MH1300 Foundations of Mathematics

Revision Notes

Quantitative Research Society @NTU

Academic Year 2025-2026, Semester 1

December 10, 2025

Overview of this document

This document unifies the core theoretical framework of the course with extensive problem-solving practice, offering a single authoritative source for conceptual mastery and exam preparation. It includes:

- **Five years of final examination coverage** (AY2020/21–AY2024/25), distilled and cross-analysed for patterns and recurring themes.
- **Complete theoretical foundations**: fully formal definitions, theorems, propositions, and proofs.
- **Deep explanatory expansion**: intuition, motivation, logical structure, geometric interpretation, and conceptual links across topics.
- **Enhanced worked examples** drawn from tutorials and past exams, with step-by-step solutions mirroring model-answer quality.
- **Visual learning aids**: TikZ diagrams, truth tables, mapping diagrams, relation graphs, and structured proof templates.
- **Exam-focused insights**: high-frequency pitfalls, common misconceptions, and targeted exam strategies.
- **Concise summary sheets** designed for rapid pre-exam review.

For academic reference only. This document is provided for educational purposes and does not constitute an official question paper, answer key, or any formally authorised academic material. Its content is not guaranteed to be complete or accurate.

Topics Covered

1. Propositional Logic, Arguments, and Proof Techniques
2. Predicate Logic, Quantifiers, and Logical Equivalence
3. Number Theory: Divisibility, Modular Arithmetic, Primes
4. Set Theory, Operations, and Fundamental Identities
5. Relations: Equivalence Relations, Partially Ordered Sets
6. Functions: Injectivity, Surjectivity, Bijectivity, Composition, Inverses
7. Mathematical Induction: Weak, Strong, and Structural Forms
8. Complex Numbers and Roots of Unity
9. Additional Topics: Floor/Ceiling Functions, Archimedean Property, and Related Extensions

This compendium is designed to serve simultaneously as a lecture replacement, a tutorial summary, an examination guide, and a complete final-revision resource.

Contents

1 Propositional Logic and Proof Techniques

1.1 Overview

Propositional logic forms the foundation of all mathematical reasoning. It provides us with the tools to construct rigorous arguments, verify the validity of mathematical statements, and build complex proofs from simple premises. This chapter introduces the formal language of logic, teaches you how to manipulate logical expressions systematically, and equips you with the essential proof techniques used throughout mathematics.

Why this matters: Every mathematical proof you encounter — whether in analysis, algebra, or discrete mathematics — relies fundamentally on the principles of propositional logic. Mastering this topic enables you to:

- Distinguish valid arguments from fallacious ones
- Construct clear, rigorous mathematical proofs
- Recognize equivalent formulations of the same mathematical statement
- Debug errors in reasoning systematically

Connection to later topics: The logical framework developed here underpins everything in MH1300. Set operations mirror logical operations, quantifiers extend propositional logic to predicates, and proof techniques directly use the rules of inference we develop in this chapter.

1.2 Definitions & Setup

Definition 1.1: Proposition

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

Example

Propositions:

- "$2 + 2 = 4$" (True)
- "The earth is flat" (False)
- "7 is a prime number" (True)

Not propositions:

- "What time is it?" (Question, not declarative)
- "Close the door" (Command)
- "$x > 5$" (Truth value depends on x — this is a *predicate*, covered later)

Definition 1.2: Logical Connectives

Propositions can be combined using **logical connectives**:

- **Negation** ($\neg p$): "not p"
- **Conjunction** ($p \wedge q$): "p and q"
- **Disjunction** ($p \vee q$): "p or q" (inclusive or)
- **Implication** ($p \to q$): "if p then q"
- **Biconditional** ($p \leftrightarrow q$): "p if and only if q"

Truth Tables: The meaning of each connective is defined by its truth table:

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

Remark

Key observations:

- The implication $p \to q$ is **false only when** p is true and q is false. In particular, if p is false, then $p \to q$ is automatically true ("vacuously true").
- The biconditional $p \leftrightarrow q$ is true exactly when p and q have the *same* truth value.
- Disjunction $p \vee q$ is **inclusive**: it's true if at least one of p or q is true (possibly both).

Definition 1.3: Tautology, Contradiction, Contingency

- A compound proposition is a **tautology** if it is true for all possible truth assignments (always T).
- A compound proposition is a **contradiction** if it is false for all possible truth assignments (always F).
- A compound proposition is a **contingency** if it is neither a tautology nor a contradiction.

Examples: Tautology, Contradiction, Contingency

- $p \vee \neg p$ is a **tautology** (law of excluded middle)
- $p \wedge \neg p$ is a **contradiction**

- $p \to q$ is a **contingency** (depends on values of p and q)

1.3 Key Theorems & Results

1.3.1 Logical Equivalence Laws

Theorem 1.1: Fundamental Logical Equivalences

Two compound propositions are **logically equivalent**, written $P \equiv Q$, if they have the same truth value under all truth assignments.

Important Equivalences:

Implication Laws:

$$\begin{aligned} p \to q &\equiv \neg p \vee q \\ p \to q &\equiv \neg q \to \neg p \quad \text{(Contrapositive)} \end{aligned}$$

Biconditional:

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

De Morgan's Laws:

$$\begin{aligned} \neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q \end{aligned}$$

Double Negation:

$$\neg\neg p \equiv p$$

Distributive Laws:

$$\begin{aligned} p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r) \\ p \vee (q \wedge r) &\equiv (p \vee q) \wedge (p \vee r) \end{aligned}$$

Associativity:

$$\begin{aligned} (p \wedge q) \wedge r &\equiv p \wedge (q \wedge r) \\ (p \vee q) \vee r &\equiv p \vee (q \vee r) \end{aligned}$$

Commutativity:

$$\begin{aligned} p \wedge q &\equiv q \wedge p \\ p \vee q &\equiv q \vee p \end{aligned}$$

Absorption Laws:

$$\begin{aligned} p \vee (p \wedge q) &\equiv p \\ p \wedge (p \vee q) &\equiv p \end{aligned}$$

Negation Laws:

$$\begin{aligned} p \lor \neg p &\equiv \top \quad \text{(Tautology)} \\ p \land \neg p &\equiv \bot \quad \text{(Contradiction)} \end{aligned}$$

Universal Bound Laws:

$$\begin{aligned} p \lor \top &\equiv \top \\ p \land \bot &\equiv \bot \end{aligned}$$

Identity Laws:

$$\begin{aligned} p \lor \bot &\equiv p \\ p \land \top &\equiv p \end{aligned}$$

Remark

Proof Strategy: To show two compound propositions are logically equivalent, you can either:

1. Construct truth tables for both and verify they match in every row, OR
2. Use a sequence of known logical equivalences to transform one into the other

Method (2) is generally faster and more elegant for complex formulas.

1.4 Worked Examples

1.4.1 Tutorial Example: Logical Equivalence

Past Exam Question (AY 24/25): Logical Equivalence

Question: Are the following pair of statements logically equivalent?

$$(p \to q) \to (p \land r) \quad \text{and} \quad p \land (q \to r)$$

Justify your answer.

