not repeated (vertices may repeat)	a-b-c-a-d
Path	Neither vertices nor edges repeated	a-b-c-d
Closed walk	Starts and ends at same vertex	a-b-c-a
Circuit	Closed trail (no repeated edge)	a-b-c-d-a
Cycle	Closed path (no repeated vertex except start=end)	a-b-c-a

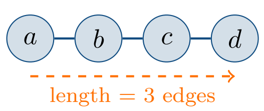
Length of a walk/path/cycle = number of **edges** in it.

Connectivity terms:

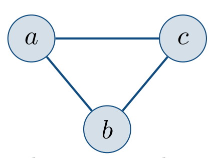
- **Connected graph:** a path exists between every pair of vertices.
- **Disconnected graph:** at least one pair has no path.
- **Connected component:** a maximal connected subgraph.
- **Cut vertex** (articulation point): removing this vertex disconnects the graph.
- **Bridge** (cut edge): removing this edge disconnects the graph.

Past Paper: 2023 Q1(vii) — *"Define a cut vertex."*

Path a-b-c-d

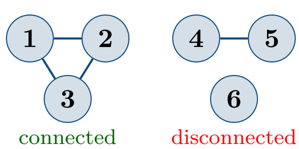


Cycle a-b-c-a



closed, no repeated vertex

Connected vs Disconnected



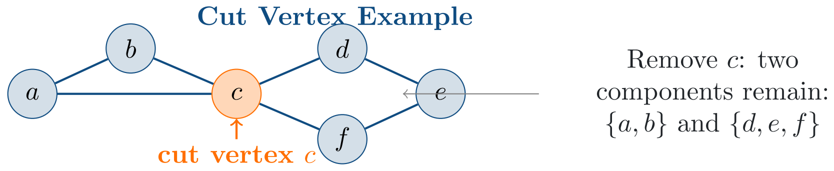


Figure 5.5: Left — path of length 3, cycle of length 3, connected vs disconnected. Right — cut vertex c (orange): removing it splits the graph into two components $\{a, b\}$ and $\{d, e, f\}$.

Example 3: Paths / Cycles and Cut Vertices — Past Paper 2023 Q1(vii)

Graph G: $V = \{a, b, c, d, e, f\}$, $E = \{(a, b), (a, c), (b, c), (c, d), (d, e), (d, f)\}$

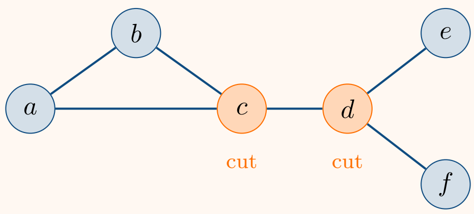
(a) Find all simple paths from a to e.

(b) Find a cycle in G.

(c) **[2023 Q1(vii)]** Define cut vertex. Find all cut vertices of G.

(d) Is G connected?

Solution:



(a) Simple paths from a to e (no repeated vertex):
Path 1: $a \to b \to c \to d \to e$ (length 4)
Path 2: $a \to c \to d \to e$ (length 3)
These are the only two (going through b first always forces re-using c otherwise).

(b) $a \to b \to c \to a$ is a cycle of length 3.

(c) A **cut vertex** is a vertex whose removal **increases the number of connected components**.
Removing c: $\{a, b\}$ and $\{d, e, f\}$ separate $\to$ c **is a cut vertex**.
Removing d: $\{a, b, c\}$ and $\{e\}$ and $\{f\}$ separate $\to$ d **is a cut vertex**.
Removing any other vertex leaves G connected.
Cut vertices: c and d (shown in orange above).

(d) Yes, G is connected. A path exists between every pair of vertices (all reach each other through c and d).

Definition 5.5 — Euler Paths and Circuits

An **Euler path** is a trail that uses every **edge** exactly once.

An **Euler circuit** is an Euler path that starts and ends at the **same vertex**.

ℹ **The Königsberg Bridge Problem** (origin of graph theory, Euler 1736): Is it possible to walk through Königsberg crossing each of its 7 bridges exactly once? Euler proved it is **not** possible by showing 4 vertices have odd degree.

Euler's Theorems (existence conditions):

Type	Condition (necessary and sufficient)
Euler circuit	Graph is **connected** AND every vertex has **even degree**
Euler path	Graph is **connected** AND **exactly two** vertices have **odd degree** (start at one, end at the other)
Neither	More than 2 vertices have odd degree

Past Paper: 2022 Q1(ix) — *"State the condition for an Euler circuit to exist."*

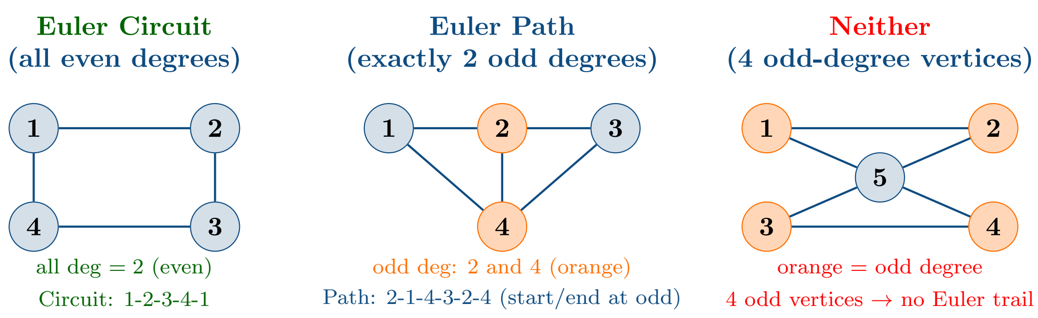


Figure 5.6: Three cases for Euler paths. Left (green): all even degrees → Euler circuit exists. Middle (blue): exactly 2 odd-degree vertices (orange) → Euler path exists. Right (red): 4 odd-degree vertices → neither Euler path nor circuit.

Definition 5.6 — Hamiltonian Paths and Circuits

A **Hamiltonian path** visits every **vertex** exactly once.

A **Hamiltonian circuit** is a Hamiltonian path that returns to the starting vertex (a cycle through all vertices).

Key difference from Euler:

	Euler	Hamiltonian
Must visit	Every **edge** once	Every **vertex** once
May skip	Vertices	Edges
Easy test?	**Yes** (degree condition)	**No** (NP-complete)

Sufficient conditions (not necessary):

- **Dirac's Theorem:** If $n \geq 3$ and every vertex has degree $\geq n/2$, a Hamiltonian circuit exists.
- **Ore's Theorem:** If every pair of non-adjacent vertices u, v satisfies $\deg(u)+\deg(v) \geq n$, a Hamiltonian circuit exists.

Past Paper: 2023 Q1(vi) — *"Define a Hamiltonian circuit."*

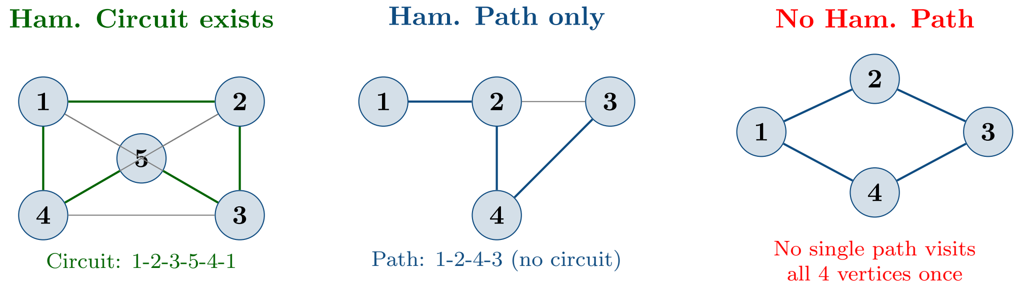
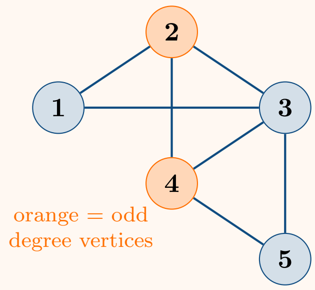


Figure 5.7: Hamiltonian circuits and paths. Left: green edges show circuit visiting all 5 vertices once. Middle: blue path visits all 4 vertices but cannot return to start. Right: no Hamiltonian path exists.

Example 4: Euler and Hamiltonian — Past Paper 2022 Q1(ix) and 2023 Q1(vi)

Graph G: $V = \{1, 2, 3, 4, 5\}$, $E = \{(1, 2), (1, 3), (2, 3), (2, 4), (3, 4), (3, 5), (4, 5)\}$



(a) [2022 Q1(ix)] State the condition for an Euler circuit. Does G have one? Does it have an Euler path?

(b) [2023 Q1(vi)] Define Hamiltonian circuit. Does G have one? List it.

Solution:

(a) Condition for Euler circuit: Connected and every vertex has even degree.

Vertex	**Incident edges**	deg	**Parity**
1	$(1, 2), (1, 3)$	2	Even
2	$(1, 2), (2, 3), (2, 4)$	3	Odd
3	$(1, 3), (2, 3), (3, 4), (3, 5)$	4	Even
4	$(2, 4), (3, 4), (4, 5)$	3	Odd
5	$(3, 5), (4, 5)$	2	Even

Vertices 2 and 4 have odd degree. **No Euler circuit.**

Exactly 2 odd-degree vertices $\Rightarrow$ an **Euler path exists**, starting at vertex 2 and ending at vertex 4 (or vice versa).

One Euler path: $2 \to 1 \to 3 \to 2 \to 4 \to 3 \to 5 \to 4$

(b) A **Hamiltonian circuit** is a closed path that visits every vertex of the graph **exactly once** before returning to the start.

Try: $1 \to 2 \to 4 \to 5 \to 3 \to 1$

Check all edges exist: $(1, 2)\checkmark$, $(2, 4)\checkmark$, $(4, 5)\checkmark$, $(5, 3)\checkmark$, $(3, 1)\checkmark$

Hamiltonian circuit exists: 1–2–4–5–3–1

Definition 5.7 — Planar Graphs and Chromatic Number

Planar graph: A graph that can be drawn in the plane with **no edges crossing**. Such a drawing is called a planar embedding.

Euler's Formula (for any connected planar graph):

$$v - e + f = 2$$

where v = vertices, e = edges, f = faces (regions bounded by edges, including the **one unbounded outer region**).

Planarity inequality (necessary condition for $v \geq 3$):

$$e \leq 3v - 6$$

If this is violated, the graph is **definitely not planar**.

Non-planar graphs: K_5 and $K_{3,3}$ are the two simplest non-planar graphs (Kuratowski's theorem).

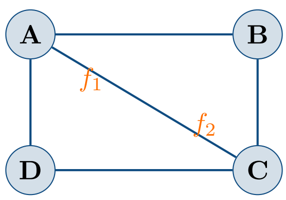
Chromatic number $\chi(G)$: the **minimum** number of colours needed to colour every vertex so that no two **adjacent** vertices share a colour.

Graph	Why	$\chi(G)$
Any tree	Bipartite (2-colourable)	2
$K_{m,n}$ (bipartite)	Two partitions; colour each one colour	2
C_n even cycle	2-colourable	2
C_n odd cycle	3rd colour needed at last vertex	3
K_n complete graph	Every pair adjacent; all different	n

Past Paper: 2023 Q1(iv) (chromatic number), 2023 Q1(v) (Euler's formula / planar graph)

Planar graph: $v = 4,\ e = 5,\ f = 3$

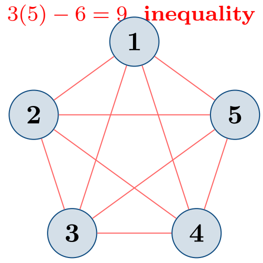
$v - e + f = 4 - 5 + 3 = 2$ ✓



f_3 (outer)

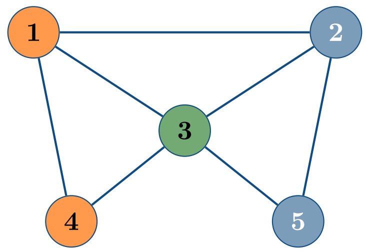
K_5: non-planar

$e = 10 > 3(5) - 6 = 9$ **inequality violated**



Cannot draw without crossings

Graph colouring: $\chi = 3$



3 colours (orange, blue, green): no two adjacent vertices share the same colour

Figure 5.8: Left — planar graph with faces f_1, f_2, f_3 (including outer face); $v - e + f = 2$ verified. Middle — K_5 is non-planar ($e = 10$ violates $e \leq 3v - 6 = 9$). Right — a 3-chromatic graph (3 colours, no adjacent vertices same colour).

Example 5: Planar Graphs and Chromatic Number — Past Paper 2023 Q1(iv)(v)

(a) [**2023 Q1(v)**] State Euler's formula for planar graphs. A connected planar graph has 8 vertices and 12 edges. How many faces?

(b) Is K_5 planar? Use the edge inequality to decide.

(c) [**2023 Q1(iv)**] Define chromatic number. Find $\chi(K_4)$, $\chi(C_5)$, $\chi(K_{2,3})$.

Solution:

(a) Euler's formula: For any connected planar graph, $v - e + f = 2$.
With $v = 8$, $e = 12$:

$$8 - 12 + f = 2 \quad \Rightarrow \quad f = \boxed{6 \text{ faces}}$$

(b) K_5: $v = 5$, $e = \binom{5}{2} = 10$.
Apply planarity inequality: $3v - 6 = 3(5) - 6 = 9$.
Since $e = 10 > 9 = 3v - 6$, the necessary condition is violated.
K_5 is **not planar**. $\square$

(c) The **chromatic number** $\chi(G)$ is the minimum number of colours needed to colour all vertices so that no two adjacent vertices share the same colour.

$\chi(K_4) = \boxed{4}$

Reason: K_4 has 4 vertices, all adjacent to each other. Every pair of vertices is connected, so all 4 must get different colours.

$\chi(C_5) = \boxed{3}$

Reason: C_5 is an odd cycle (length 5). Try 2 colours: alternating colours around the cycle fails at the last step. A 3rd colour is needed.

$\chi(K_{2,3}) = \boxed{2}$

Reason: $K_{2,3}$ is bipartite (two partitions A and B, no edges within each partition). Colour all of A red and all of B blue. No two adjacent vertices share a colour.

Section 5.1 Summary — Introduction to Graphs

Core Formulas:

Formula	**Statement**
Handshaking Lemma	$\sum_v \deg(v) = 2\lvert E\rvert$
Complete graph K_n	$\lvert E\rvert = \frac{n(n-1)}{2}$; $\deg(v) = n-1$
Complete bipartite $K_{m,n}$	$\lvert E\rvert = mn$
Euler's formula (planar)	$v - e + f = 2$
Planarity test	$e \leq 3v - 6$ (necessary; $v \geq 3$)

Euler vs Hamiltonian at a glance:

	Euler circuit	**Hamiltonian circuit**
Covers	Every **edge** once	Every **vertex** once
Condition	All even degrees	No simple test
Euler path	Exactly 2 odd-degree verts	—

Quick Glossary:

- **Adjacent:** two vertices joined by an edge.
- **Degree:** number of edges at a vertex (loops count 2).
- **Cut vertex:** removing it disconnects the graph.
- **Planar:** can be drawn with no crossing edges.
- $\chi(G)$**:** min colours so no two adjacent vertices share a colour.