Solution:

We use logical equivalence laws to transform the first expression:

$$\begin{aligned}
(p \to q) \to (p \wedge r) &\equiv \neg(p \to q) \vee (p \wedge r) && \text{(Implication law)} \\
&\equiv \neg(\neg p \vee q) \vee (p \wedge r) && \text{(Implication law)} \\
&\equiv (\neg\neg p \wedge \neg q) \vee (p \wedge r) && \text{(De Morgan's law)} \\
&\equiv (p \wedge \neg q) \vee (p \wedge r) && \text{(Double negation)} \\
&\equiv p \wedge (\neg q \vee r) && \text{(Distributive law)} \\
&\equiv p \wedge (q \to r) && \text{(Implication law)}
\end{aligned}$$

Thus the two statements are logically equivalent: $(p \to q) \to (p \wedge r) \equiv p \wedge (q \to r)$. □

Common Mistake

Common Error: Students sometimes try to "cancel" terms or manipulate logical formulas like algebraic expressions. For example, writing

$$(p \to q) \to (p \wedge r) \overset{?}{\equiv} q \to (p \wedge r)$$

is **incorrect**. You *cannot* cancel p from an implication. Always use the formal equivalence laws.

1.4.2 Past Exam Example: Tautology Classification

Past Exam Question (AY 22/23): Is This a Tautology?

Question: Is the following statement a tautology, a contradiction, or neither?

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

Method 1: Truth Table

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

The final column is all T, so the expression is a **tautology**.

Method 2: Logical Equivalence

$$
\begin{aligned}
&(p \wedge \neg q) \vee ((\neg p \wedge q) \vee (\neg p \vee q)) \\
&\equiv (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \vee q) && \text{(Associativity)} \\
&\equiv (p \wedge \neg q) \vee (\neg p \vee q) && \text{(Absorption: } (\neg p \wedge q) \vee (\neg p \vee q) \equiv (\neg p \vee q)) \\
&\equiv (p \wedge \neg q) \vee \neg p \vee q \\
&\equiv ((p \wedge \neg q) \vee \neg p) \vee q \\
&\equiv (p \vee \neg p) \wedge (\neg q \vee \neg p) \vee q && \text{(Distributive)} \\
&\equiv \top \wedge (\neg q \vee \neg p) \vee q && \text{(Negation law)} \\
&\equiv (\neg q \vee \neg p) \vee q \\
&\equiv \neg p \vee (\neg q \vee q) && \text{(Associativity, commutativity)} \\
&\equiv \neg p \vee \top && \text{(Negation law)} \\
&\equiv \top && \text{(Universal bound)}
\end{aligned}
$$

Thus the expression is a **tautology**. □

Exam Tip

Exam Tip: If a truth table has 3 variables, it has $2^3 = 8$ rows. For 4 variables, $2^4 = 16$ rows. When you have 3 or more variables, using logical equivalences is often faster than constructing a full truth table. However, truth tables are more systematic and less error-prone for beginners.

1.4.3 Additional Constructed Example: Proving a Tautology

Constructed Example: Verifying $(p \to (q \wedge \neg r)) \to (\neg q \to \neg p)$ is a Tautology

Claim: The statement $(p \to (q \wedge \neg r)) \to (\neg q \to \neg p)$ is a tautology.

Proof (using equivalences):

$$\begin{aligned}
&(p \to (q \wedge \neg r)) \to (\neg q \to \neg p) \\
&\equiv \neg(p \to (q \wedge \neg r)) \vee (\neg q \to \neg p) && \text{(Implication)} \\
&\equiv \neg(\neg p \vee (q \wedge \neg r)) \vee (\neg\neg q \vee \neg p) && \text{(Implication } \times 2\text{)} \\
&\equiv (\neg\neg p \wedge \neg(q \wedge \neg r)) \vee (q \vee \neg p) && \text{(De Morgan, double negation)} \\
&\equiv (p \wedge (\neg q \vee r)) \vee (q \vee \neg p) && \text{(Double negation, De Morgan)} \\
&\equiv (p \wedge (\neg q \vee r)) \vee q \vee \neg p \\
&\equiv ((p \wedge (\neg q \vee r)) \vee q) \vee \neg p \\
&\equiv (((p \wedge \neg q) \vee (p \wedge r)) \vee q) \vee \neg p && \text{(Distributive)} \\
&\equiv (p \wedge \neg q) \vee (p \wedge r) \vee q \vee \neg p \\
&\equiv (p \wedge \neg q) \vee q \vee (p \wedge r) \vee \neg p \\
&\equiv ((p \vee q) \wedge (\neg q \vee q)) \vee (p \wedge r) \vee \neg p && \text{(Distributive)} \\
&\equiv ((p \vee q) \wedge \top) \vee (p \wedge r) \vee \neg p \\
&\equiv (p \vee q) \vee \neg p \vee (p \wedge r) \\
&\equiv (p \vee \neg p) \vee q \vee (p \wedge r) && \text{(Associativity, commutativity)} \\
&\equiv \top \vee q \vee (p \wedge r) \\
&\equiv \top
\end{aligned}$$

Therefore the statement is a tautology. □

1.5 Rules of Inference and Argument Validity

Definition 1.4: Valid Argument

An **argument** consists of a sequence of propositions called **premises** and a final proposition called the **conclusion**. An argument is **valid** if whenever all the premises are true, the conclusion must also be true.
Symbolically, an argument with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$$

is a tautology.

Theorem 1.2: Common Rules of Inference

1. Modus Ponens:

$$\begin{array}{c} p \to q \\ p \\ \hline \therefore q \end{array}$$

2. Modus Tollens:

$$\begin{array}{c} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

3. Disjunctive Syllogism:

$$\begin{array}{c} p \lor q \\ \neg p \\ \hline \therefore q \end{array} \quad \text{or} \quad \begin{array}{c} p \lor q \\ \neg q \\ \hline \therefore p \end{array}$$

4. Hypothetical Syllogism:

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

5. Conjunction:

$$\begin{array}{c} p \\ q \\ \hline \therefore p \land q \end{array}$$

6. Simplification:

$$\begin{array}{c} p \land q \\ \hline \therefore p \end{array} \quad \text{or} \quad \begin{array}{c} p \land q \\ \hline \therefore q \end{array}$$

7. Addition:

$$\begin{array}{c} p \\ \hline \therefore p \lor q \end{array}$$

8. Resolution:

$$\begin{array}{c} p \lor q \\ \neg p \lor r \\ \hline \therefore q \lor r \end{array}$$

1.5.1 Worked Example: Proving Argument Validity

Past Exam Question (AY 22/23): Show Argument is Valid

Question: Show that the following argument form is valid. State all rules of inference used.

$$\begin{array}{l} p \lor q \\ (\neg q) \lor s \\ r \to (\neg s) \\ \neg p \\ \therefore \neg r \end{array}$$

Solution (using indirect proof):

1.	$p \lor q$	Premise
2.	$\neg q \lor s$	Premise
3.	$r \to \neg s$	Premise
4.	$\neg p$	Premise
5.	q	From 1,4 (Disjunctive Syllogism)
6.	s	From 2,5 (Disjunctive Syllogism)
7.	Assume r	Assumption for Indirect Proof
8.	$\neg s$	From 3,7 (Modus Ponens)
9.	$s \land \neg s$	From 6,8 (Contradiction)
10.	$\neg r$	From 7–9 (Indirect Proof)

The argument form is valid. □

Remark

Indirect proof (also called *proof by contradiction* or *reductio ad absurdum*) works by assuming the negation of what you want to prove, deriving a contradiction, and concluding that your assumption must be false.

1.6 Proof Techniques

Definition 1.5: Major Proof Techniques

1. **Direct Proof:** Assume the hypothesis p is true, then use logical steps to show the conclusion q must be true.

2. **Proof by Contrapositive:** To prove $p \to q$, instead prove $\neg q \to \neg p$ (which is logically equivalent).

3. **Proof by Contradiction:** To prove a statement p, assume $\neg p$ and derive a contradiction.

4. **Proof by Cases:** Break the argument into exhaustive cases and prove the conclusion in each case separately.

5. **Vacuous Proof:** To prove $p \to q$, if you can show p is false, then $p \to q$ is automatically true.

6. **Trivial Proof:** To prove $p \to q$, if you can show q is true, then $p \to q$ is automatically true.

We will see extensive applications of these techniques throughout the course, particularly in Number Theory and Mathematical Induction.

1.7 Common Mistakes & Exam Tips

Common Mistake

Mistake 1: Confusing $p \to q$ with its converse $q \to p$
These are **not** equivalent! For example:

- $p \to q$: "If it rains, then the ground is wet"
- $q \to p$: "If the ground is wet, then it rains" (False! Could be from a sprinkler)

The **contrapositive** $\neg q \to \neg p$ is equivalent to $p \to q$, but the converse is not.

Common Mistake

Mistake 2: Incorrect use of De Morgan's Laws
Wrong: $\neg(p \vee q) \equiv \neg p \vee \neg q$ (Missing the change from $\vee$ to $\wedge$!)
Correct: $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Common Mistake

Mistake 3: Treating logical equivalence like equation solving
You cannot "move" terms across equivalences arbitrarily. Each step must use a known logical equivalence law.

Exam Tip

Exam Strategy for Logical Equivalence Problems:

1. Write down the expression clearly
2. Apply **one equivalence law at a time**, citing the law
3. For implications, convert to disjunctions early: $p \to q \equiv \neg p \vee q$
4. Use De Morgan's laws to push negations inward
5. Use distributive laws to factor or expand
6. Simplify using absorption, negation laws, and universal bounds

Exam Tip

Exam Strategy for Validity Proofs:

1. List all premises and what needs to be proven
2. Look for simple deductions (Modus Ponens, Disjunctive Syllogism)
3. If stuck, try assuming the opposite of the conclusion and deriving a contradiction

4. Clearly cite each rule of inference used

1.8 Topic Summary

Propositional Logic Quick Reference

Core Definitions:

- Proposition: declarative sentence that is T or F
- Tautology: always T; Contradiction: always F; Contingency: neither
- Logical equivalence: $P \equiv Q$ if same truth values under all assignments

Key Equivalences to Memorize:

$$\begin{aligned} p \to q &\equiv \neg p \vee q \equiv \neg q \to \neg p \\ p \leftrightarrow q &\equiv (p \to q) \wedge (q \to p) \\ \neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q \\ p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r) \\ p \vee (p \wedge q) &\equiv p \end{aligned}$$

Essential Rules of Inference:

- Modus Ponens: $p \to q, p \therefore q$
- Modus Tollens: $p \to q, \neg q \therefore \neg p$
- Disjunctive Syllogism: $p \vee q, \neg p \therefore q$
- Hypothetical Syllogism: $p \to q, q \to r \therefore p \to r$

Proof Techniques:

1. Direct: assume p, derive q
2. Contrapositive: prove $\neg q \to \neg p$ instead of $p \to q$
3. Contradiction: assume $\neg p$, derive contradiction
4. Cases: prove in all exhaustive cases

Common Traps:

- $p \to q \not\equiv q \to p$ (converse is not equivalent!)
- Always apply one equivalence law at a time
- Cite your rules of inference in validity proofs

2 Predicate Logic and Quantifiers

2.1 Overview

While propositional logic allows us to reason about statements that are simply true or false, many mathematical statements involve variables and make claims about entire sets of objects. For example, "For every integer n, $n^2 \geq 0$" or "There exists a real number x such that $x^2 = 2$" cannot be adequately expressed in propositional logic alone.

Predicate logic extends propositional logic by introducing:

- **Predicates:** statements involving variables whose truth depends on the values of those variables
- **Quantifiers:** symbols that express "for all" ($\forall$) and "there exists" ($\exists$)

This machinery is essential for expressing and proving mathematical theorems rigorously.

2.2 Definitions & Setup

Definition 2.1: Predicate

A **predicate** (or propositional function) $P(x)$ is a statement involving a variable x that becomes a proposition once x is assigned a specific value from a specified **domain of discourse** (or universe).
Example: $P(x) : x^2 > 0$ with domain $\mathbb{R}$ is a predicate. $P(2)$ is true, $P(0)$ is false.

Definition 2.2: Quantifiers

Universal Quantifier ($\forall$): "for all", "for every", "for each"

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

means "$P(x)$ is true for every x in the domain."
Existential Quantifier ($\exists$): "there exists", "there is at least one", "for some"

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

means "$P(x)$ is true for at least one x in the domain."

Example

Let the domain be $\mathbb{Z}$ (integers) and let $E(n)$ denote "n is even."

- $\forall n\, E(n)$ is **false** (not all integers are even; e.g., 3 is odd)
- $\exists n\, E(n)$ is **true** (e.g., $n = 2$ is even)

Definition 2.3: Negation of Quantified Statements

Key Rule: Negation swaps quantifiers and negates the predicate:

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

Negating Quantified Statements

Statement: "Every student in this class has taken calculus."
Formal: $\forall x\, C(x)$ where $C(x)$: "student x has taken calculus"
Negation: $\exists x\, \neg C(x)$ — "There exists a student who has not taken calculus."

2.3 Worked Examples

2.3.1 Tutorial Example: Determining Truth of Quantified Statements

Past Exam Question (AY 22/23): Quantifiers Over $\mathbb{R}$

Question: Let $P(x, y)$ be the predicate $x^2 + y < 0$, where the domain for x, y is the set of real numbers. Determine if each of the following is true or false and justify your answers:

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

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

Solution:
(i) $\forall y \, \exists x \, P(x, y)$:
This asks: for every real y, is there some real x such that $x^2 + y < 0$?
Take $y = 1$. Then for any real x,

$$x^2 + 1 \geq 1 > 0,$$

so $P(x, 1)$ is false for all $x \in \mathbb{R}$.
Thus for this particular $y = 1$, there is *no* suitable x.
Hence $\forall y \, \exists x \, P(x, y)$ is **false**. □

(ii) $\exists y \, \forall x \, P(x, y)$:
This asks: is there some $y \in \mathbb{R}$ such that $x^2 + y < 0$ for every $x \in \mathbb{R}$?
Suppose such a y exists. Then in particular, for $x = 0$,

$$0^2 + y < 0 \quad \Rightarrow \quad y < 0.$$

Now choose x large enough so that $x^2 > -y$ (possible since $y < 0$). Then

$$x^2 + y > 0,$$

contradicting the requirement that $x^2 + y < 0$ for all x.
Hence no such y exists, and $\exists y \, \forall x \, P(x, y)$ is **false**. □

Remark

Order matters! $\forall y \, \exists x$ means: for each y, we can choose a (possibly different) x that depends on y. But $\exists y \, \forall x$ means: there is one fixed y that works for every x simultaneously. These are very different!