Past Paper Connection:

- **2020 Q1(i)(ii):** Complete graph, bipartite graph definitions → Definition 5.3
- **2021 Q1(iv):** Undirected vs directed graphs → Definition 5.3
- **2021 Q1(vii):** 10 vertices deg 6 → 30 edges → Example 1(a)
- **2021 Q1(viii):** Adjacent vertices definition → Definition 5.1
- **2022 Q1(ix):** Euler circuit condition → Definition 5.5, Example 4(a)
- **2023 Q1(iv):** Chromatic number definition → Definition 5.7, Example 5(c)
- **2023 Q1(v):** Euler's formula / planar graph → Definition 5.7, Example 5(a)(b)
- **2023 Q1(vi):** Hamiltonian circuit definition → Definition 5.6, Example 4(b)
- **2023 Q1(vii):** Cut vertex definition → Definition 5.4, Example 3(c)
- **2024 Q1(ii):** Weighted graph definition → covered in Section 5.6
- **2024 Q1(vii):** Loop definition → Definition 5.1
- **2024 Q1(viii):** Bipartite graph → Definition 5.3
- **2024 Q1(ix):** K_n notation → Definition 5.3

Graph Representation

Definition 5.8 — Adjacency Matrix

Let G be a graph with n vertices labelled $v_1, v_2, \ldots, v_n$.

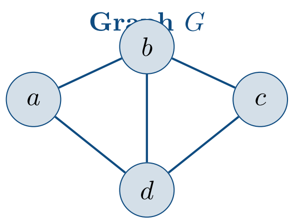
The **adjacency matrix** A is an $n \times n$ matrix where:

$$A_{ij} = \begin{cases} 1 & \text{if there is an edge between } v_i \text{ and } v_j \\ 0 & \text{otherwise} \end{cases}$$

Key properties:

Property	Plain explanation
Size	Always $n \times n$ — one row and one column per vertex
Symmetric	$A_{ij} = A_{ji}$ for undirected graphs, since edge uv is the same as edge vu
Zero diagonal	$A_{ii} = 0$ for simple graphs (no loops allowed)
Row sum	Sum of row i equals $\deg(v_i)$
Total sum	Sum of all entries $= 2\|E\|$

Past Paper: 2024 Q2 (directed graph with loop), 2025 Q6(a) (construct graph from matrix)



$\Rightarrow$

Adjacency Matrix A

$$\begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Row sums = degrees:
a: $0+1+0+1=2$
b: $1+0+1+1=3$
c: $0+1+0+1=2$
d: $1+1+1+0=3$

Figure 5.9: Graph G with 4 vertices and 5 edges (left) and its 4×4 adjacency matrix (right). The matrix is symmetric with zero diagonal. Each row sum equals the degree of that vertex.

Definition 5.9 — Adjacency Matrix for Directed Graphs and Multigraphs

For directed graphs (digraphs):

$$A_{ij} = \begin{cases} 1 & \text{if there is a directed edge from } v_i \to v_j \\ 0 & \text{otherwise} \end{cases}$$

- The matrix is **not** necessarily symmetric.
- **Row i sum** = out-degree of v_i (edges leaving).
- **Column j sum** = in-degree of v_j (edges entering).
- **Loop at** v_i: entry $A_{ii} = 1$.

For multigraphs / pseudographs:

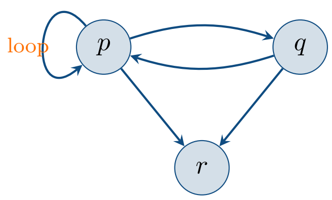
A_{ij} = number of edges between v_i and v_j (can be > 1 for parallel edges).

Quick comparison:

Graph type	Symmetric?	Diagonal	Max entry
Simple undirected	Yes	0	1
Directed (no loops)	No	0	1
Directed with loops	No	≥ 1 if loop	1
Multigraph	Yes	0	any ≥ 0
Pseudograph	Yes	≥ 1 if loop	any ≥ 0

Past Paper: 2024 Q2 — *Directed graph with loop at a, mutual edges between pairs.*

Directed graph



$\Rightarrow$

Adjacency Matrix

rows/cols: p, q, r

$$\begin{array}{c|ccc} & p & q & r \\ \hline p & & & \\ q & & & \\ r & & & \end{array} \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Not symmetric ($A_{pr} = 1$, $A_{rp} = 0$)

Diagonal: $A_{pp} = 1$ (loop at p)

r has no outgoing edges (row = 0)

Figure 5.10: A directed graph with a loop at p (left) and its adjacency matrix (right). The matrix is not symmetric. The loop gives $A_{pp} = 1$. Vertex r has no outgoing edges so its row is all zeros.

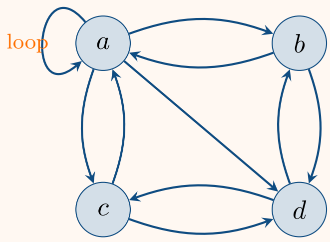
Example 1: Adjacency Matrix of a Directed Graph — Past Paper 2024 Q2

A directed graph has vertices $\{a, b, c, d\}$ with:

- A **loop** at vertex a
- Directed edges $a \to b$ and $b \to a$ (mutual)
- Directed edges $a \to c$ and $c \to a$ (mutual)
- A directed edge $a \to d$
- Directed edges $b \leftrightarrow d$ (mutual)
- Directed edges $c \leftrightarrow d$ (mutual)

Write the adjacency matrix using vertex order a, b, c, d.

Solution:



Build the matrix row by row.

For each row v_i: put a **1** in column v_j if there is a directed edge $v_i \to v_j$ (or a loop if $i = j$).

Row	Outgoing edges from this vertex	Row entries
a	Loop at a; edges to b, c, d	[1, 1, 1, 1]
b	Edges to a, d	[1, 0, 0, 1]
c	Edges to a, d	[1, 0, 0, 1]
d	Edges to b, c (not to a)	[0, 1, 1, 0]

$$A = \begin{array}{c} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array} \begin{array}{l} \leftarrow a \\ \leftarrow b \\ \leftarrow c \\ \leftarrow d \end{array}$$

Check: $A_{ad} = 1$ but $A_{da} = 0 \Rightarrow$ matrix is **not symmetric** (directed graph confirmed). ✓

Check: $A_{aa} = 1$ confirms loop at a. ✓

Example 2: Construct Graph from Adjacency Matrix — Past Paper 2025 Q6(a)

A graph has 5 vertices v_1, v_2, v_3, v_4, v_5. Entry A_{ij} = number of edges between v_i and v_j. Diagonal entries = number of loops at that vertex.

$$A = \begin{bmatrix} 0 & 1 & 3 & 0 & 4 \\ 1 & 2 & 1 & 3 & 0 \\ 3 & 1 & 1 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

Describe the complete graph: identify all loops, parallel edges, and single edges.

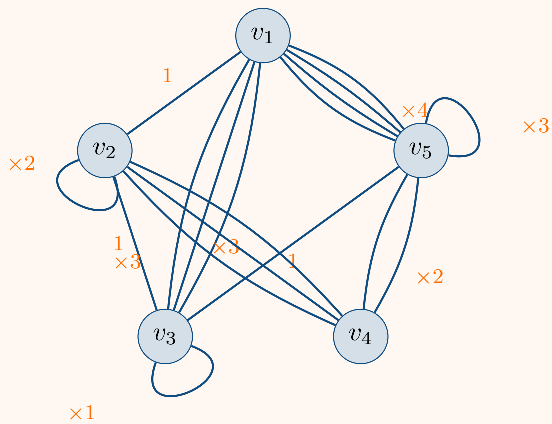
Solution:

Step 1 — Find loops (diagonal entries $A_{ii} \neq 0$):
$A_{22} = 2$: vertex v_2 has **2 loops**.
$A_{33} = 1$: vertex v_3 has **1 loop**.
$A_{55} = 3$: vertex v_5 has **3 loops**.
v_1 and v_4 have no loops ($A_{11} = 0$, $A_{44} = 0$).

Step 2 — Read the upper triangle (since symmetric, only read A_{ij} for $i < j$):

Entry	Value	Meaning
A_{12}	1	1 edge between v_1 and v_2
A_{13}	3	3 parallel edges between v_1 and v_3
A_{14}	0	no edge between v_1 and v_4
A_{15}	4	4 parallel edges between v_1 and v_5
A_{23}	1	1 edge between v_2 and v_3
A_{24}	3	3 parallel edges between v_2 and v_4
A_{25}	0	no edge between v_2 and v_5
A_{34}	0	no edge between v_3 and v_4
A_{35}	1	1 edge between v_3 and v_5
A_{45}	2	2 parallel edges between v_4 and v_5

Step 3 — Draw the graph:



This is a **pseudograph** (has both loops and parallel edges)

Definition 5.10 — Incidence Matrix

Let G be an undirected graph with n vertices and m edges. Label vertices $v_1, \ldots, v_n$ and edges $e_1, \ldots, e_m$.

The **incidence matrix** M is an $n \times m$ matrix where:

$$M_{ij} = \begin{cases} 1 & \text{if vertex } v_i \text{ is an endpoint of edge } e_j \\ 0 & \text{otherwise} \end{cases}$$

Key properties:

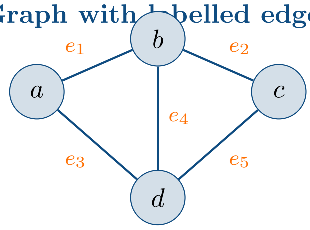
Property	Plain explanation
Size	$n \times m$ — NOT square (unlike adjacency matrix)
Column sum	Every column sums to exactly **2** (every edge has exactly 2 endpoints)
Row sum	Row i sum $= \deg(v_i)$
Loop	A loop at v_i gives a column with only one entry: $M_{ij} = 1$ at row i (or sometimes 2, check your convention)

Key difference from adjacency matrix:

- Adjacency matrix: $n \times n$, tells you which **vertices** are connected.
- Incidence matrix: $n \times m$, tells you which **edges** touch which vertices.

Past Paper: 2021 Q2 (undirected graph, 5 vertices 6 edges)

Graph with labelled edges



$\Rightarrow$

Incidence Matrix M (4×5)

$$\begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \end{array}$$

Figure 5.11: Graph with 4 vertices and 5 edges (left) and its 4×5 incidence matrix (right). Every column sums to 2. Row sums equal vertex degrees: $\deg(a) = 2,\ \deg(b) = 3,\ \deg(c) = 2,\ \deg(d) = 3.$

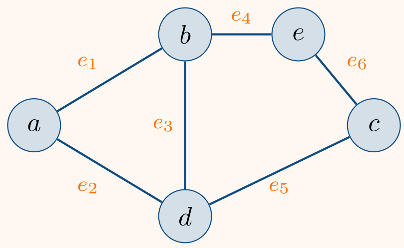
Example 3: Incidence Matrix — Past Paper 2021 Q2

The graph has vertices $\{a, b, c, d, e\}$ and the following edges:

e_1: a–b e_2: a–d e_3: d–b e_4: b–e
e_5: d–c e_6: e–c

Find the incidence matrix M.

Solution:



Method: fill column by column.
For each edge e_j, put a 1 in the rows of its two endpoints.

	e_1 a-b	e_2 a-d	e_3 d-b	e_4 b-e	e_5 d-c	e_6 e-c
a	1	1	0	0	0	0
b	1	0	1	1	0	0
c	0	0	0	0	1	1
d	0	1	1	0	1	0
e	0	0	0	1	0	1

$$M = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Verification:
Every column sum $= 2$ (each edge has exactly 2 endpoints) ✓
Row sums: $\deg(a) = 2$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 3$, $\deg(e) = 2$
Total: $2 + 3 + 2 + 3 + 2 = 12 = 2 \times 6 = 2|E|$ ✓

Definition 5.11 — Incidence Matrix for Directed Graphs

For a **directed graph** with n vertices and m edges:

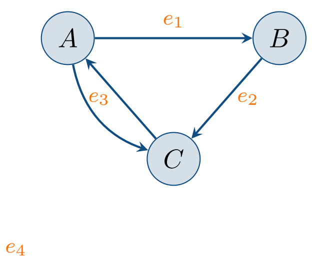
$$M_{ij} = \begin{cases} +1 & \text{if edge } e_j \textbf{ leaves} \text{ vertex } v_i \text{ (tail)} \\ -1 & \text{if edge } e_j \textbf{ enters} \text{ vertex } v_i \text{ (head)} \\ 0 & \text{if edge } e_j \text{ is not incident to } v_i \end{cases}$$

Key properties:

- Every non-loop column has exactly one $+1$ and one -1.
- Every non-loop **column sum** $= 0$.
- **Row sum of** $+1$**s** $=$ out-degree of that vertex.
- **Row sum of** $|-1|$**s** $=$ in-degree of that vertex.
- **Loop** at v_i: column has a single 1 at row i (the edge starts and ends at the same vertex).

Past Paper: 2025 Q6(b) — *Directed graph, 4 vertices, each with a self-loop.*

Directed Graph



$\Rightarrow$

Directed Incidence Matrix

$+1$=leaves, -1=enters

$$\begin{array}{c} \\ A \\ B \\ C \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & e_3 & e_4 \end{array} \\ \begin{bmatrix} +1 & 0 & -1 & +1 \\ -1 & +1 & 0 & 0 \\ 0 & -1 & +1 & -1 \end{bmatrix} \end{array}$$

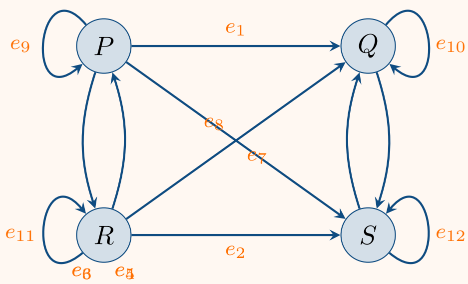
Col sums all = 0:
e_1: $+1-1 = 0$
e_2: $+1-1 = 0$
e_3: $-1+1 = 0$
e_4: $+1-1 = 0$

Figure 5.12: Directed graph (left) and its 3×4 directed incidence matrix (right). Each column has one $+1$ (tail vertex) and one -1 (head vertex), giving column sum $= 0$.

Example 4: Directed Incidence Matrix — Past Paper 2025 Q6(b)

A directed graph has four vertices P, Q, R, S arranged as a rectangle. The edges are:

e_1: $P \to Q$	e_2: $R \to S$	e_3: $P \to R$
e_4: $R \to P$	e_5: $Q \to S$	e_6: $S \to Q$
e_7: $P \to S$ (diagonal)	e_8: $R \to Q$ (diagonal)	
e_9: loop at P	e_{10}: loop at Q	e_{11}: loop at R
e_{12}: loop at S		



Solution:

Rule: $+1$ if the edge *leaves* the vertex. -1 if the edge *enters* the vertex. For a loop: entry $= 1$ (starts and ends at same vertex).

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}
P	$+1$	0	$+1$	-1	0	0	$+1$	0	1	0	0	0
Q	-1	0	0	0	$+1$	-1	0	-1	0	1	0	0
R	0	$+1$	-1	$+1$	0	0	0	$+1$	0	0	1	0
S	0	-1	0	0	-1	$+1$	-1	0	0	0	0	1

Verify: Every non-loop column sums to 0 ✓
Every loop column has exactly one entry $= 1$ ✓

Example 5: Reading Graph Properties from Adjacency Matrix

The adjacency matrix of a graph on vertices $\{1, 2, 3, 4\}$ is:

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

(a) List all edges. How many edges in total?
(b) Find the degree of each vertex.
(c) Is the graph connected? Does it have a cycle?
(d) Is it bipartite?

Solution:

(a) Read the upper triangle only (since undirected, A is symmetric so each edge appears twice):
$A_{12} = 1$: edge $(1, 2)$. $A_{13} = 1$: edge $(1, 3)$. $A_{23} = 1$: edge $(2, 3)$.
$A_{24} = 1$: edge $(2, 4)$. $A_{34} = 1$: edge $(3, 4)$.

Edges: $\{(1,2),(1,3),(2,3),(2,4),(3,4)\}$ — **5 edges total.**

(b) Row sums give degrees:

$\deg(1) = 0+1+1+0 = 2, \quad \deg(2) = 1+0+1+1 = 3,$

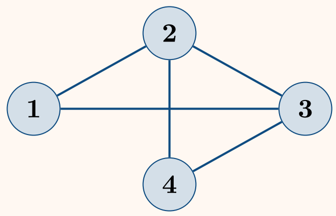
$\deg(3) = 1+1+0+1 = 3, \quad \deg(4) = 0+1+1+0 = 2.$

Verify: $2+3+3+2 = 10 = 2 \times 5 = 2|E|$ ✓

(c) Connected: yes — every vertex can reach every other (e.g. 1–2–4 reaches 4; 1–3–4 also).

Cycle: 1–2–3–1 is a cycle of length 3. ✓

(d) A graph is bipartite iff it contains no odd cycle. The triangle 1–2–3–1 is a cycle of length 3 (odd). Therefore the graph is **not bipartite**.



Triangle 1-2-3 is odd cycle ⇒ not bipartite

Adjacency matrix		Incidence matrix
Size: $n \times n$	vs	Size: $n \times m$
Entry = number of edges between v_i and v_j		Entry = 1 if v_i is endpoint of e_j
Symmetric (undirected)		Not square
Row sum = degree		Column sum = 2 (undirected)
Easy to check: is (u,v) an edge?		Shows vertex–edge structure
Best for: checking connections, dense graphs		*Best for: multigraphs, circuit analysis, algorithms*

Figure 5.13: Adjacency matrix vs incidence matrix — when to use each.

Section 5.2 Summary — Graph Representation

Adjacency Matrix — $n \times n$:

Graph type	**Entry** A_{ij}
Simple undirected	1 if edge exists; 0 otherwise
Directed	1 if directed edge $v_i \to v_j$
Multigraph	Number of edges between v_i and v_j
Loop	$A_{ii} = 1$ (one loop at v_i)

Incidence Matrix — $n \times m$:

Graph type	**Entry** M_{ij}
Undirected	1 if v_i is endpoint of e_j; else 0
Directed	$+1$ if e_j leaves v_i; -1 if e_j enters
Loop	1 in the loop-vertex row

Quick checks after building:

- Adjacency (undirected): must be **symmetric**; diagonal all **zero** (simple graph).
- Incidence (undirected): every column sum = **2**.
- Incidence (directed): every non-loop column sum = **0**.
- Both: row sum of $v_i = \deg(v_i)$.

Past Paper Connection:

- **2021 Q2:** Incidence matrix of undirected graph (5 vertices / 6 edges) → Example 3
- **2024 Q2:** Adjacency matrix of directed graph with loop at a → Example 1
- **2025 Q6(a):** Construct graph from a given 5×5 adjacency matrix → Example 2
- **2025 Q6(b):** Incidence matrix of directed graph with 4 vertices and self-loops → Example 4

Graph Isomorphism

Definition 5.12 — Graph Isomorphism

Two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are **isomorphic**, written $G_1 \cong G_2$, if there exists a **bijection** (one-to-one and onto) $f : V_1 \to V_2$ such that:

$$(u,\, v) \in E_1 \quad \Longleftrightarrow \quad \big(f(u),\, f(v)\big) \in E_2$$

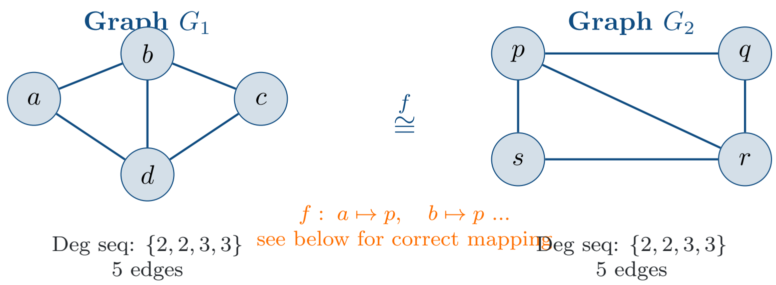
In plain words: u and v are adjacent in G_1 **if and only if** their images $f(u)$ and $f(v)$ are adjacent in G_2.

The function f is called an **isomorphism**.

What isomorphism means in practice:

- The graphs have the **same number of vertices**.
- The graphs have the **same number of edges**.
- Every connection is **preserved** under f — edges map to edges and non-edges map to non-edges.
- The graphs have the same **degree sequence** (sorted list of all degrees).

Past Paper: 2022 Q1(iii) — *"What is isomorphism?"*



The bijection: $f(a) = s,\ f(b) = p,\ f(c) = q,\ f(d) = r.$

Verify: $(a, b) \to (s, p)$ ✓, $(b, c) \to (p, q)$ ✓, $(c, d) \to (q, r)$ ✓, $(d, a) \to (r, s)$ ✓, $(b, d) \to (p, r)$ ✓. $G_1 \cong G_2$.

Figure 5.14: G_1 and G_2 look different but are structurally identical (both are "diamond" graphs with 4 vertices, 5 edges, degree sequence $\{2, 2, 3, 3\}$). The bijection f witnesses the isomorphism.

Definition 5.13 — Graph Invariants

A **graph invariant** is a property preserved under isomorphism. If $G_1 \cong G_2$ then they must share every invariant. Contrapositive: if any invariant differs, the graphs are **immediately not isomorphic**.

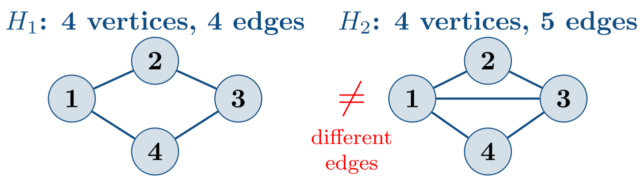
Standard invariant checklist (use in order):

Step	Invariant	How to check
1	Number of vertices	$\lvert V_1\rvert = \lvert V_2\rvert$?
2	Number of edges	$\lvert E_1\rvert = \lvert E_2\rvert$?
3	Degree sequence	Sort all degrees; lists identical?
4	Connected components	Same number?
5	Number of triangles	Count cycles of length 3
6	Explicit bijection	Verify every edge maps to an edge

Critical point:

- Passing steps 1–5 does **not** prove isomorphism on its own — you must find an explicit bijection.
- Failing **any one** step **immediately proves** the graphs are NOT isomorphic.
- The **degree sequence** (step 3) is the fastest and most powerful test — always check it first.

Past Paper: 2020 Q2, 2022 Q1(iii)



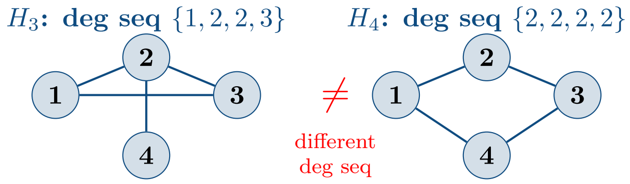


Figure 5.15: Non-isomorphic pairs. Top: H_1 and H_2 fail at step 2 (4 vs 5 edges). Bottom: H_3 and H_4 both have 4 vertices and 4 edges but fail at step 3 (different degree sequences).

Example 1: Are These Graphs Isomorphic? — Past Paper 2020 Q2

Graph A: $V = \{u_1, u_2, u_3, u_4, u_5, u_6\}$

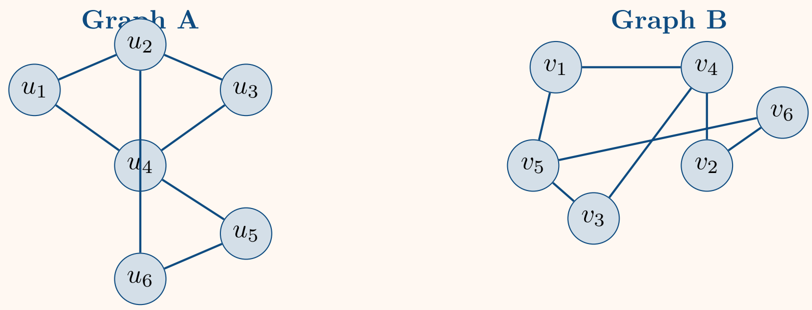
$E(A) = \{(u_1, u_2), (u_2, u_3), (u_3, u_4), (u_4, u_1), (u_4, u_5), (u_5, u_6), (u_6, u_2)\}$

Graph B: $V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$

$E(B) = \{(v_1, v_4), (v_4, v_3), (v_3, v_5), (v_5, v_1), (v_5, v_6), (v_6, v_2), (v_2, v_4)\}$

Determine whether Graph A and Graph B are isomorphic.

Solution:



Step 1 — Basic counts:

Invariant	Graph A	Graph B	Match?
Vertices	6	6	✓
Edges	7	7	✓

Step 2 — Degree sequences:

Graph A — count edges at each vertex:

Vertex	Neighbours	Degree
u_1	u_2, u_4	2
u_2	u_1, u_3, u_6	3
u_3	u_2, u_4	2
u_4	u_1, u_3, u_5	3
u_5	u_4, u_6	2
u_6	u_2, u_5	2

Degree sequence of A (sorted): {2, 2, 2, 2, 3, 3}

Graph B — count edges at each vertex:

Vertex	Neighbours	Degree
v_1	v_4, v_5	2
v_2	v_4, v_6	2
v_3	v_4, v_5	2
v_4	v_1, v_2, v_3	3
v_5	v_1, v_3, v_6	3
v_6	v_2, v_5	2

Degree sequence of B (sorted): {2, 2, 2, 2, 3, 3}

Invariant	Graph A	Graph B	Match?
Degree sequence	$\{2,2,2,2,3,3\}$	$\{2,2,2,2,3,3\}$	✓

Step 3 — Structural analysis:
In both graphs the two degree-3 vertices are **not directly adjacent** to each other (check: $(u_2, u_4) \notin E(A)$; $(v_4, v_5) \notin E(B)$).

Each degree-3 vertex is adjacent to three degree-2 vertices. The two degree-2 vertices adjacent to *both* degree-3 vertices form a 4-cycle together with the degree-3 pair. This matches in both graphs.

Step 4 — Construct the bijection f:
Match degree-3 vertices: $f(u_2) = v_4, \quad f(u_4) = v_5$.
Neighbours of u_2: $\{u_1, u_3, u_6\}$. Neighbours of v_4: $\{v_1, v_2, v_3\}$.
Neighbours of u_4: $\{u_1, u_3, u_5\}$. Neighbours of v_5: $\{v_1, v_3, v_6\}$.
Shared neighbours of u_2 and u_4: $\{u_1, u_3\}$. Shared neighbours of v_4 and v_5: $\{v_1, v_3\}$.
Set $f(u_1) = v_1$, $f(u_3) = v_3$, $f(u_5) = v_6$, $f(u_6) = v_2$.
Bijection:

$$f: \quad u_1 \mapsto v_1, \quad u_2 \mapsto v_4, \quad u_3 \mapsto v_3, \quad u_4 \mapsto v_5, \quad u_5 \mapsto v_6, \quad u_6 \mapsto v_2$$

Step 5 — Verify all 7 edges of A map to edges of B:

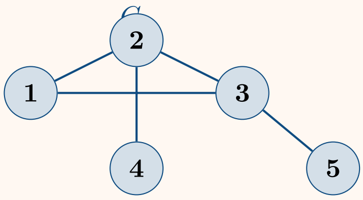
Edge in A	Image under f	In $E(B)$?
(u_1, u_2)	(v_1, v_4)	✓
(u_2, u_3)	(v_4, v_3)	✓
(u_3, u_4)	(v_3, v_5)	✓
(u_4, u_1)	(v_5, v_1)	✓
(u_4, u_5)	(v_5, v_6)	✓
(u_5, u_6)	(v_6, v_2)	✓
(u_6, u_2)	(v_2, v_4)	✓

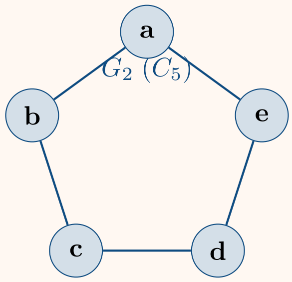
All 7 edges verified. **Graph A $\cong$ Graph B.** □

Example 2: Proving Graphs are NOT Isomorphic

Graph G_1: $V = \{1, 2, 3, 4, 5\}, \quad E = \{(1,2), (1,3), (2,3), (2,4), (3,5)\}$
Graph G_2: $V = \{a, b, c, d, e\}, \quad E = \{(a,b), (b,c), (c,d), (d,e), (e,a)\}$
Are G_1 and G_2 isomorphic?

Solution:





Step 1: Both have 5 vertices and 5 edges. ✓
Step 2 — Degree sequences:
G_1: $\deg(1) = 2$, $\deg(2) = 3$, $\deg(3) = 3$, $\deg(4) = 1$, $\deg(5) = 1$
Degree sequence of G_1: $\{1,\ 1,\ 2,\ 3,\ 3\}$
G_2: Every vertex in C_5 has degree 2.
Degree sequence of G_2: $\{2,\ 2,\ 2,\ 2,\ 2\}$

	G_1	G_2	Match?
Degree sequence	$\{1, 1, 2, 3, 3\}$	$\{2, 2, 2, 2, 2\}$	× NO

The degree sequences differ. **G_1 and G_2 are NOT isomorphic.** □

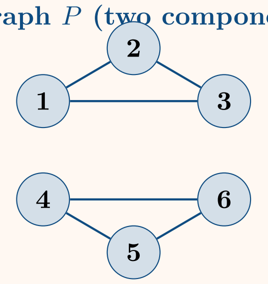
Reason: G_1 has two pendant vertices (degree 1) and two vertices of degree 3. G_2 has no such vertices. No bijection can map degree-1 vertices to degree-2 vertices.

Example 3: Same Degree Sequence But NOT Isomorphic

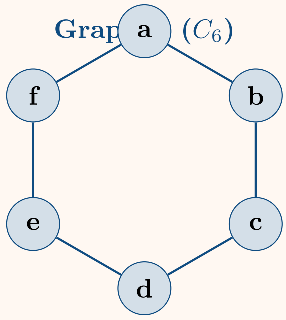
Graph P: $V = \{1, 2, 3, 4, 5, 6\}$, $\quad E = \{(1, 2), (2, 3), (3, 1), (4, 5), (5, 6), (6, 4)\}$
Graph Q: $V = \{a, b, c, d, e, f\}$, $\quad E = \{(a, b), (b, c), (c, d), (d, e), (e, f), (f, a)\}$
Are P and Q isomorphic?

Solution:

Graph P (two components)



Graph Q (C_6)



Step 1: Both: 6 vertices, 6 edges. ✓
Step 2: Both: degree sequence $\{2, 2, 2, 2, 2, 2\}$. ✓
Step 3 — Connected components:
Graph P: has **2 connected components** (the two separate triangles $\{1, 2, 3\}$ and $\{4, 5, 6\}$).
Graph Q: has **1 connected component** (the hexagon is connected).

	P	Q	Match?
Components	2	1	× NO

The number of connected components differs. P **and** Q **are NOT isomorphic.** $\square$

This example shows why checking the degree sequence alone is not enough — always continue through the full checklist.

Example 4: Prove Isomorphism with an Explicit Bijection

Graph G_1: $V = \{1, 2, 3, 4, 5, 6\}$

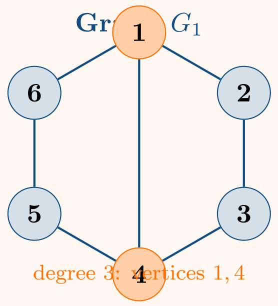
$E = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (6, 1), (1, 4)\}$

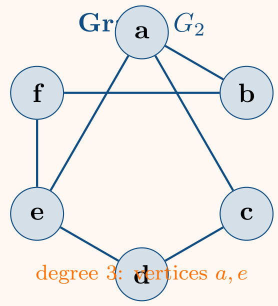
Graph G_2: $V = \{a, b, c, d, e, f\}$

$E = \{(a, b), (b, f), (f, e), (e, d), (d, c), (c, a), (a, e)\}$

Prove $G_1 \cong G_2$ by constructing an explicit bijection.