2.4 Common Mistakes & Exam Tips

Common Mistake

Mistake: Confusing quantifier order
$\forall x\, \exists y\, P(x, y)$ is NOT the same as $\exists y\, \forall x\, P(x, y)$.
Example: Let $P(x, y)$ be "$x < y$" over $\mathbb{R}$.

- $\forall x\, \exists y\, (x < y)$ is **true** (for any x, take $y = x + 1$).
- $\exists y\, \forall x\, (x < y)$ is **false** (no single y is larger than all x).

Common Mistake

Mistake: Incorrect negation of quantifiers
Wrong: $\neg(\forall x\, P(x)) \equiv \forall x\, \neg P(x)$
Correct: $\neg(\forall x\, P(x)) \equiv \exists x\, \neg P(x)$
Remember: negation *swaps* the quantifier!

Exam Tip

Strategy for Showing $\forall x\, P(x)$ is false:
Find ONE counterexample — one specific x for which $P(x)$ fails.
Strategy for Showing $\exists x\, P(x)$ is false:
Show that $P(x)$ fails for *all* x in the domain.

2.5 Topic Summary

Predicate Logic Quick Reference

Core Concepts:

- Predicate $P(x)$: statement with variable; truth depends on value of x
- Domain of discourse: set from which x is drawn
- $\forall x\, P(x)$: $P(x)$ is true for every x in the domain
- $\exists x\, P(x)$: $P(x)$ is true for at least one x in the domain

Negation Rules:

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

Order of Quantifiers:

- $\forall x\, \exists y\, P(x, y)$: for each x, there is (possibly different) y making P true
- $\exists y\, \forall x\, P(x, y)$: there is one fixed y making P true for all x

Exam Tips:

- To disprove $\forall x\, P(x)$: give one counterexample
- To disprove $\exists x\, P(x)$: show $P(x)$ fails for all x
- Always specify the domain of discourse clearly
- When negating, swap quantifiers and negate the predicate

3 Number Theory: Divisibility, Parity, and Modular Arithmetic

3.1 Overview

Number theory is the study of properties of integers. In MH1300, we focus on:

- **Divisibility:** understanding when one integer divides another
- **Parity:** properties of even and odd integers
- **Modular arithmetic:** arithmetic modulo n
- **GCD and the Euclidean algorithm**
- **Primes and unique factorization**
- **Irrationality proofs**

These topics provide the foundation for rigorous proofs and are heavily tested in MH1300 exams.

3.2 Definitions & Setup

Definition 3.1: 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 $b = ak$.
If a does not divide b, we write $a \nmid b$.

Example

- $3 \mid 12$ because $12 = 3 \cdot 4$
- $5 \nmid 13$ because $13 = 5 \cdot 2 + 3$ (remainder is non-zero)
- $7 \mid 0$ because $0 = 7 \cdot 0$
- For any $n \neq 0$, $n \mid 0$ and $1 \mid n$

Definition 3.2: Even and Odd Integers

An integer n is **even** if $2 \mid n$, i.e., $n = 2k$ for some integer k.
An integer n is **odd** if $n = 2k + 1$ for some integer k.

Remark

Every integer is either even or odd, but not both. This is the foundation of many proof-by-cases arguments.

Definition 3.3: Division Algorithm (Quotient-Remainder Theorem)

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}$ with $d > 0$. Then there exist unique integers q (quotient) and r (remainder) such that

$$a = dq + r, \quad 0 \leq r < d.$$

We write $q = a \operatorname{div} d$ and $r = a \bmod d$.

Example

- $17 = 5 \cdot 3 + 2$, so $17 \operatorname{div} 5 = 3$ and $17 \bmod 5 = 2$
- $-17 = 5 \cdot (-4) + 3$, so $-17 \operatorname{div} 5 = -4$ and $-17 \bmod 5 = 3$

Definition 3.4: Modular Congruence

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}$ with $n > 0$. We say a is **congruent to** b **modulo** n, written

$$a \equiv b \pmod{n},$$

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

Example

- $17 \equiv 5 \pmod{12}$ because $17 - 5 = 12$ and $12 \mid 12$
- $-3 \equiv 7 \pmod{10}$ because $-3 - 7 = -10$ and $10 \mid -10$
- $25 \equiv 1 \pmod{8}$ because both have remainder 1 when divided by 8

3.3 Key Theorems & Results

Theorem 3.1: Properties of Divisibility

Let $a, b, c \in \mathbb{Z}$.

1. **Transitivity:** If $a \mid b$ and $b \mid c$, then $a \mid c$.
2. **Linear Combination:** If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.
3. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

4. If $a \mid b$ and $b \mid a$, then $a = \pm b$.

Theorem 3.2: Properties of Modular Arithmetic

Let $a, b, c, d \in \mathbb{Z}$ and $n > 0$.

1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:
   - $a + c \equiv b + d \pmod{n}$
   - $a - c \equiv b - d \pmod{n}$
   - $ac \equiv bd \pmod{n}$
2. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any $k \geq 0$.

Theorem 3.3: GCD and Euclidean Algorithm

The **greatest common divisor** $\gcd(a, b)$ is the largest positive integer that divides both a and b.
The **Euclidean algorithm** computes $\gcd(a, b)$ by repeatedly applying:

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

until the remainder is 0.

3.4 Worked Examples

3.4.1 Tutorial Example: Parity Proof

Past Exam Question (AY 21/22): Parity of $a - b$ and $a^2 + b^2$

Question: Let a and b be integers. Prove that $a - b$ and $a^2 + b^2$ have the same parity.

Solution (by cases):
We divide into two cases, according to the parity of $a - b$.
Case 1: $a - b$ is odd.
Then $a + b = (a - b) + 2b = \text{odd} + \text{even} = \text{odd}$.
Therefore

$$a^2 - b^2 = (a + b)(a - b) = \text{odd} \times \text{odd} = \text{odd}.$$

Hence

$$a^2 + b^2 = (a^2 - b^2) + 2b^2 = \text{odd} + \text{even} = \text{odd}.$$

Case 2: $a - b$ is even.
Then $a + b = (a - b) + 2b = \text{even} + \text{even} = \text{even}$, so

$$a^2 - b^2 = (a + b)(a - b) = \text{even} \times \text{even} = \text{even},$$

and hence

$$a^2 + b^2 = (a^2 - b^2) + 2b^2 = \text{even} + \text{even} = \text{even}.$$

In both cases, $a - b$ and $a^2 + b^2$ have the same parity. □

3.4.2 Past Exam Example: Divisibility and Modular Arithmetic

Past Exam Question (AY 24/25): Prove $n^4 - 1 \not\equiv 0 \pmod 5 \Rightarrow 5 \mid n$

Question: Prove that for every integer n, if $n^4 - 1$ is not divisible by 5 then n is divisible by 5.