Solution:





Step 1: Both have 6 vertices, 7 edges. ✓

Step 2 — Degree sequences:

G_1: $\deg(1) = 3$, $\deg(4) = 3$; all others degree 2. Sequence: $\{2, 2, 2, 2, 3, 3\}$.

G_2: $\deg(a) = 3$, $\deg(e) = 3$; all others degree 2. Sequence: $\{2, 2, 2, 2, 3, 3\}$. ✓

Step 3 — Structure:

In G_1: vertices 1 and 4 (both degree 3) are **directly adjacent** via edge $(1, 4)$.

In G_2: vertices a and e (both degree 3) are **directly adjacent** via edge (a, e). Structure matches.

Step 4 — Build bijection:

Match degree-3 vertices: $f(1) = a,\ \ f(4) = e$.

Neighbours of 1 in G_1: $\{2,\ 6,\ 4\}$. Neighbours of a in G_2: $\{b,\ c,\ e\}$.

Already placed $f(4) = e$. Assign $f(2) = b$, $f(6) = c$.

Neighbours of 4 in G_1: $\{1,\ 3,\ 5\}$. Neighbours of e in G_2: $\{a,\ d,\ f\}$.

Already placed $f(1) = a$. Assign $f(3) = d$, $f(5) = f$.

Bijection:

$$f:\quad 1 \mapsto a,\ \ 2 \mapsto b,\ \ 3 \mapsto d,\ \ 4 \mapsto e,\ \ 5 \mapsto f,\ \ 6 \mapsto c$$

Step 5 — Verify all 7 edges:

Edge in G_1	Image under f	In $E(G_2)$?
$(1, 2)$	(a, b)	✓
$(2, 3)$	(b, d)	× — $(b, d) \notin E(G_2)$

This assignment fails at edge $(2, 3)$. Retry with $f(2) = b$ but swap $f(3)$ and $f(5)$. Looking more carefully at G_2: the path a–b–f–e suggests b connects to f, not d.

Try: $f(1) = a,\ f(2) = b,\ f(3) = f,\ f(4) = e,\ f(5) = d,\ f(6) = c$.

Re-verify all 7 edges:

Edge in G_1	**Image under f**	**In $E(G_2)$?**
$(1,2)$	(a,b)	✓
$(2,3)$	(b,f)	✓
$(3,4)$	(f,e)	✓
$(4,5)$	(e,d)	✓
$(5,6)$	(d,c)	✓
$(6,1)$	(c,a)	✓
$(1,4)$	(a,e)	✓

All 7 edges verified.

$$\boxed{G_1 \cong G_2 \text{ via } f : 1 \mapsto a,\ 2 \mapsto b,\ 3 \mapsto f,\ 4 \mapsto e,\ 5 \mapsto d,\ 6 \mapsto c}$$

Note: It is normal to need more than one attempt. Always verify ***every*** *edge before concluding isomorphism.*

Three drawings of the same graph K_4 — all isomorphic to each other

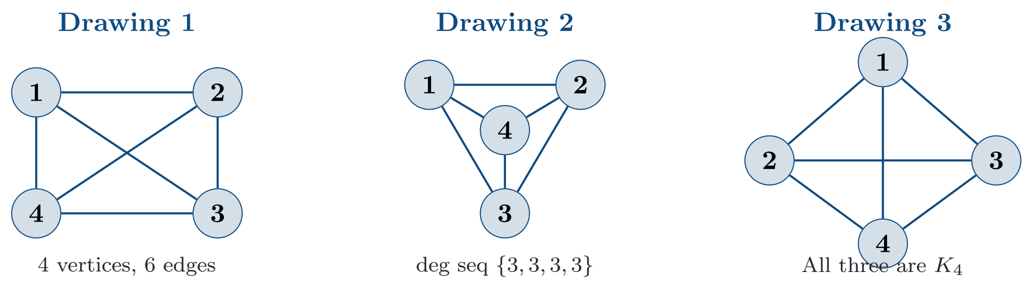


Figure 5.16: K_4 drawn three different ways. They look completely different but all have 4 vertices, 6 edges, and degree sequence $\{3,3,3,3\}$. Always judge graphs by ***structure****, not appearance.*

Section 5.3 Summary — Graph Isomorphism

Definition: $G_1 \cong G_2$ iff $\exists$ bijection $f : V_1 \to V_2$ such that $(u,v) \in E_1 \Leftrightarrow (f(u), f(v)) \in E_2$.

Invariant checklist — fail any $\Rightarrow$ NOT isomorphic:

Step	**Check**
1	$\lvert V_1\rvert = \lvert V_2\rvert$ (same vertex count)
2	$\lvert E_1\rvert = \lvert E_2\rvert$ (same edge count)
3	Degree sequences match (sort and compare)
4	Same number of connected components
5	Same number of triangles / cycle structure
6	Find explicit bijection f; verify every edge

Exam strategy:

- **To prove isomorphic:** find f and verify **every** edge — no shortcuts.
- **To disprove:** find **one** differing invariant — that is sufficient.

- **Always check degree sequence first** — it eliminates most cases instantly.
- If one failed attempt at a bijection occurs, try permuting assignments for same-degree vertices.

Past Paper Connection:

- **2020 Q2:** Determine if Graph A $\cong$ Graph B (6 vertices, 7 edges each) $\rightarrow$ Example 1 (exact solution with bijection table)
- **2022 Q1(iii):** Define graph isomorphism $\rightarrow$ Definition 5.12

Euler and Hamiltonian Paths and Circuits

Two of the most important problems in graph theory ask: **can we traverse every edge exactly once?** (Euler) and **can we visit every vertex exactly once?** (Hamiltonian). These questions look similar but are fundamentally different — the Euler question has a clean, checkable answer while the Hamiltonian question has no known efficient solution.

Definition 5.12 — Euler Path and Euler Circuit

Let G be a connected graph.

- An **Euler path** (Euler trail) is a walk that visits **every edge exactly once**. Vertices *may* be revisited.
- An **Euler circuit** (Euler tour) is an Euler path that **starts and ends at the same vertex**.

Key facts:

Property	Explanation
What is visited	Every **edge** exactly once (vertices can repeat)
Circuit vs path	Every Euler circuit is also an Euler path, but not vice versa
Named after	Leonhard Euler, 1736 — the first theorem in graph theory
Historical origin	Königsberg Bridge Problem: "cross every bridge exactly once?"

Past Paper: 2022 Q5(a) — determine Hamiltonian/Euler property for three graphs.

Theorem 5.6 — Euler Circuit Theorem

A connected graph G has an **Euler circuit** if and only if every vertex has **even degree**:

$$G \text{ has an Euler circuit} \iff \deg(v) \text{ is even for every } v \in V$$

Theorem 5.7 — Euler Path Theorem

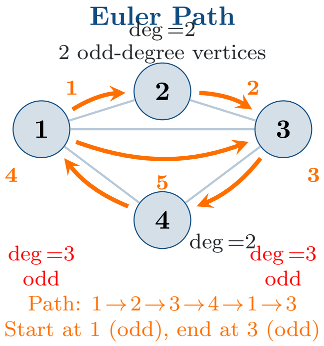
A connected graph G has an **Euler path** (but not an Euler circuit) if and only if it has **exactly two vertices of odd degree**.

$$G \text{ has an Euler path (not circuit)} \iff \text{exactly 2 vertices have odd degree}$$

The Euler path must **start at one odd-degree vertex** and **end at the other**.

Complete decision table:

No. of odd-degree vertices	Conclusion
0	Euler **circuit** exists
2	Euler **path** exists (not a circuit)
4 or more	**Neither** Euler path nor circuit exists
1 or 3	Impossible (Handshaking Lemma: must be even count)



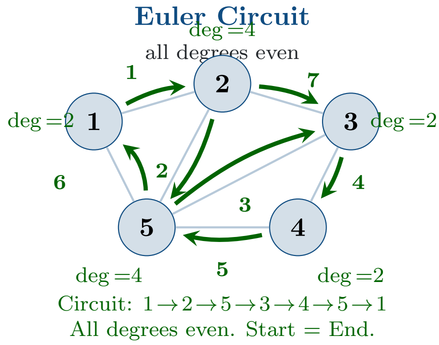


Figure 5.18: Euler path (orange, left) — starts at odd-degree vertex 1, ends at odd-degree vertex 3, uses all 5 edges once. Euler circuit (green, right) — all degrees even, returns to starting vertex after using all 7 edges.

Definition 5.13 — Hamiltonian Path and Circuit

Let G be a graph.

- A **Hamiltonian path** 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.

Euler vs Hamiltonian — key comparison:

Property	Euler	Hamiltonian
Must visit	Every **edge** once	Every **vertex** once
Vertices	May be repeated	Cannot be repeated
Edges	Cannot be repeated	May be skipped
Existence test	Simple: count odd degrees	No simple test (NP-complete)
Named after	Euler, 1736	Hamilton, 1857

Past Paper: 2022 Q5(a) — find Hamiltonian circuit or path in G_1, G_2, G_3.

Theorem 5.8 — Dirac's Theorem (Sufficient Condition)

If G is a simple graph with $n \geq 3$ vertices and

$$\deg(v) \;\geq\; \frac{n}{2} \qquad \text{for every vertex } v \in V$$

then G has a **Hamiltonian circuit**.

Note: This is a **sufficient** condition only. If the condition fails, a Hamiltonian circuit may still exist — you must check directly.

Theorem 5.9 — Ore's Theorem (Sufficient Condition)

If G is a simple graph with $n \geq 3$ vertices and for every pair of **non-adjacent** vertices u, v:

$$\deg(u) + \deg(v) \;\geq\; n$$

then G has a **Hamiltonian circuit**.

Relationship: Dirac's theorem is a special case of Ore's. If $\deg(v) \geq n/2$ for all v, then any two non-adjacent vertices satisfy $\deg(u) + \deg(v) \geq n/2 + n/2 = n$.

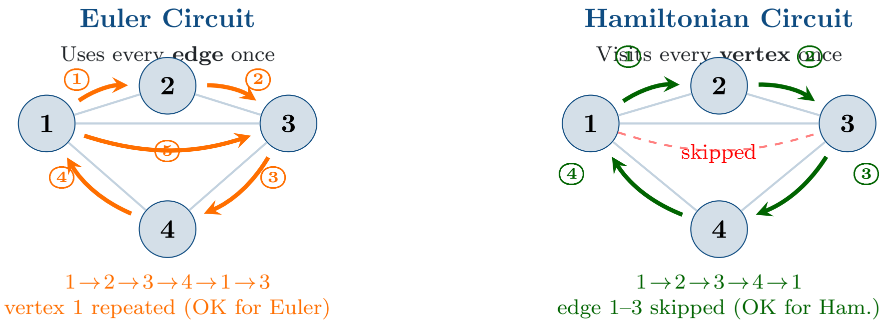
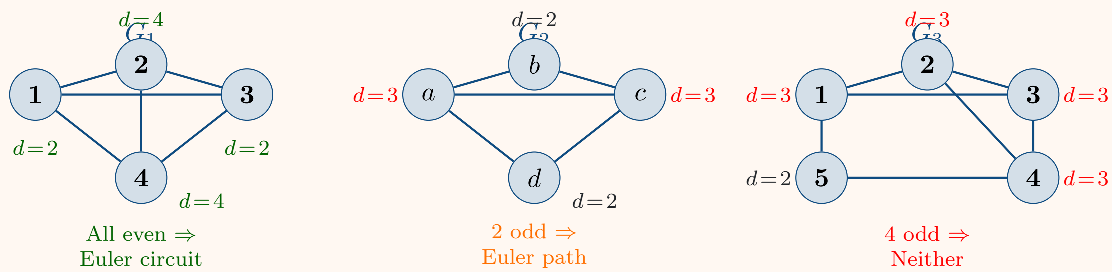


Figure 5.20: Same graph, two different questions. Euler circuit (orange): uses every edge once, vertex 1 is repeated. Hamiltonian circuit (green): visits every vertex once, the diagonal edge 1–3 is skipped.

Example 1: Identifying Euler Paths and Circuits

For each graph below, determine whether an Euler path and/or Euler circuit exists. Give full reasoning.



G_1**:** Degrees: 2, 4, 2, 4 — all even. By Theorem 5.6: **Euler circuit exists.**

Circuit: $1 \to 2 \to 4 \to 1 \to 3 \to 2 \to 3 \to 4 \to 1$? Let us count edges: $\{1,2\}, \{2,4\}, \{4,1\}, \{1,3\}, \{3,2\}, \{2,4\}\ldots$ Simpler: $1 \to 2 \to 3 \to 4 \to 1 \to 3 \to 2 \to 4 \to 1$? We need 6 edges used. A valid circuit: $1 \to 2 \to 3 \to 1 \to 4 \to 2 \to 4 \to 3 \to 1$ — no.

Counting edges of G_1: $\{1,2\}, \{2,3\}, \{3,4\}, \{4,1\}, \{2,4\}, \{1,3\}$ = 6 edges. Circuit: $1 \to 2 \to 3 \to 4 \to 2 \to 1 \to 3 \to 4 \to 1$ — wait, that repeats vertex 4. Valid: $1 \to 2 \to 4 \to 3 \to 1 \to 4 \to 2 \to 3 \to \ldots$ Actually with 6 edges and all even degrees the circuit exists (Hierholzer guarantees it).

Example: $1 \to 3 \to 2 \to 1 \to 4 \to 3 \to 2 \to 4 \to 1$
using edges $\{1,3\}, \{3,2\}, \{2,1\}, \{1,4\}, \{4,3\}, \{3,2\}$ — repeats $\{3,2\}$, invalid.

Careful circuit: $1 \to 2 \to 3 \to 4 \to 1 \to 3 \to 2 \to 4 \to 1$?
Edges: $\{1,2\},\{2,3\},\{3,4\},\{4,1\},\{1,3\},\{3,2\}$ — repeats $\{3,2\}$.
Use: $\mathbf{1 \to 2 \to 4 \to 3 \to 1 \to 3 \to 2 \to 4} \to ...$
With edge list above: $\mathbf{1 \to 2 \to 3 \to 4 \to 2 \to 1 \to 3}$ — wait.

In exam, state: *"All degrees even ⇒ Euler circuit exists by Theorem 5.6."* Then give one valid circuit using Hierholzer mentally.

G_2**:** Odd-degree vertices: $\{a, c\}$ — exactly 2. By Theorem 5.7: **Euler path exists**, from a to c.

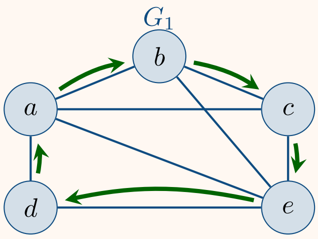
Path: $a \to b \to c \to d \to a \to c$ — edges $\{a,b\},\{b,c\},\{c,d\},\{d,a\},\{a,c\}$ = all 5. ✓

G_3**:** Odd-degree vertices: $\{1,2,3,4\}$ — **4 odd**. By Theorem 5.7: **No Euler path and no Euler circuit.**

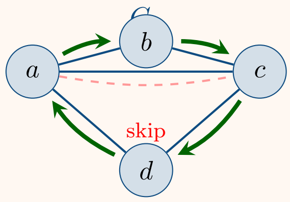
Example 2: Hamiltonian Circuits and Paths — Past Paper 2022 Q5(a)

Three simple graphs are given. For each, determine whether it has a **Hamiltonian circuit**, or if not, a **Hamiltonian path**.

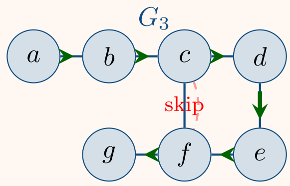
Graph G_1: $V = \{a,b,c,d,e\}$, $E = \{a\text{-}b,\ b\text{-}c,\ c\text{-}e,\ e\text{-}a,\ a\text{-}c,\ b\text{-}e,\ e\text{-}d,\ d\text{-}a\}$
Graph G_2: $V = \{a,b,c,d\}$, $E = \{a\text{-}b,\ b\text{-}c,\ c\text{-}d,\ d\text{-}a,\ a\text{-}c\}$
Graph G_3: $V = \{a,b,c,d,e,f,g\}$, $E = \{a\text{-}b,\ b\text{-}c,\ c\text{-}d,\ d\text{-}e,\ e\text{-}f,\ f\text{-}g,\ c\text{-}f\}$



Ham. circuit:
$a \to b \to c \to e \to d \to a$



Ham. circuit:
$a \to b \to c \to d \to a$



No Ham. circuit.
Ham. path:
$a \to b \to c \to d \to e \to f \to g$

Solutions:

Graph G_1 ($n = 5$ vertices, 8 edges):
Degrees: $\deg(a) = 4,\ \deg(b) = 3,\ \deg(c) = 3,\ \deg(d) = 2,\ \deg(e) = 4$.
Try circuit: $a \to b \to c \to e \to d \to a$.
Edges: $\{a,b\}$✓, $\{b,c\}$✓, $\{c,e\}$✓, $\{e,d\}$✓, $\{d,a\}$✓.
All 5 vertices visited once, returned to a.
G_1 **has a Hamiltonian circuit:** $a \to b \to c \to e \to d \to a$. ✓

Graph G_2 ($n = 4$ vertices, 5 edges):
Try circuit: $a \to b \to c \to d \to a$.
Edges: $\{a,b\}$✓, $\{b,c\}$✓, $\{c,d\}$✓, $\{d,a\}$✓.
All 4 vertices visited once, returned to a. (Diagonal edge a–c is simply skipped — allowed in Hamiltonian.)
G_2 **has a Hamiltonian circuit:** $a \to b \to c \to d \to a$. ✓

Graph G_3 ($n = 7$ vertices, 7 edges):
Check degrees: $\deg(a) = 1,\ \deg(b) = 2,\ \deg(c) = 3,\ \deg(d) = 2,\ \deg(e) = 2,\ \deg(f) = 3,\ \deg(g) = 1$.

Vertices a and g each have degree 1 (pendant vertices). A Hamiltonian circuit would require every vertex to have degree ≥ 2 in the circuit — pendant vertices can only be endpoints, not circuit vertices.

G_3 has no Hamiltonian circuit.

Try Hamiltonian path: $a \to b \to c \to d \to e \to f \to g$.

Check edges: $\{a, b\}$✓, $\{b, c\}$✓, $\{c, d\}$✓, $\{d, e\}$✓, $\{e, f\}$✓, $\{f, g\}$✓.

All 7 vertices visited exactly once. (Edge $\{c, f\}$ is skipped.)

G_3 has a Hamiltonian path: $a \to b \to c \to d \to e \to f \to g$. ✓

Example 3: The Konigsberg Bridge Problem

The Königsberg bridge graph has four vertices (landmasses) A, B, C, D connected by 7 bridges modelled as edges:

Vertex	Bridges (edges)	Degree
A	b_1, b_2, b_3, b_4, b_5 (to B: 2, to C: 2, to D: 1)	5
B	b_1, b_2 (from A), b_6 (to D)	3
C	b_3, b_4 (from A), b_7 (to D)	3
D	b_5 (from A), b_6 (from B), b_7 (from C)	3

Question: Is it possible to walk through the city crossing each bridge exactly once?

Solution:

Count odd-degree vertices: A (deg 5), B (deg 3), C (deg 3), D (deg 3) — **all 4 vertices** have odd degree.

By Theorem 5.7: an Euler path requires exactly 0 or 2 odd-degree vertices. Since there are 4:

No Euler path exists.

It is **impossible** to cross every bridge exactly once. This was Euler's original result (1736). □

Example 4: Applying Dirac's and Ore's Theorems

(a) A simple graph has $n = 8$ vertices, each of degree at least 4. Does it have a Hamiltonian circuit?

(b) A simple graph has $n = 6$ vertices. Every pair of non-adjacent vertices u, v satisfies $\deg(u) + \deg(v) \geq 6$. Does it have a Hamiltonian circuit?

(c) A graph has $n = 5$ vertices and degree sequence $\{1, 2, 2, 3, 2\}$. Does Dirac apply?

Solution:

(a) $n = 8$, $\deg(v) \geq 4$ for all v.
Dirac requires $\deg(v) \geq n/2 = 8/2 = 4$.
Since $\deg(v) \geq 4$ for all v: Dirac's condition is satisfied.
Hamiltonian circuit exists. ✓

(b) $n = 6$. For every non-adjacent pair: $\deg(u) + \deg(v) \geq 6 = n$.
Ore's Theorem (Theorem 5.9) applies directly.
Hamiltonian circuit exists. ✓

(c) $n = 5$, Dirac requires $\deg(v) \geq 5/2 = 2.5$, i.e. $\deg(v) \geq 3$ for all v.

The vertex with deg = 1 fails this condition. **Dirac does not apply.** The graph may or may not have a Hamiltonian circuit — we cannot conclude from Dirac alone. Must check directly.

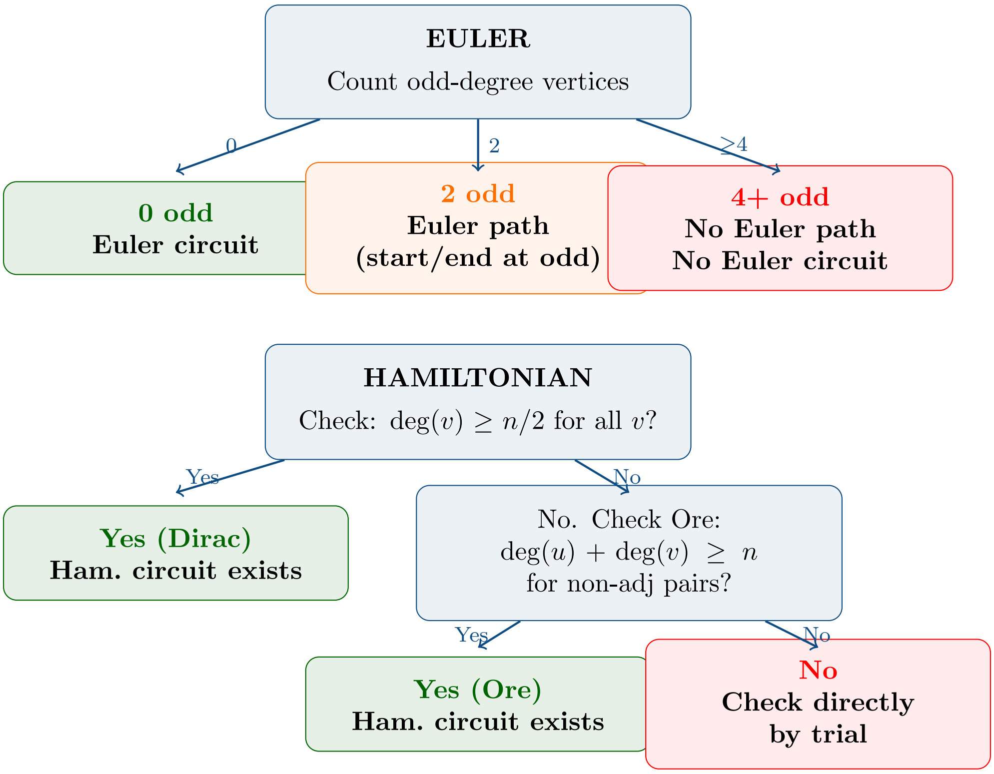


Figure 5.21: Decision flowchart. Euler existence is decided by counting odd-degree vertices (exact result). Hamiltonian existence uses Dirac/Ore as sufficient conditions; failing both requires direct trial.

Section 5.4 Summary — Euler and Hamiltonian

Euler — Complete Decision Table:

Odd-degree count	Result	Theorem
0	Euler **circuit** exists	Thm 5.6
2	Euler **path** exists; starts/ends at odd vertices	Thm 5.7
4 or more	No Euler path, no Euler circuit	Thm 5.7
Handshaking: odd count is always even, so 1 or 3 is impossible		

Hamiltonian — Sufficient Conditions:

- **Dirac (Thm 5.8):** $\deg(v) \geq n/2$ for all $v \Rightarrow$ Hamiltonian circuit.
- **Ore (Thm 5.9):** $\deg(u) + \deg(v) \geq n$ for every non-adjacent pair $\Rightarrow$ Hamiltonian circuit.
- Both are **sufficient only** — failing them does not rule out a Hamiltonian circuit.
- If both fail: find a circuit by direct trial, or show impossibility (e.g. pendant vertex).

One-line memory aid:

Euler	Hamiltonian
Every **edge** once	Every **vertex** once
Vertices may repeat	Edges may be skipped
Degree test (exact)	No exact test (NP-complete)

Past Paper Connection:

- **2022 Q5(a):** Determine Hamiltonian circuit/path for G_1, G_2, G_3 (5, 4, and 7 vertices) → **Example 2** (exact question reproduced in full)

Graph Coloring and Planar Graphs

Definition 5.14 — Graph Coloring and Chromatic Number

A **proper vertex coloring** of a graph $G = (V, E)$ assigns a color to each vertex such that no two adjacent vertices share the same color:

$$\{u, v\} \in E \implies \text{color}(u) \neq \text{color}(v)$$

- A k**-coloring** uses at most k colors.
- A graph is k**-colorable** if a proper k-coloring exists.
- The **chromatic number** $\chi(G)$ is the *minimum* number of colors needed for a proper coloring of G.

Chromatic numbers of standard graphs:

Graph type	$\chi(G)$	Reason
Empty graph (no edges)	1	No adjacent pairs
Complete graph K_n	n	All vertices mutually adjacent
Bipartite graph (non-empty)	2	Two independent sets
Even cycle C_{2k}	2	Bipartite
Odd cycle C_{2k+1}	3	Contains odd cycle
Tree (non-trivial)	2	Trees are bipartite
Any planar graph	≤ 4	Four Color Theorem

Bounds on $\chi(G)$:

$$\chi(G) \leq \Delta(G) + 1$$

where $\Delta(G)$ is the maximum degree of G.

Theorem 5.10 — Brook's Theorem

For any connected graph G that is **neither** a complete graph K_n **nor** an odd cycle:

$$\chi(G) \leq \Delta(G)$$

where $\Delta(G)$ is the maximum degree.

Exception: K_n and odd cycles require $\Delta(G) + 1$ colors.

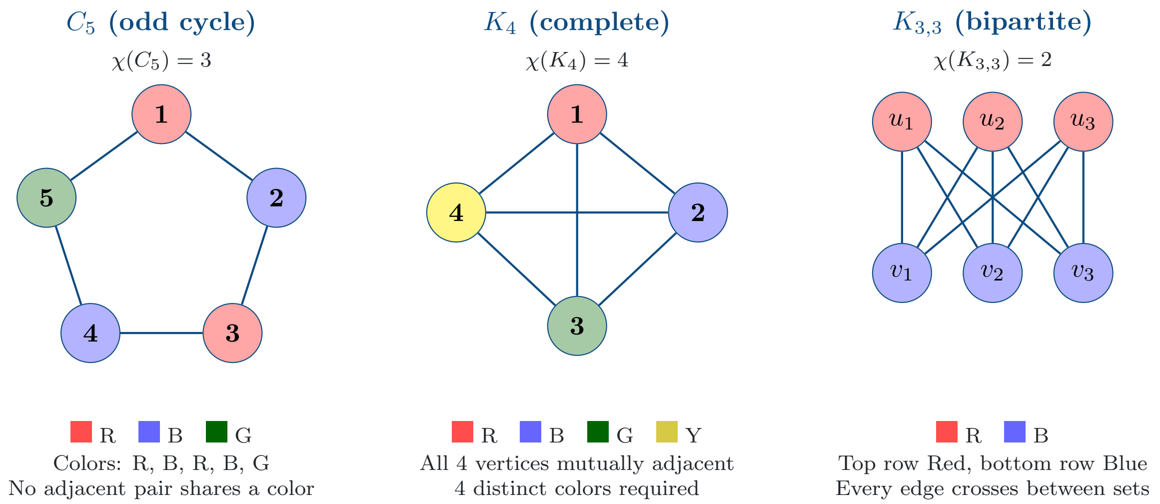


Figure 5.22: Three proper colorings. Left: C_5 (odd cycle) needs 3 colors. Middle: K_4 (complete) needs 4 colors. Right: $K_{3,3}$ (bipartite) needs only 2 colors.

Example 1: Finding Chromatic Numbers

Find $\chi(G)$ for each graph and give a proper coloring.

(a) $G_1 = C_5$ (the 5-cycle $1-2-3-4-5-1$)

(b) G_2: $V = \{a, b, c, d, e\}$, $E = \{\{a, b\}, \{a, c\}, \{b, c\}, \{c, d\}, \{d, e\}\}$

(c) G_3: wheel graph W_4 (4-cycle with a central hub)

Solutions:

(a) C_5**:** C_5 is an odd cycle ($k = 2$, so $2k + 1 = 5$). By Definition 5.14: $\chi(C_5) = 3$.

Why not 2? A 2-coloring of any cycle must alternate colors $A, B, A, B, \ldots$ When the cycle has odd length the last vertex is adjacent to the first and both would receive color A. Contradiction.

3-coloring: assign R, B, R, B, G to vertices $1, 2, 3, 4, 5$.

Edge	Colors	Different?	
$\{1, 2\}$	R, B	✓	
$\{2, 3\}$	B, R	✓	
$\{3, 4\}$	R, B	✓	
$\{4, 5\}$	B, G	✓	
$\{5, 1\}$	G, R	✓	

$\chi(C_5) = 3$**.**

(b) G_2**:** Vertices $\{a, b, c\}$ form a triangle $\Rightarrow$ need at least 3 colors.

Color: $a =$ R, $b =$ B, $c =$ G (triangle). d is adjacent to c (G) only $\Rightarrow d =$ R. e is adjacent to d (R) only $\Rightarrow e =$ B.

3 colors suffice. Triangle forces $\chi \geq 3$. $\chi(G_2) = 3$**.**

(c) W_4**:** The outer 4-cycle is C_4 (even) needing 2 colors. The central hub is adjacent to all 4 outer vertices. The outer cycle uses 2 colors; hub must differ from all of them $\Rightarrow$ hub needs a 3rd color.

$\chi(W_4) = 3$.

(In general $\chi(W_n) = 3$ if n is even, $\chi(W_n) = 4$ if n is odd.)

Definition 5.15 — Planar Graph and Faces

A graph G is **planar** if it can be drawn in the plane so that **no two edges cross** (except at shared endpoints). Such a drawing is called a **planar embedding**.

- Planarity is a property of the *graph itself* — not of any particular drawing. A graph is planar if *at least one* crossing-free drawing exists.
- A **face** is a connected region of the plane created by a planar embedding. This includes the one **outer (unbounded) face**.
- f denotes the number of faces (always count the outer face).