Solution (by contrapositive):
We prove the contrapositive: if n is not divisible by 5, then $n^4 - 1$ is divisible by 5. Let n be an integer not divisible by 5. By the quotient–remainder theorem,

$$n = 5q + 1,\ 5q + 2,\ 5q + 3,\ \text{or}\ 5q + 4$$

for some integer q.
Case 1: $n = 5q + 1$.

$$n - 1 = 5q \quad \Rightarrow \quad n^4 - 1 = (n^2 + 1)(n + 1)(n - 1) = 5q \cdot (\cdots),$$

so $5 \mid (n^4 - 1)$.
Case 2: $n = 5q + 2$.

$$n^2 = (5q + 2)^2 = 25q^2 + 20q + 4 \equiv 4 \pmod 5$$

$$n^2 + 1 \equiv 5 \equiv 0 \pmod 5$$

so $5 \mid (n^2 + 1)$, and hence $5 \mid (n^4 - 1) = (n^2 + 1)(n + 1)(n - 1)$.
Case 3: $n = 5q + 3$.

$$n^2 = (5q + 3)^2 = 25q^2 + 30q + 9 \equiv 4 \pmod 5$$

$$n^2 + 1 \equiv 0 \pmod 5$$

so $5 \mid (n^4 - 1)$.
Case 4: $n = 5q + 4$.

$$n + 1 = 5q + 5 = 5(q + 1),$$

so $5 \mid (n + 1)$, and hence $5 \mid (n^4 - 1)$.
In all cases, $5 \mid (n^4 - 1)$. Hence the contrapositive is true, so the original statement holds. □

3.4.3 Additional Constructed Example: Euclidean Algorithm

Constructed Example: Finding $\gcd(630, 96)$

Question: Use the Euclidean algorithm to find $\gcd(630, 96)$.

Solution:
Apply the Euclidean algorithm:

$$\begin{aligned}
630 &= 96 \cdot 6 + 54 \\
96 &= 54 \cdot 1 + 42 \\
54 &= 42 \cdot 1 + 12 \\
42 &= 12 \cdot 3 + 6 \\
12 &= 6 \cdot 2 + 0
\end{aligned}$$

The last non-zero remainder is 6, so $\gcd(630, 96) = 6$. □

3.5 Common Mistakes & Exam Tips

Common Mistake

Mistake: Confusing "$a \mid b$" with "a/b"
$a \mid b$ is a *relation* (true or false), not a number!
Correct: $3 \mid 12$ (true statement)
Incorrect: $3 \mid 12 = 4$ (meaningless!)

Common Mistake

Mistake: Forgetting that the remainder must be non-negative
In the division algorithm, $0 \le r < d$ always.
For $-17 = 5q + r$, we have $q = -4$ and $r = 3$ (NOT $q = -3$ and $r = -2$).

Exam Tip

Exam Strategy for Parity Proofs:

1. Use the definitions: even $= 2k$, odd $= 2k + 1$
2. Divide into cases (often: both even, both odd, opposite parity)
3. Use parity rules: even ± even = even, odd ± odd = even, even × anything = even, odd × odd = odd

Exam Tip

Exam Strategy for Divisibility Proofs:

1. Use the quotient-remainder theorem to split into cases modulo the divisor
2. Use modular arithmetic to simplify computations
3. Remember: to prove $d \mid (a+b)$, it suffices to show $d \mid a$ and $d \mid b$

3.6 Topic Summary

Number Theory Quick Reference

Core Definitions:

- $a \mid b$: $\exists k \in \mathbb{Z}, b = ak$
- Even: $n = 2k$; Odd: $n = 2k + 1$
- $a \equiv b \pmod{n}$: $n \mid (a - b)$
- $\gcd(a, b)$: largest positive integer dividing both a and b

Key Properties:

- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$
- Parity rules: even ± even = even, odd ± odd = even, even × anything = even, odd × odd = odd

Euclidean Algorithm:

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

Repeat until remainder is 0.

Proof Techniques:

- Parity: divide into cases (even/odd)
- Divisibility: use quotient-remainder theorem or modular arithmetic
- Contrapositive: often easier for divisibility statements

4 Set Theory and Operations

4.1 Overview

Set theory provides the fundamental language for all of mathematics. Every mathematical object—numbers, functions, geometric figures—can be described in terms of sets. In MH1300, we focus on the basic operations on sets and rigorous methods for proving set identities and relationships.

Why this matters: Understanding sets is crucial because:

- Functions are defined as special types of relations, which are sets of ordered pairs
- Probability theory is built on set operations (events are sets)
- Logic and set theory are deeply connected: set operations mirror logical operations
- The element method of proof is used constantly throughout mathematics

Connection to later topics: Relations are sets of ordered pairs. Functions are special relations. Equivalence classes partition sets. All these concepts build directly on the set theory foundation.

4.2 Definitions & Setup

Definition 4.1: Set

A **set** is an unordered collection of distinct objects. The objects in a set are called its **elements** or **members**.
Notation:

- $x \in A$ means "x is an element of A"
- $x \notin A$ means "x is not an element of A"
- $\{a, b, c\}$ is roster notation (list all elements)
- $\{x \mid P(x)\}$ is set-builder notation ("the set of all x such that $P(x)$ is true")

Definition 4.2: Special Sets

- $\varnothing$ or $\{\}$: the **empty set** (contains no elements)
- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$: natural numbers (some texts exclude 0)
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$: integers
- $\mathbb{Q}$: rational numbers
- $\mathbb{R}$: real numbers
- $\mathbb{C}$: complex numbers

Definition 4.3: Subset

Let A and B be sets. We say A is a **subset** of B, written $A \subseteq B$, if every element of A is also an element of B. Formally:

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

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

Remark

Key observations:

- $\varnothing \subseteq A$ for any set A (the empty set is a subset of every set)
- $A \subseteq A$ for any set A (every set is a subset of itself)
- To prove $A = B$, prove both $A \subseteq B$ and $B \subseteq A$ (double inclusion method)

Definition 4.4: Set Operations

Let A and B be sets.
Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
Difference: $A - B = A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$
Complement: If $A \subseteq U$ (universal set), then $A^c = \overline{A} = U - A = \{x \in U \mid x \notin A\}$
Symmetric Difference: $A \triangle B = (A - B) \cup (B - A)$

Example

Let $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$.

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5, 6\} \\ A \cap B &= \{3, 4\} \\ A - B &= \{1, 2\} \\ B - A &= \{5, 6\} \\ A \triangle B &= \{1, 2, 5, 6\} \end{aligned}$$

Definition 4.5: Cartesian Product

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

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

where (a, b) is an **ordered pair**.
Important: $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Example

Let $A = \{1, 2\}$ and $B = \{x, y\}$.

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

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

Note: $A \times B \neq B \times A$ in general (not commutative).