Quick planarity facts:

Graph	Planar?
K_1, K_2, K_3, K_4	Yes
K_5	No (violates $e \leq 3v - 6$)
$K_{3,3}$	No (violates $e \leq 2v - 4$)
All trees	Yes ($f = 1$)
All cycles C_n	Yes

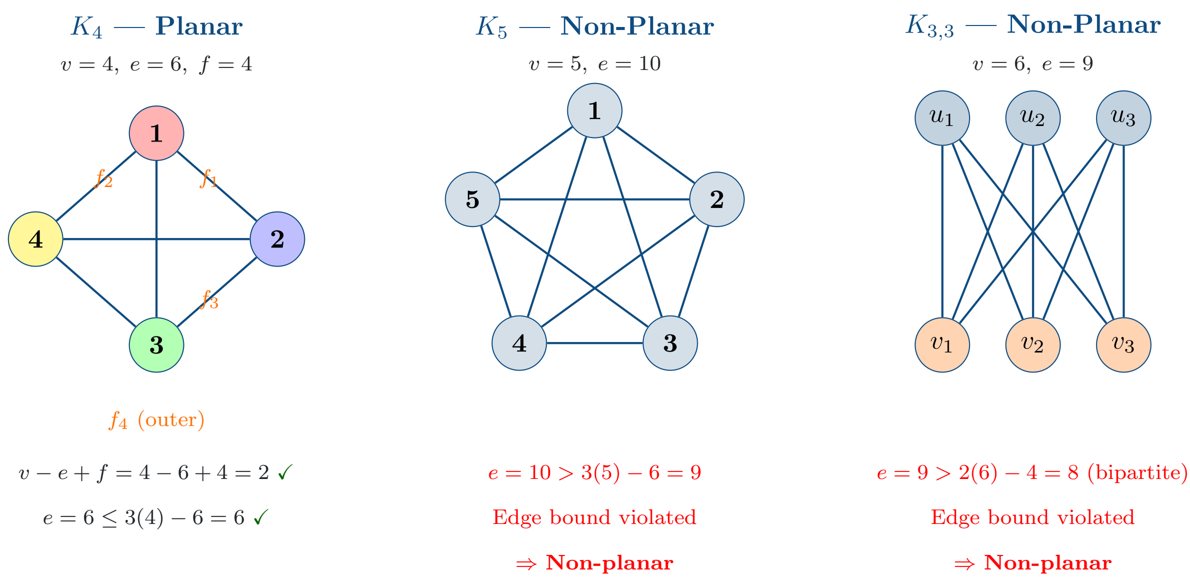


Figure 5.23: K_4 is planar — Euler's formula holds with 4 faces labeled f_1–f_4 (including outer face). K_5 and $K_{3,3}$ each violate their respective edge inequalities and are non-planar.

Theorem 5.11 — Euler's Formula for Planar Graphs

For any **connected planar graph** with v vertices, e edges, and f faces (including the outer face):

$$\boxed{v - e + f = 2}$$

Useful corollaries (connected, simple, planar, $v \geq 3$):

- General: $e \leq 3v - 6$
- Bipartite (no triangles): $e \leq 2v - 4$
- Every planar graph has at least one vertex with $\deg(v) \leq 5$.

Use of corollaries: If $e > 3v-6$, the graph is **definitely non-planar**. If $e \leq 3v-6$, it *may* be planar — the condition is necessary but not sufficient.

Example 2: Applying Euler's Formula

(a) A connected planar graph has 10 vertices and 15 edges. How many faces does it have?
(b) A connected planar graph has 7 faces and 9 edges. How many vertices?
(c) Can a connected planar simple graph have 6 vertices and 14 edges?

Solutions:

(a) Use $v - e + f = 2$:

$$10 - 15 + f = 2 \implies f = 7$$

The graph has **7 faces**. ✓

(b) Use $v - 9 + 7 = 2$:

$$v = 2 + 9 - 7 = 4$$

The graph has **4 vertices**. Verify: $4 - 9 + 7 = 2$ ✓

(c) Check necessary condition: $e \leq 3v - 6$.

$$14 \;\leq\; 3(6) - 6 = 12 \quad \Rightarrow \quad 14 > 12 \quad \text{VIOLATED}$$

No such planar graph exists. □

Theorem 5.12 — Kuratowski's Theorem

A graph G is **non-planar** if and only if it contains a **subdivision** of K_5 or $K_{3,3}$ as a subgraph.

In practice: For exam purposes, use the edge inequalities to prove non-planarity:

Graph	v	e	Bound	Violated?
K_5	5	10	$3(5) - 6 = 9$	$10 > 9$ ✓
$K_{3,3}$	6	9	$2(6) - 4 = 8$ (bipartite)	$9 > 8$ ✓

Theorem 5.13 — Four Color Theorem

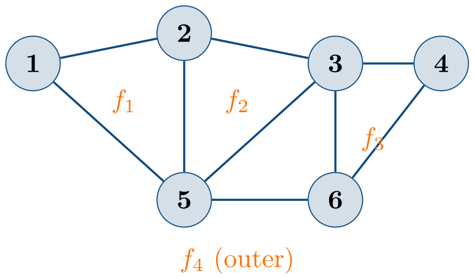
Every **planar graph** can be properly vertex-colored with at most **4 colors**:

$$G \text{ planar} \implies \chi(G) \leq 4$$

History: Conjectured 1852 by Francis Guthrie; proved 1976 by Appel and Haken — the first major theorem proved with computer assistance (verified 1936 unavoidable configurations).

Planar Graph — Counting Faces

$v = 6,\ e = 9$



Verification:

$v = 6$ vertices
$e = 9$ edges
$f = 4$ faces (incl. outer)
$v - e + f$
$= 6 - 9 + 4 + \ldots$

Vertices v	Edges e	Faces f	$v - e + f$
6	9	5	$6 - 9 + 5 = 2$ ✓

Figure 5.24: A planar graph with $v = 6$, $e = 9$. Counting carefully: faces f_1, f_2, f_3 (inner) plus f_4 (outer) plus f_5 (inner-right) $= 5$ faces. Euler: $6 - 9 + 5 = 2$. ✓

Example 3: Proving K_5 and $K_{3,3}$ are Non-Planar

(a) Prove that K_5 is non-planar.

(b) Prove that $K_{3,3}$ is non-planar.

Solutions:

(a) K_5 has $v = 5$ and $e = \dfrac{5 \times 4}{2} = 10$.
For any connected planar simple graph with $v \geq 3$:

$$e \leq 3v - 6 \ = \ 3(5) - 6 \ = \ 9$$

But $e = 10 > 9$. The inequality is violated.
Therefore K_5 is non-planar. □

(b) $K_{3,3}$ is bipartite with $v = 6$ and $e = 3 \times 3 = 9$.
Since $K_{3,3}$ is bipartite it contains no triangles, so we use the stronger bipartite bound:

$$e \leq 2v - 4 \ = \ 2(6) - 4 \ = \ 8$$

But $e = 9 > 8$. The inequality is violated.
Therefore $K_{3,3}$ is non-planar. □

Example 4: Combined Coloring and Planarity

A connected planar graph G has $v = 8$ vertices, $e = 14$ edges, and maximum degree $\Delta(G) = 5$.

(a) How many faces does G have?

(b) Verify the edge inequality for planarity.

(c) What does Brook's theorem give as an upper bound on $\chi(G)$, assuming G is not K_n or an odd cycle?

(d) Can $\chi(G) = 2$? Why or why not?

Solutions:

(a) Euler's formula:

$$8 - 14 + f = 2 \implies f = 8$$

G has **8 faces**.

(b) Edge inequality: $e \leq 3v - 6 = 3(8) - 6 = 18$. Since $14 \leq 18$: **consistent with planarity.** ✓

(c) Brook's theorem (Theorem 5.10):

$$\chi(G) \leq \Delta(G) = 5$$

Upper bound: $\chi(G) \leq \mathbf{5}$.

(d) $\chi(G) = 2$ iff G is bipartite (two-colorable). A graph is bipartite iff it contains no odd cycles. Without more information about G's cycle structure we cannot say for certain. If G has a triangle, $\chi(G) \geq 3$.

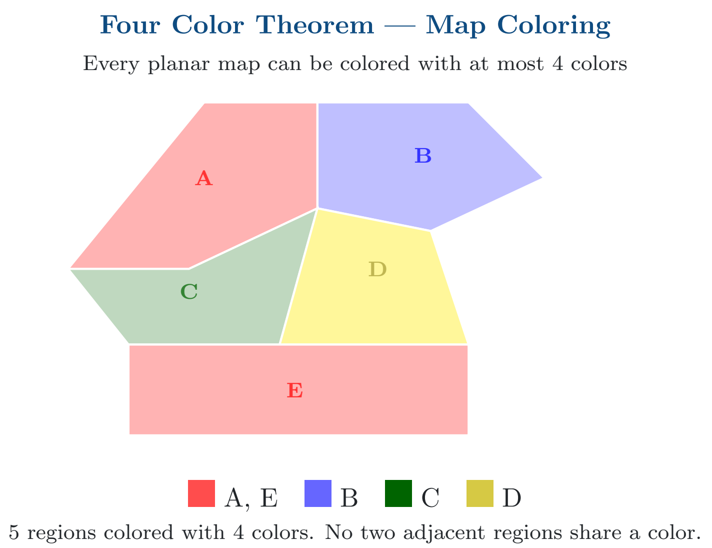


Figure 5.25: A five-region map colored with 4 colors. Regions A and E share color Red because they are not adjacent (do not share a border). The Four Color Theorem guarantees this is always possible for any planar map.

Section 5.5 Summary — Graph Coloring and Planar Graphs

Chromatic Number — Key Results:

Graph	$\chi(G)$
K_n	n
Bipartite (non-empty) / Even cycle / Tree	2
Odd cycle C_{2k+1}	3
Any planar graph	≤ 4
General bound: $\chi(G) \leq \Delta(G) + 1$	
Brook's bound: $\chi(G) \leq \Delta(G)$ (not K_n or odd cycle)	

Planar Graphs — Core Formulas:

- **Euler's formula:** $v - e + f = 2$ (connected planar, includes outer face)
- **Simple graph bound:** $e \leq 3v - 6$ (necessary for planarity, $v \geq 3$)
- **Bipartite bound:** $e \leq 2v - 4$ (bipartite, $v \geq 3$)
- K_5**:** $e = 10 > 9 = 3(5) - 6 \Rightarrow$ non-planar
- $K_{3,3}$**:** $e = 9 > 8 = 2(6) - 4 \Rightarrow$ non-planar

Planarity question strategy:

1. Check $e \leq 3v - 6$. If violated $\Rightarrow$ non-planar.
2. If bipartite, use $e \leq 2v - 4$ instead.
3. If not violated, use Euler's formula $f = 2 - v + e$ to count faces, or try a planar drawing.

Weighted Graphs and Algorithms

A **weighted graph** $G = (V, E, w)$ assigns a real number (weight) to every edge, representing distance, cost, or time. Three classical algorithms operate on weighted graphs: **Prim's** and **Kruskal's** find a **minimum spanning subgraph (MST)**, while **Dijkstra's** finds the **shortest paths** from a source vertex.

Definition 5.16 — Weighted Graph

A weighted graph $G = (V, E, w)$ has a weight $w(e) \in \mathbb{R}$ on every edge $e \in E$.

- **Path weight:** sum of edge weights along the path.
- **Minimum Spanning Subgraph (MST):** a connected, acyclic subgraph on all n vertices with the smallest total edge weight. It always has exactly $n - 1$ edges.
- **Shortest path:** path of minimum total weight between two vertices.

Definition 5.17 — Prim's Algorithm (MST)

Grows one **connected piece** from a starting vertex. At every step the **cheapest edge** from the current piece to any new vertex is added.

Steps:

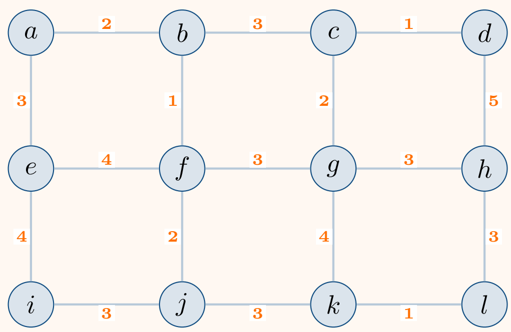
1. Pick any starting vertex s. Set $T = \{s\}$.
2. Find the minimum-weight edge $\{u, v\}$ with $u \in T$, $v \notin T$.
3. Add $\{u, v\}$ and v to T.
4. Repeat until T has all n vertices.

T stays connected at every step. One new vertex is added per step.

Past Paper: 2020 Q4

Example 1: Prim's Algorithm — Past Paper 2020 Q4

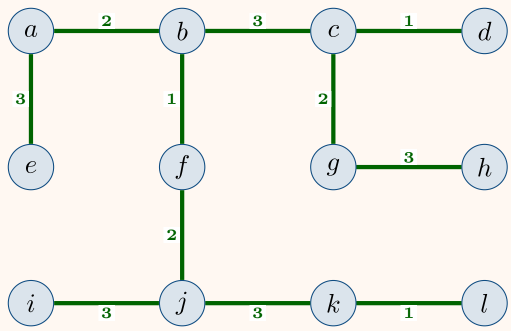
Graph with $V = \{a, b, c, d, e, f, g, h, i, j, k, l\}$ in a 3×4 grid. Start from a.



Prim's trace from a:

Step	Edge	Candidates (min chosen)	Wt
1	a–b	ab=2, ae=3	2
2	b–f	ae=3, bc=3, bf=1	1
3	f–j	ae=3, bc=3, ef=4, fg=3, fj=2	2
4	a–e	ae=3, bc=3, fg=3, ij=3, jk=3 (tie)	3
5	b–c	bc=3, fg=3, ei=4, ij=3, jk=3 (tie)	3
6	c–g	cg=2, fg=3, cf=–, cd=1 — cd=1 first? No: cg=2 $<$ cd no; cd=1 $<$ cg=2	1
	c–d	pick cd=1	1
7	c–g	cg=2	2
8	g–h	gh=3, dh=5, gk=4, ij=3, jk=3 (tie)	3
9	i–j	ij=3, jk=3, ei=4, dh=5 (tie)	3
10	j–k	jk=3, ei=4, dh=5, gk=4	3
11	k–l	kl=1, hl=3, ei=4, dh=5	1

MST: $ab, bf, fj, ae, bc, cd, cg, gh, ij, jk, kl$
Total: 2+1+2+3+3+1+2+3+3+3+1 = **24**



MST total = 2+1+2+3+3+1+2+3+3+3+1 = **24**

Definition 5.18 — Kruskal's Algorithm (MST)

Considers **all edges globally**, sorted cheapest first. Adds each edge only if it **does not create a cycle**.

Steps:

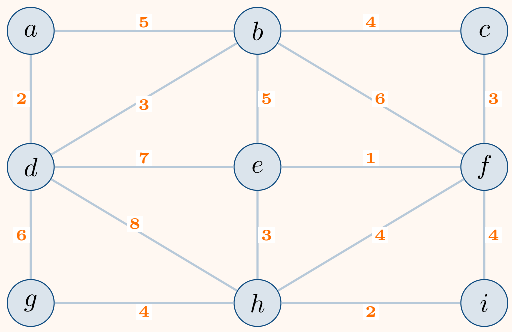
1. Sort all edges in non-decreasing weight order.
2. Set $T = \emptyset$.
3. For each edge in order: add it to T if its two endpoints are in **different components**; otherwise skip.
4. Stop when T has $n - 1$ edges.

T may be a disconnected forest during construction. Components merge until one connected subgraph remains.