Definition 4.6: Power Set

The **power set** of A, denoted $\mathcal{P}(A)$ or 2^A, is the set of all subsets of A:

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

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

Example

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

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

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

Definition 4.7: Cardinality

For a finite set A, the **cardinality** $|A|$ is the number of elements in A.
Properties:

- $|A \cup B| = |A| + |B| - |A \cap B|$
- If A and B are disjoint ($A \cap B = \varnothing$), then $|A \cup B| = |A| + |B|$
- $|A \times B| = |A| \cdot |B|$
- $|\mathcal{P}(A)| = 2^{|A|}$

4.3 Key Theorems & Results

Theorem 4.1: Set Identity Laws

For any sets A, B, C:

Commutative Laws:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Associative Laws:

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

Distributive Laws:

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

De Morgan's Laws:

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

Identity Laws:

$$A \cup \varnothing = A$$
$$A \cap U = A$$

Domination Laws:

$$A \cup U = U$$
$$A \cap \varnothing = \varnothing$$

Complement Laws:

$$A \cup A^c = U$$
$$A \cap A^c = \varnothing$$
$$(A^c)^c = A$$

Absorption Laws:

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

Set Difference:

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

Remark

Proof Strategy for Set Identities:
To prove $A = B$, use the **element method** (double inclusion):

1. Prove $A \subseteq B$: Let $x \in A$ be arbitrary. Show $x \in B$.
2. Prove $B \subseteq A$: Let $x \in B$ be arbitrary. Show $x \in A$.
3. Conclude $A = B$.

Alternatively, use known set identities to transform one side into the other (like logical equivalences).

4.4 Worked Examples

4.4.1 Tutorial Example: Set Identity Proof

Past Exam Question (AY 24/25 Q4b): Prove Set Identity

Question: Let A, B and C be sets. Prove that

$$(A \cap (A - B)) \cup (A^c \cup B)^c = A - B.$$

Solution (using set identities):

$$\begin{aligned}
&(A \cap (A - B)) \cup (A^c \cup B)^c \\
&= (A \cap (A \cap B^c)) \cup (A^c \cup B)^c && \text{[Set difference: } A - B = A \cap B^c\text{]} \\
&= (A \cap (A \cap B^c)) \cup ((A^c)^c \cap B^c) && \text{[De Morgan's law]} \\
&= (A \cap (A \cap B^c)) \cup (A \cap B^c) && \text{[Double complement]} \\
&= (A \cap B^c) \cup ((A \cap B^c) \cap A) && \text{[Commutativity]} \\
&= A \cap B^c && \text{[Absorption]} \\
&= A - B && \text{[Definition of set difference]}
\end{aligned}$$

Therefore $(A \cap (A - B)) \cup (A^c \cup B)^c = A - B$. □

4.4.2 Past Exam Example: Cartesian Product Identity (Counterexample)

Past Exam Question (AY 22/23 Q2b): Cartesian Product vs Intersection

Question: For sets A, B, C, determine whether

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

Solution:

This statement is **false**. We provide a counterexample.
Let $A = \{1\}$, $B = \{1, 2\}$, $C = \{1\}$.
Then:

$$B \cap C = \{1\}, \quad A \times (B \cap C) = \{1\} \times \{1\} = \{(1, 1)\}.$$

On the other hand:

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

$$(A \times B) \cap C = \{(1, 1), (1, 2)\} \cap \{1\} = \varnothing,$$

since no ordered pair equals the element 1.
Thus $A \times (B \cap C) \neq (A \times B) \cap C$, so the statement is false. □

Common Mistake

Common Error: Students often confuse $(A \times B) \cap C$ with $A \times (B \cap C)$.
The first is the intersection of a *set of ordered pairs* with a set C (usually gives $\varnothing$ unless C contains ordered pairs).
The second is the Cartesian product of A with the intersection $B \cap C$ (always gives a set of ordered pairs).

4.4.3 Past Exam Example: Power Set Inclusion

Past Exam Question (AY 24/25 Q4a): Power Set Inclusion

Question: If X, Y are sets, prove that $\mathcal{P}(X - Y) \setminus \{\varnothing\} \subseteq \mathcal{P}(X) \setminus \mathcal{P}(Y)$.
Give a counterexample to show that equality does not hold in general.

Solution:
Part 1: Prove the inclusion.
Let $A \in \mathcal{P}(X - Y) \setminus \{\varnothing\}$. Then:

- $A \in \mathcal{P}(X - Y)$, so $A \subseteq X - Y$
- $A \notin \{\varnothing\}$, so $A \neq \varnothing$

Since $A \subseteq X - Y \subseteq X$, we have $A \subseteq X$, hence $A \in \mathcal{P}(X)$.
Also, $A \subseteq X - Y$ means that no element of A lies in Y. Therefore A cannot be a subset of Y, so $A \notin \mathcal{P}(Y)$.
Thus $A \in \mathcal{P}(X) \setminus \mathcal{P}(Y)$.
Therefore $\mathcal{P}(X - Y) \setminus \{\varnothing\} \subseteq \mathcal{P}(X) \setminus \mathcal{P}(Y)$. □

Part 2: Counterexample for equality.
Take $X = \{0, 1\}$ and $Y = \{0\}$. Then $X - Y = \{1\}$.

$$\mathcal{P}(X - Y) = \{\varnothing, \{1\}\}, \quad \mathcal{P}(X - Y) \setminus \{\varnothing\} = \{\{1\}\}.$$

$$\mathcal{P}(X) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}, \quad \mathcal{P}(Y) = \{\varnothing, \{0\}\}.$$

$$\mathcal{P}(X) \setminus \mathcal{P}(Y) = \{\{1\}, \{0, 1\}\}.$$

Since $\{\{1\}\} \neq \{\{1\}, \{0, 1\}\}$, equality does not hold. □

4.4.4 Additional Constructed Example: Proving $B \cup C = B \cap C \Rightarrow B = C$

Constructed Example: Union Equals Intersection

Question: Let B and C be sets where $B \cup C = B \cap C$. Prove that $B = C$.

Solution (element method):
We prove both $B \subseteq C$ and $C \subseteq B$.
($B \subseteq C$): Let $x \in B$. Then $x \in B \cup C$. Since $B \cup C = B \cap C$, we have $x \in B \cap C$, so $x \in C$. Thus $B \subseteq C$.
($C \subseteq B$): Let $x \in C$. Then $x \in C \cup B = B \cup C$. Using commutativity and the given equality, $x \in B \cap C$, hence $x \in B$. Thus $C \subseteq B$.
Therefore $B = C$. □

4.5 Common Mistakes & Exam Tips

Common Mistake

Mistake 1: Confusing $\in$ and $\subseteq$
Wrong: $\{1\} \in \{1, 2, 3\}$
Correct: $1 \in \{1, 2, 3\}$ and $\{1\} \subseteq \{1, 2, 3\}$
The element $\{1\}$ is a set, not a member of $\{1, 2, 3\}$ unless we're dealing with sets of sets.

Common Mistake

Mistake 2: Forgetting $\varnothing$ and the set itself in power sets
For any set A, both $\varnothing \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$.
These are often forgotten when listing all elements of a power set.

Common Mistake

Mistake 3: Misapplying distributive laws
Wrong: $A \cup (B \cap C) = (A \cup B) \cap C$
Correct: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
You must distribute A to *both* terms inside the parentheses.

Exam Tip

Exam Strategy for Set Identity Proofs:

1. **Element method:** Show $A \subseteq B$ and $B \subseteq A$ by taking arbitrary elements

2. **Identity method:** Transform one side using known identities until it matches the other
3. **For counterexamples:** Use small, simple sets (often $\varnothing$, $\{0\}$, $\{1\}$, $\{0, 1\}$ suffice)
4. Always write set operations explicitly before manipulating them

Exam Tip

Exam Strategy for Cartesian Products:

- Remember: $(a, b) = (c, d)$ if and only if $a = c$ AND $b = d$
- $A \times B \neq B \times A$ in general (not commutative)
- $|A \times B| = |A| \cdot |B|$
- Be careful with intersections involving Cartesian products — they're sets of different types!