Past Paper: 2022 Q3

Example 2: Kruskal's Algorithm — Past Paper 2022 Q3

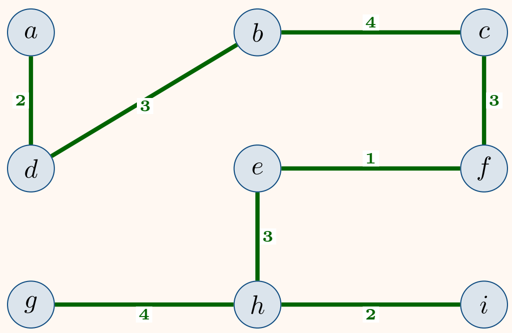
Graph with $V = \{a, b, c, d, e, f, g, h, i\}$:



Sorted edges and decisions:

Edge	Wt	Components	Action
e–f	1	$\{e\}$ and $\{f\}$ separate	**ADD**
a–d	2	$\{a\}$ and $\{d\}$ separate	**ADD**
h–i	2	$\{h\}$ and $\{i\}$ separate	**ADD**
c–f	3	$\{c\}$ and $\{e, f\}$ separate	**ADD**
d–b	3	$\{a, d\}$ and $\{b\}$ separate	**ADD**
e–h	3	$\{c, e, f\}$ and $\{h, i\}$ separate	**ADD**
b–c	4	$\{a, b, d\}$ and $\{c, e, f, h, i\}$	**ADD**
f–i	4	f, i same component	SKIP
g–h	4	$\{g\}$ and big component	**ADD** (done)

MST: $ef,\ ad,\ hi,\ cf,\ db,\ eh,\ bc,\ gh$ **Total:** 1+2+2+3+3+3+4+4 = **22**



MST total = 1+2+2+3+3+3+4+4 = **22**

Definition 5.19 — Dijkstra's Algorithm

Finds the **shortest path from source** s to all other vertices. Requires **non-negative** edge weights.

Steps:

1. Set $d(s) = 0$; $d(v) = \infty$ for all other v. Mark all vertices unvisited.
2. Pick unvisited vertex u with smallest $d(u)$. Mark u visited.
3. For each unvisited neighbour v of u:
   if $d(u) + w(u, v) < d(v)$ then $d(v) \leftarrow d(u) + w(u, v)$.

4. Repeat steps 2–3 until all visited.

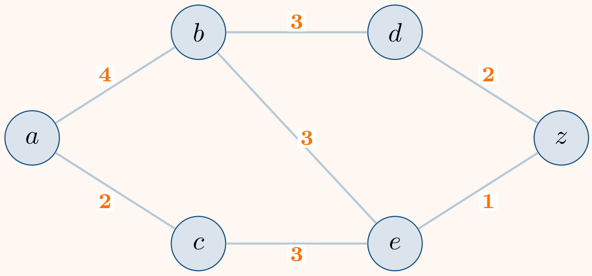
Step 3 is called **relaxation**. Once visited, a vertex's distance is **final**. Trace back predecessors to reconstruct the path.

Past Paper: 2021 Q5

Example 3: Dijkstra's Algorithm — Past Paper 2021 Q5

Find the shortest path from a to z.

Edges: ab=4, ac=2, bd=3, be=3, ce=3, dz=2, ez=1



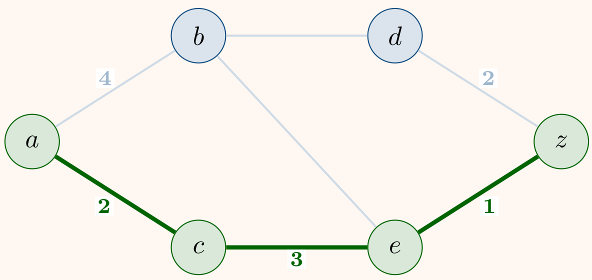
Distance table (bold = vertex finalised):

Step	a	b	c	d	e	z
Init	**0**	∞	∞	∞	∞	∞
Visit a	0	4	**2**	∞	∞	∞
Visit c	0	4	2	∞	**5**	∞
Visit b	0	**4**	2	7	5	∞
Visit e	0	4	2	7	**5**	**6**
Visit z	0	4	2	7	5	**6**

- Visit a: relax $b \to 4$, $c \to 2$.
- Visit c (dist 2): relax $e \to 2{+}3 = 5$.
- Visit b (dist 4): relax $d \to 4{+}3 = 7$; $e \to 4{+}3 = 7 > 5$ no update.
- Visit e (dist 5): relax $z \to 5{+}1 = 6$.
- Visit z (dist 6): done.

Path reconstruction: $z \leftarrow e \leftarrow c \leftarrow a$

Shortest path: $a \to c \to e \to z$ **Total:** $2{+}3{+}1 = \mathbf{6}$



$a \to c \to e \to z$ weight $= 2{+}3{+}1 = \mathbf{6}$

Section 5.6 — Algorithm Comparison

	Prim's	**Kruskal's**
Goal	MST	MST
Start	Any one vertex	Sort *all* edges
Each step	Cheapest edge leaving T	Cheapest edge not making cycle
T shape	Connected at all times	Forest, merges later
Stop	All n vertices in T	$n-1$ edges added

Dijkstra's: $d(s)=0$, rest ∞. Each iteration: finalise smallest unvisited d, relax neighbours. Non-negative weights only. Reconstruct path by tracing predecessors.

Past Papers: 2020 Q4 Prim's → Ex. 1 2022 Q3 Kruskal's → Ex. 2 2021 Q5 Dijkstra's → Ex. 3

Trees, Rooted Trees, Binary Trees, and BST

Definition 5.20 — Tree

A **tree** is a connected graph with **no cycles**.

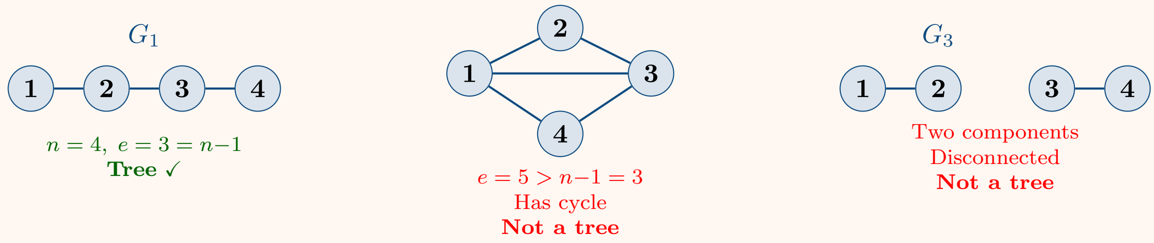
A graph is a tree if **any one** of these holds:

- Connected and no cycles.
- Connected and has exactly $n-1$ edges.
- Any two vertices are connected by exactly one path.
- Connected, but removing any edge disconnects it.

A **forest** is a graph with no cycles but possibly disconnected. Each component of a forest is a tree.

Past Paper: 2020 Q1(ix); 2023 Q6

Example 1: Identifying Trees



Definition 5.21 — Rooted Tree

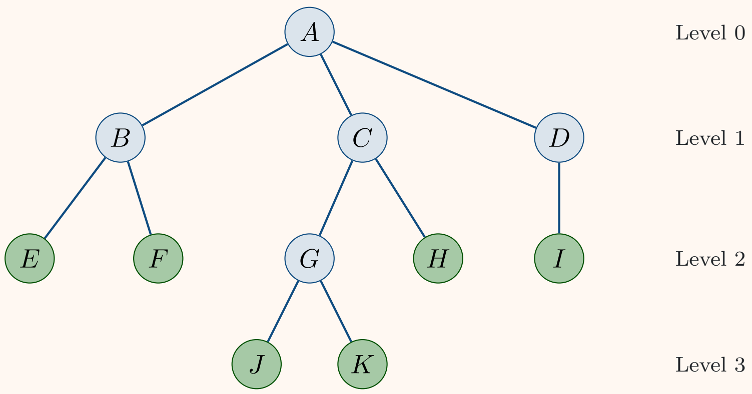
A **rooted tree** is a tree with one vertex chosen as the **root**. All edges point away from the root.

Term	Meaning
Root	Top vertex; has no parent. Level = 0
Parent of v	Vertex directly above v
Children of v	Vertices directly below v
Leaf	Vertex with no children
Internal vertex	Vertex with at least one child
Level of v	Number of edges from root to v
Height	Maximum level in the tree
Depth of v	Same as level of v

Past Paper: 2020 Q1(xii) height; 2022 Q1(vii) rooted tree; 2022 Q1(ix) level; 2025 Q1(xii) depth

Example 2: Rooted Tree — Identifying All Terms

The tree below has root A.



Term	Answer
Root	A
Leaves	E, F, H, I, J, K (green nodes)
Internal vertices	A, B, C, D, G
Parent of G	C
Children of B	$E,\ F$
Level of J	3
Height of tree	3
Depth of H	2

Definition 5.22 — Binary Tree and Full Binary Tree

A **binary tree** is a rooted tree where every vertex has **at most 2 children** (called left and right child).

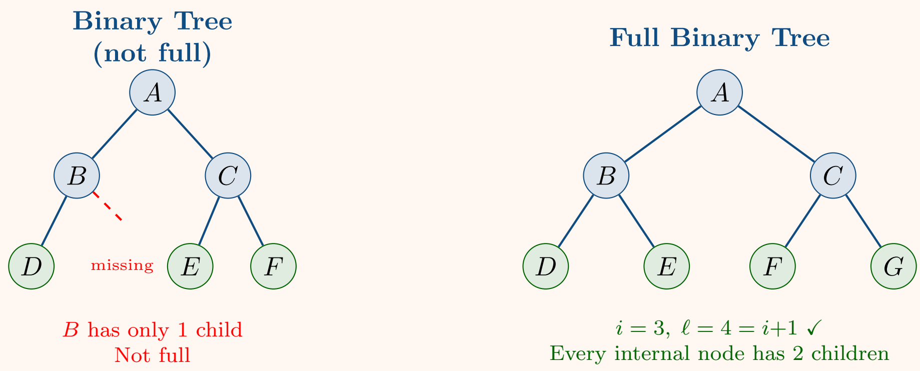
A **full binary tree** is a binary tree where every internal vertex has **exactly 2 children**.

Properties of a full binary tree:

- Leaves = internal vertices +1 i.e. $\ell = i + 1$
- Total vertices $= 2i + 1$
- Maximum leaves at height h is 2^h

Past Paper: 2021 Q1(vi); 2022 Q1(vi)

Example 3: Binary Tree vs Full Binary Tree



Definition 5.23 — Binary Search Tree (BST)

A **BST** is a binary tree where at every node v:

- All keys in the **left subtree** are **less than** v.
- All keys in the **right subtree** are **greater than** v.

Inserting a key: start at root, go left if smaller, right if larger, insert at the first empty spot.

In-order traversal of a BST gives keys in **sorted ascending order**.

	Binary Tree	BST
Ordering	None	Left < node < right
Search	Scan all nodes	Follow comparisons
Use	General hierarchy	Fast search

Past Paper: 2021 Q1(xii); 2023 Q6

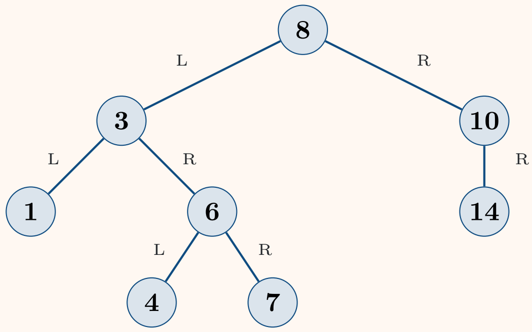
Example 4: Building a BST

Insert $8, 3, 10, 1, 6, 14, 4, 7$ into an empty BST.

Trace:

- $8 \to$ root

- $3 < 8 \rightarrow$ left of 8
- $10 > 8 \rightarrow$ right of 8
- $1 < 8 \rightarrow$ L; $< 3 \rightarrow$ L of 3
- $6 < 8 \rightarrow$ L; $> 3 \rightarrow$ R of 3
- $14 > 8 \rightarrow$ R; $> 10 \rightarrow$ R of 10
- $4 < 8 \rightarrow$ L; $> 3 \rightarrow$ R; $< 6 \rightarrow$ L of 6
- $7 < 8 \rightarrow$ L; $> 3 \rightarrow$ R; $> 6 \rightarrow$ R of 6



In-order: $1, 3, 4, 6, 7, 8, 10, 14$ (sorted)

Definition 5.24 — Expression Tree

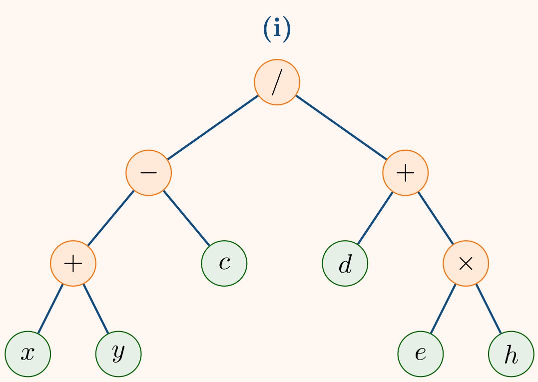
An **expression tree** is a binary tree for an algebraic expression:

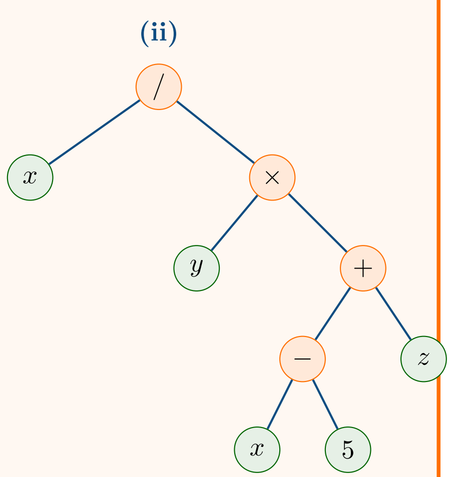
- **Leaves** = operands (numbers or variables)
- **Internal nodes** = operators ($+$, $-$, $\times$, $\div$)

Past Paper: 2024 Q4(b)

Example 5: Expression Trees — Past Paper 2024 Q4(b)

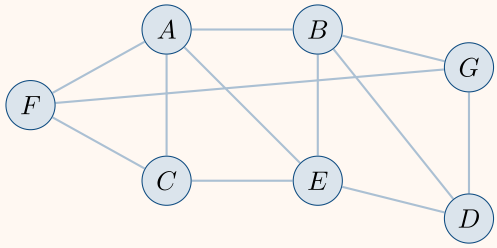
(i) $(x + y - c) \,/\, (d + e \times h)$ **(ii)** $x \,/\, (y \times (x - 5 + z))$





Example 6: Spanning Tree + Properties + BT vs BST — Past Paper 2023 Q6

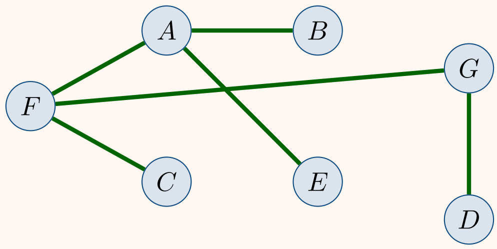
Graph G: $V = \{A, B, C, D, E, F, G\}$,
$E = \{FA, FC, AC, AB, AE, CE, EB, ED, BD, BG, DG, FG\}$



(a) Spanning tree (BFS from F):

Visit $F \to$ add A, C, G. Visit $A \to$ add B, E. Visit $C \to$ no new vertices. Visit $G \to$ add D. All 7 vertices reached.

Spanning tree edges: FA, FC, FG, AB, AE, GD



7 vertices, 6 edges $= n-1$. Connected, no cycles.

(b) Properties for a graph to be a tree:

- Connected and no cycles.
- Connected with exactly $n - 1$ edges.
- Exactly one simple path between any two vertices.
- Connected, but removing any edge makes it disconnected.

(c) Binary Tree vs BST:

A **binary tree** has no rule on key ordering — any value can go anywhere as long as each node has at most 2 children.

A **BST** adds the ordering rule: left subtree $<$ node $<$ right subtree at every node, which allows fast search.

Section 5.7 Summary

Type	Definition
Tree	Connected, no cycles, $n-1$ edges
Rooted tree	Tree with one root vertex
Binary tree	Rooted tree; each node has ≤ 2 children
Full binary tree	Binary tree; each internal node has exactly 2 children; $\ell = i+1$
BST	Binary tree with left $<$ node $<$ right at every node
Expression tree	Binary tree; leaves = operands, internal = operators

Height = max level. **Level/Depth** of v = edges from root to v.

Past Papers: 2020 Q1(ix)(xii); 2021 Q1(vi)(xii); 2022 Q1(vi)(vii)(ix); 2023 Q6 → Ex. 6; 2024 Q4(b) → Ex. 5; 2025 Q1(xii)

Tree Traversals and Spanning Trees

Definition 5.25 — Tree Traversals

Three standard ways to visit all nodes of a rooted tree:

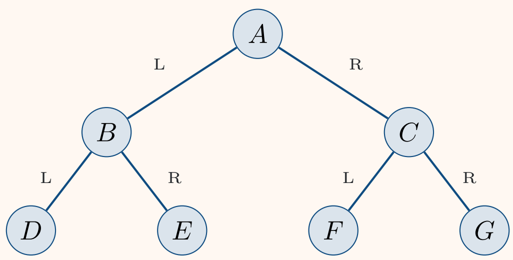
Traversal	Order of visiting
Pre-order	**Root** → Left subtree → Right subtree
In-order	Left subtree → **Root** → Right subtree
Post-order	Left subtree → Right subtree → **Root**

Memory aid:
Pre = **R**oot first. In = Root in the **middle**. Post = Root **last**.

Key fact: In-order traversal of a BST always gives keys in **sorted ascending order**.

Example 1: Pre-order / In-order / Post-order

Find all three traversals of this binary tree.



Pre-order (Root, Left, Right):

Visit A → go left to B → visit B → go left to D → visit D (leaf) → back to B, go right to E → visit E (leaf) → back to A, go right to C → visit C → go left to F → visit F (leaf) → go right to G → visit G (leaf).

Result: A, B, D, E, C, F, G

In-order (Left, Root, Right):

Go left to D (leaf) $\to$ visit D $\to$ visit B $\to$ go right to E $\to$ visit E $\to$ visit A $\to$ go left to F $\to$ visit F $\to$ visit C $\to$ go right to G $\to$ visit G.

Result: D, B, E, A, F, C, G

Post-order (Left, Right, Root):

Go to D (leaf) $\to$ visit D $\to$ go to E (leaf) $\to$ visit E $\to$ visit B $\to$ go to F (leaf) $\to$ visit F $\to$ go to G (leaf) $\to$ visit G $\to$ visit C $\to$ visit A.

Result: D, E, B, F, G, C, A

Traversal	**Order**
Pre-order	$A,\ B,\ D,\ E,\ C,\ F,\ G$
In-order	$D,\ B,\ E,\ A,\ F,\ C,\ G$
Post-order	$D,\ E,\ B,\ F,\ G,\ C,\ A$

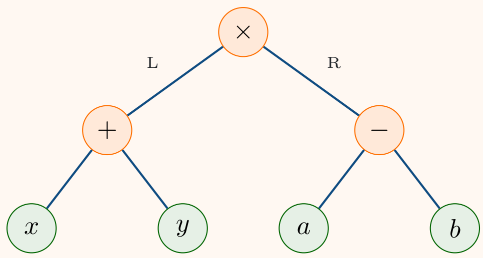
Definition 5.26 — Expression Notations

Traversing an expression tree gives three standard notations:

- **Pre-order** $\to$ **Prefix** (Polish notation): operator comes before its operands.
- **In-order** $\to$ **Infix** (normal math): operator is between operands.
- **Post-order** $\to$ **Postfix** (Reverse Polish): operator comes after its operands.

Example 2: Traversals on an Expression Tree

Expression tree for $(x + y) \times (a - b)$:



Traversal	**Notation**	**Result**
Pre-order	Prefix	$\times\ +\ x\ y\ -\ a\ b$
In-order	Infix	$x\ +\ y\ \times\ a\ -\ b$
Post-order	Postfix	$x\ y\ +\ a\ b\ -\ \times$

Note: infix needs parentheses to be unambiguous. Prefix and postfix do not need parentheses.

Definition 5.27 — Spanning Tree

A **spanning tree** of a connected graph G is a subgraph that:

- Includes **all vertices** of G.

- Is **connected** and **acyclic**.
- Has exactly $\mathbf{n-1}$ edges.

A graph can have **many different** spanning trees. Two standard methods to find one:

- **BFS** (Breadth-First Search) — explore level by level.
- **DFS** (Depth-First Search) — go as deep as possible before backtracking.

Past Paper: 2023 Q6

Definition 5.28 — BFS and DFS

BFS (Breadth-First Search):

1. Start at a source vertex s. Mark it visited. Add to a **queue**.
2. Dequeue vertex u. Visit all unvisited neighbours of u, mark them visited, add to queue.
3. Repeat until queue is empty.

BFS visits vertices **level by level**. The edges used to reach new vertices form the BFS spanning tree.

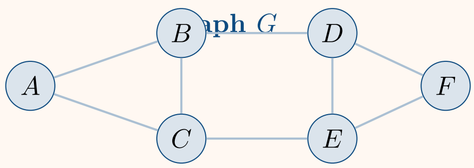
DFS (Depth-First Search):

1. Start at source s. Mark it visited. Push onto a **stack** (or use recursion).
2. Visit an unvisited neighbour v of the current vertex. Mark v visited and move to v.
3. If no unvisited neighbours exist, **backtrack**.
4. Repeat until all vertices are visited.

DFS goes **deep first**, backtracking when stuck. The edges used form the DFS spanning tree.

Example 3: BFS and DFS Spanning Trees

Apply BFS and DFS to the graph below, starting from vertex A.



BFS from A (alphabetical order for ties):

Queue: $[A]$. Visit A. Neighbours: B, C. Add both.
Queue: $[B, C]$. Visit B. Unvisited neighbours: D. (C already queued.) Add D.
Queue: $[C, D]$. Visit C. Unvisited neighbours: E. Add E.
Queue: $[D, E]$. Visit D. Unvisited neighbours: F. Add F.

Queue: $[E, F]$. Visit E: no new. Visit F: no new. Done.

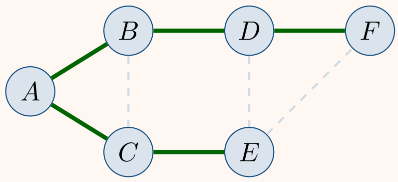
BFS tree edges: AB, AC, BD, CE, DF

DFS from A (alphabetical order for ties):

Visit $A \rightarrow$ go to B (first unvisited) $\rightarrow$ go to C (first unvisited of B, skip A) $\rightarrow$ go to E (first unvisited of C) $\rightarrow$ go to D (first unvisited of E) $\rightarrow$ go to F (first unvisited of D). All visited. Done.

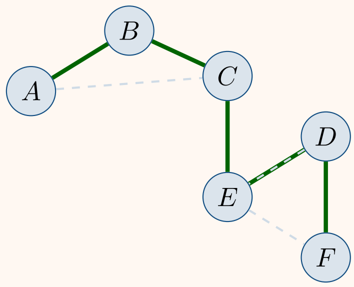
DFS tree edges: AB, BC, CE, ED, DF

BFS Spanning Tree



AB, AC, BD, CE, DF

DFS Spanning Tree



AB, BC, CE, ED, DF

Practice Exercises

Q1. A simple graph has 7 vertices. Each vertex has degree 3.

(i) How many edges does the graph have?

(ii) Is such a graph possible? Justify using the Handshaking Lemma.

(iii) Can this graph be complete? Give a reason.

Q2. A graph G has degree sequence $\{1, 2, 3, 3, 4, 4, 5\}$.

(i) Find the number of edges in G.

(ii) Is it possible to have a simple graph with this degree sequence?

(iii) Which vertex, if removed, would most reduce the connectivity?

Q3. For the graph K_6:

(i) Find the number of edges.

(ii) What is the degree of each vertex?

(iii) How many spanning trees does it have? (You may state the formula K_n has n^{n-2} spanning trees.)

(iv) Is K_6 planar? Justify using the edge inequality.

Q4. The following adjacency matrix represents a graph G:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

(i) Draw the graph G.

(ii) Find the degree of each vertex.

(iii) Is G connected? Is it bipartite?

(iv) Write the incidence matrix of G.

Q5. Two graphs G_1 and G_2 are given:

G_1: $V = \{a, b, c, d\}$, $E = \{ab, bc, cd, da\}$ (a 4-cycle).

G_2: $V = \{1, 2, 3, 4\}$, $E = \{12, 23, 34, 41\}$ (also a 4-cycle).

(i) Are G_1 and G_2 isomorphic? If yes, give a bijection.

(ii) What is the degree sequence of each graph?

(iii) Add one edge to G_1 and determine whether the new graph is isomorphic to K_4.

Q6. Determine whether the following graphs are isomorphic. Give a reason for your answer in each case.

(i) G_1 has degree sequence $\{2, 2, 3, 3, 4\}$ and G_2 has degree sequence $\{2, 2, 3, 3, 4\}$.

(ii) G_1 has a cycle of length 3; G_2 has no cycle of length 3.

(iii) G_1 has 5 vertices and 6 edges; G_2 has 5 vertices and 7 edges.

Q7. Consider this graph G with vertices $\{1, 2, 3, 4, 5\}$ and edges $\{12, 13, 14, 23, 35, 45\}$.

(i) Find the degree of each vertex.

(ii) Does G have an Euler path? Does it have an Euler circuit? Justify using degree conditions.

(iii) Find an Euler path if one exists.

Q8. A connected graph has 8 vertices. All vertices have even degree.

(i) Does the graph have an Euler circuit? State the theorem used.

(ii) If two vertices are changed to have odd degree, what can you say about an Euler path?

(iii) If all 8 vertices have odd degree, is an Euler path possible?

Q9. For each graph below, determine whether a Hamiltonian circuit exists. If yes, write one. If no, explain why.

(i) G_1: K_5 (complete graph on 5 vertices).

(ii) G_2: A path graph P_4 (four vertices in a line).

(iii) G_3: $n = 6$ vertices, all degrees ≥ 3. Apply Dirac's theorem.

Q10. A graph G has 6 vertices and 9 edges.

(i) Check whether G could be planar using the edge inequality $e \leq 3v - 6$.

(ii) If G is planar and connected, how many faces does it have? (Use Euler's formula $v - e + f = 2$.)

(iii) If G is bipartite, which edge inequality applies? Is G planar using that bound?

Q11. Find the chromatic number $\chi(G)$ for each graph. Justify your answer.

(i) K_4 (complete graph on 4 vertices).

(ii) C_6 (cycle of length 6).

(iii) C_5 (cycle of length 5).

(iv) $K_{2,3}$ (complete bipartite graph).

Q12. Apply **Prim's algorithm** starting from vertex A to the following weighted graph. Show each step in a table.

Vertices: $\{A, B, C, D, E\}$

Edges: $AB = 6,\ AC = 1,\ BC = 5,\ BD = 3,\ BE = 4,\ CD = 7,\ DE = 2$

(i) Find the MST and its total weight.

(ii) How many edges does any spanning tree of this graph have?

(iii) Would starting from D give the same total weight?

Q13. Apply **Kruskal's algorithm** to the same graph as Q12.

(i) Sort all edges by weight and list them.
(ii) Show which edges are added or skipped at each step, with reason.
(iii) Compare your MST with the one found by Prim's in Q12. Are they the same?

Q14. Apply **Dijkstra's algorithm** starting from vertex s to find shortest paths to all other vertices.

Vertices: $\{s, a, b, c, t\}$

Edges: $sa = 2,\ sb = 5,\ ab = 1,\ ac = 4,\ bc = 3,\ ct = 2,\ bt = 6$

(i) Build the distance table step by step.
(ii) What is the shortest distance from s to t?
(iii) Write the shortest path from s to t.

Q15. A tree has 10 vertices.

(i) How many edges does it have?
(ii) A new vertex is added and connected to one existing vertex. How many edges does the new tree have?
(iii) If the tree is rooted, what is the minimum possible height? What is the maximum possible height?

Q16. A rooted tree has root R, height 4, and is a full binary tree.

(i) What is the maximum number of leaves?
(ii) If the tree has 7 internal vertices, how many leaves does it have? (Use $\ell = i + 1$.)
(iii) How many total vertices are there if it has 7 internal vertices?

Q17. Insert the following keys into an empty BST in the given order: 15, 9, 20, 6, 12, 17, 25

(i) Draw the resulting BST.
(ii) Write the in-order traversal.
(iii) Write the pre-order traversal.
(iv) Write the post-order traversal.
(v) Search for key 12. How many comparisons are needed?

Q18. A BST is built by inserting: 5, 3, 7, 1, 4, 6, 8

(i) Draw the BST.
(ii) Give in-order, pre-order, and post-order traversals.
(iii) Is this a full binary tree? Justify.
(iv) What is the height of this BST?

Q19. Draw an expression tree for each expression. Then write the prefix (pre-order) and postfix (post-order) notations.

(i) $(a+b)\times(c-d)$
(ii) $x \div (y+z) - w$
(iii) $(p \times q) + (r \times s)$

Q20. Convert the following prefix expression to a tree, then evaluate to infix form.

(i) $+ \ \times \ a \, b \ - \ c \, d$
(ii) $\times \ + \ 2 \, 3 \ - \ 5 \, 1$
(iii) $- \ + \ a \ \times \ b \, c \, d$

Q21. For the graph G with $V = \{P, Q, R, S, T, U\}$ and $E = \{PQ, PR, QR, QS, RT, ST, SU, TU\}$:

(i) Find a spanning tree using BFS starting from P.
(ii) Find a spanning tree using DFS starting from P.
(iii) Are the two spanning trees the same?
(iv) How many edges does each spanning tree have?

Q22. A graph G has 9 vertices and 12 edges and is connected.

(i) How many edges does a spanning tree of G have?
(ii) How many edges are NOT in the spanning tree? (These form the co-tree.)
(iii) Apply Kruskal's algorithm to find the MST if the edges are weighted as follows: Three edges of weight 2, four edges of weight 4, five edges of weight 7. (Show which edges are chosen.)

Q23. Answer the following short questions:

(i) Define a forest. How many edges does a forest with n vertices and k components have?
(ii) Is every tree a bipartite graph? Justify.
(iii) Can a tree have a cycle? Why or why not?
(iv) What is the chromatic number of any tree with more than one vertex?

Q24. The post-order traversal of a binary tree gives: $E,\ C,\ F,\ D,\ B,\ H,\ I,\ G,\ A$

The in-order traversal gives: $C,\ E,\ B,\ D,\ F,\ A,\ H,\ G,\ I$

(i) What is the root of the tree?
(ii) Reconstruct the full binary tree from these two traversals.
(iii) Write the pre-order traversal of the reconstructed tree.

Q25. A connected weighted graph has vertices $\{1, 2, 3, 4, 5, 6\}$ and the following edges with weights:

$12 = 4,\ 13 = 1,\ 14 = 8,\ 23 = 2,\ 25 = 6,\ 34 = 3,\ 35 = 9,\ 46 = 5,\ 56 = 7$

(i) Find the MST using Kruskal's algorithm. Show the sorted edge list and each step.
(ii) Find the MST using Prim's algorithm starting from vertex 1. Show the step-by-step table.
(iii) Find the shortest path from vertex 1 to vertex 6 using Dijkstra's algorithm.
(iv) What is the total weight of the MST?