4.6 Topic Summary

Set Theory Quick Reference

Core Definitions:

- $A \subseteq B$: every element of A is in B
- $A \cup B$: elements in A or B (or both)
- $A \cap B$: elements in both A and B
- $A - B = A \cap B^c$: elements in A but not in B
- $A \times B$: set of all ordered pairs (a, b) with $a \in A$, $b \in B$
- $\mathcal{P}(A)$: set of all subsets of A; $|\mathcal{P}(A)| = 2^{|A|}$

Key Identities to Memorize:

$$\begin{aligned}
(A \cup B)^c &= A^c \cap B^c \quad \text{(De Morgan)} \\
(A \cap B)^c &= A^c \cup B^c \quad \text{(De Morgan)} \\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \quad \text{(Distributive)} \\
A \cup (A \cap B) &= A \quad \text{(Absorption)} \\
A - B &= A \cap B^c
\end{aligned}$$

Proof Techniques:

1. **Element method:** Show $A \subseteq B$ and $B \subseteq A$ to prove $A = B$
2. **Identity method:** Transform using known set identities
3. **Counterexample:** For false statements, find specific sets showing inequality

Common Traps:

- Don't confuse $\in$ (element) with $\subseteq$ (subset)
- $\varnothing$ and A are always in $\mathcal{P}(A)$
- $(A \times B) \cap C$ usually makes no sense (different types!)
- Distributive law requires distributing to BOTH terms

5 Relations

5.1 Overview

Relations generalize the concept of "relationship" between elements of sets. Functions, which we study next, are special types of relations. Understanding relations—particularly equivalence relations and partial orders—is fundamental to discrete mathematics, computer science, and abstract algebra.

Why this matters:

- Equivalence relations formalize the notion of "sameness up to some property" (e.g., congruence modulo n, similar triangles)
- Partial orders capture hierarchical structures (e.g., subset relation, divisibility)
- Database operations rely heavily on relational algebra
- Functions are defined as special relations with unique outputs

Connection to later topics: Functions are relations satisfying specific properties. Equivalence relations create partitions, which appear throughout mathematics. Order relations underpin sorting algorithms and data structures.

5.2 Definitions & Setup

Definition 5.1: Binary Relation

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

$$R \subseteq A \times B$$

If $(a, b) \in R$, we write $a \, R \, b$ and say "a is related to b by R".
When $A = B$, we say R is a **relation on** A.

Example

Examples of relations:

- $<$ on $\mathbb{R}$: $(x, y) \in <$ if $x < y$
- Divisibility on $\mathbb{Z}$: $(a, b) \in |$ if $a \mid b$
- Congruence mod n on $\mathbb{Z}$: $(a, b) \in \equiv_n$ if $a \equiv b \pmod{n}$
- "Is a friend of" on a set of people

Definition 5.2: Properties of Relations

Let R be a relation on a set A. Then R is:
Reflexive if $\forall a \in A,\ (a,a) \in R$
Symmetric if $\forall a, b \in A,\ (a,b) \in R \to (b,a) \in R$
Antisymmetric if $\forall a, b \in A,\ ((a,b) \in R \land (b,a) \in R) \to a = b$
Transitive if $\forall a, b, c \in A,\ ((a,b) \in R \land (b,c) \in R) \to (a,c) \in R$

Checking Properties of Relations

Let $A = \{1, 2, 3, 4\}$ and $R = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\}$.

- **Reflexive?** Yes: all (a,a) are present
- **Symmetric?** Yes: $(1,2) \in R$ and $(2,1) \in R$; all pairs have their symmetric counterpart
- **Antisymmetric?** No: $(1,2) \in R$ and $(2,1) \in R$ but $1 \neq 2$
- **Transitive?** Yes: check all combinations (e.g., $(1,2)$ and $(2,1)$ give $(1,1)$, which is in R)

Definition 5.3: Equivalence Relation

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

1. Reflexive
2. Symmetric
3. Transitive

Example

Examples of equivalence relations:

- Equality $(=)$ on any set
- Congruence modulo n on $\mathbb{Z}$
- “Has the same birthday as” on a set of people
- “Is similar to” on the set of triangles

Definition 5.4: Equivalence Class

Let R be an equivalence relation on A. For $a \in A$, the **equivalence class** of a is

$$[a]_R = \{x \in A \mid (a,x) \in R\}$$

The set of all equivalence classes is called the **quotient set** or **partition**:

$$A/R = \{[a]_R \mid a \in A\}$$

Theorem 5.1: Equivalence Classes Form a Partition

If R is an equivalence relation on A, then the equivalence classes of R partition A:

1. Every element $a \in A$ belongs to exactly one equivalence class
2. If $[a]_R \cap [b]_R \neq \varnothing$, then $[a]_R = [b]_R$
3. $\bigcup_{a \in A} [a]_R = A$

Definition 5.5: Partial Order

A relation R on A is a **partial order** if it is:

1. Reflexive
2. Antisymmetric
3. Transitive

If R is a partial order, we often write $\preceq$ instead of R, and $(A, \preceq)$ is called a **partially ordered set** or **poset**.

Example

Examples of partial orders:

- $\leq$ on $\mathbb{R}$
- $\subseteq$ on $\mathcal{P}(A)$ (power set)
- Divisibility $\mid$ on $\mathbb{Z}^+$ (positive integers)

Definition 5.6: Composition of Relations

Let $R \subseteq A \times B$ and $S \subseteq B \times C$. The **composition** $S \circ R$ is defined as:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B,\ (a, b) \in R \wedge (b, c) \in S\}$$

Note: Composition is read *right to left*: $(S \circ R)(a) = S(R(a))$.

Remark

Warning: Relation composition is generally **not commutative**: $S \circ R \neq R \circ S$ in general.

5.3 Worked Examples

5.3.1 Tutorial Example: Non-Commutativity of Composition

Past Exam Question (AY 22/23 Q2c): Relations Don't Commute

Question: If S and R are relations on a set X, is it true that $S \circ R = R \circ S$?

Solution:
This statement is **false**. We provide a counterexample.
Let $X = \{0, 1\}$, $S = \{(0, 1)\}$, and $R = \{(1, 0)\}$.
Computing $S \circ R$:

$$S \circ R = \{(x, z) \in X \times X \mid \exists y \in X,\ (x, y) \in R \wedge (y, z) \in S\}$$

The only element of R is $(1, 0)$. For this to compose with S, we need $(0, z) \in S$ for some z.
Since $S = \{(0, 1)\}$, we have $(1, 0) \in R$ and $(0, 1) \in S$, so $(1, 1) \in S \circ R$.
Thus $S \circ R = \{(1, 1)\}$.
Computing $R \circ S$:

$$R \circ S = \{(x, z) \in X \times X \mid \exists y \in X,\ (x, y) \in S \wedge (y, z) \in R\}$$

The only element of S is $(0, 1)$. We need $(1, z) \in R$ for some z.
Since $R = \{(1, 0)\}$, we have $(0, 1) \in S$ and $(1, 0) \in R$, so $(0, 0) \in R \circ S$.
Thus $R \circ S = \{(0, 0)\}$.
Since $\{(1, 1)\} \neq \{(0, 0)\}$, we have $S \circ R \neq R \circ S$. □

5.3.2 Past Exam Example: Equivalence Relation on $\mathbb{Z}$

Past Exam Question (AY 24/25 Q7): Congruence Modulo 8

Question: Define a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \iff a \equiv b \pmod 8$$

Prove that $\sim$ is an equivalence relation and describe its equivalence classes.

Solution:
We verify the three properties:
Reflexive: For any $a \in \mathbb{Z}$, $a - a = 0 = 8 \cdot 0$, so $8 \mid (a - a)$, hence $a \equiv a \pmod 8$. Thus $a \sim a$.

Symmetric: Suppose $a \sim b$. Then $8 \mid (a-b)$, so $a - b = 8k$ for some $k \in \mathbb{Z}$. Then $b - a = 8(-k)$, so $8 \mid (b-a)$, hence $b \equiv a \pmod 8$. Thus $b \sim a$.
Transitive: Suppose $a \sim b$ and $b \sim c$. Then $8 \mid (a-b)$ and $8 \mid (b-c)$, so $a - b = 8k_1$ and $b - c = 8k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Adding:

$$a - c = (a-b) + (b-c) = 8k_1 + 8k_2 = 8(k_1 + k_2)$$

Thus $8 \mid (a-c)$, so $a \equiv c \pmod 8$, hence $a \sim c$.
Therefore $\sim$ is an equivalence relation. □

Equivalence Classes:
The equivalence classes are the residue classes modulo 8:

$$\begin{aligned}
[0] &= \{\ldots, -16, -8, 0, 8, 16, \ldots\} = \{8k \mid k \in \mathbb{Z}\} \\
[1] &= \{\ldots, -15, -7, 1, 9, 17, \ldots\} = \{8k+1 \mid k \in \mathbb{Z}\} \\
[2] &= \{\ldots, -14, -6, 2, 10, 18, \ldots\} = \{8k+2 \mid k \in \mathbb{Z}\} \\
&\vdots \\
[7] &= \{\ldots, -9, -1, 7, 15, 23, \ldots\} = \{8k+7 \mid k \in \mathbb{Z}\}
\end{aligned}$$

There are exactly 8 equivalence classes: $[0], [1], [2], \ldots, [7]$, and they partition $\mathbb{Z}$. □

5.3.3 Additional Constructed Example: Intersection of Equivalence Relations

Constructed Example (from AY 20/21 Q7a): $E \cap F$ is an Equivalence Relation

Question: Let E and F be equivalence relations on a non-empty set A. Show that $E \cap F$ is an equivalence relation on A.

Solution:
We check the three properties:
Reflexive: Let $a \in A$. Since E and F are equivalence relations, $(a,a) \in E$ and $(a,a) \in F$. Hence $(a,a) \in E \cap F$.
Symmetric: Let $(a,b) \in E \cap F$. Then $(a,b) \in E$ and $(a,b) \in F$. Since E and F are symmetric, $(b,a) \in E$ and $(b,a) \in F$. Thus $(b,a) \in E \cap F$.
Transitive: Let $(a,b) \in E \cap F$ and $(b,c) \in E \cap F$. Then:

- $(a,b) \in E$ and $(b,c) \in E$, so $(a,c) \in E$ (since E is transitive)
- $(a,b) \in F$ and $(b,c) \in F$, so $(a,c) \in F$ (since F is transitive)

Hence $(a,c) \in E \cap F$.
Therefore $E \cap F$ is an equivalence relation on A. □

5.4 Common Mistakes & Exam Tips

Common Mistake

Mistake 1: Confusing antisymmetric with "not symmetric"
A relation can be **both** symmetric and antisymmetric (e.g., equality).
A relation can be **neither** symmetric nor antisymmetric.
Antisymmetric means: if both (a, b) and (b, a) are in R, then $a = b$.
Not symmetric means: there exist $(a, b) \in R$ such that $(b, a) \notin R$.

Common Mistake

Mistake 2: Forgetting to check all three properties for equivalence relations
To prove R is an equivalence relation, you MUST verify:

1. Reflexive
2. Symmetric
3. Transitive

All three are required; two is not enough!

Common Mistake

Mistake 3: Computing composition in the wrong order
$(S \circ R)(a) = S(R(a))$ — apply R first, then S.
Don't confuse this with function composition notation you may have seen elsewhere.

Exam Tip

Exam Strategy for Relation Properties:

1. **Reflexive:** Check if $(a, a) \in R$ for all a
2. **Symmetric:** Check if $(a, b) \in R \Rightarrow (b, a) \in R$
3. **Antisymmetric:** Check if $((a, b) \in R \wedge (b, a) \in R) \Rightarrow a = b$
4. **Transitive:** Check if $((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R$
5. For small finite sets, you can check all pairs explicitly
6. For infinite sets, use the definitions algebraically

Exam Tip

Exam Strategy for Equivalence Relations:

- To find equivalence classes, pick a representative from each class
- For congruence mod n, there are exactly n equivalence classes: $[0], [1], \ldots, [n-1]$
- Equivalence classes partition the set (disjoint and cover everything)
- $[a] = [b]$ if and only if $a \sim b$

5.5 Topic Summary

Relations Quick Reference

Core Definitions:

- Binary relation R from A to B: $R \subseteq A \times B$
- $(a, b) \in R$ written as $a \; R \; b$
- Reflexive: $\forall a, (a, a) \in R$
- Symmetric: $(a, b) \in R \Rightarrow (b, a) \in R$
- Antisymmetric: $((a, b) \in R \wedge (b, a) \in R) \Rightarrow a = b$
- Transitive: $((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R$

Special Relations:

- **Equivalence relation:** reflexive + symmetric + transitive
- **Partial order:** reflexive + antisymmetric + transitive
- Equivalence class: $[a]_R = \{x \in A \mid a \; R \; x\}$
- Equivalence classes partition the set

Composition:

$$S \circ R = \{(a, c) \mid \exists b, (a, b) \in R \wedge (b, c) \in S\}$$

Generally $S \circ R \neq R \circ S$ (not commutative).

Common Equivalence Relations:

- Equality $(=)$
- Congruence mod n: $a \equiv b \pmod{n}$ iff $n \mid (a - b)$

Proof Tips:

- To prove equivalence relation: check all 3 properties
- For counterexamples: use small finite sets
- Composition: trace through step by step

6 Functions

6.1 Overview

Functions are among the most important objects in mathematics. They formalize the notion of assigning to each input exactly one output. Functions appear everywhere: in calculus (derivatives, integrals), in algebra (homomorphisms), in computer science (algorithms, programs), and in daily life (temperature as a function of time).

Why this matters:

- Functions are the primary way we model relationships between quantities
- Understanding injective, surjective, and bijective functions is crucial for counting, cryptography, and invertibility
- Composition of functions mirrors function composition in programming
- Image and preimage operations are fundamental in topology and analysis

Connection to later topics: Functions are special relations. Bijective functions establish one-to-one correspondences used in cardinality arguments. Inverse functions are central to solving equations. Composition connects to group theory and category theory.

6.2 Definitions & Setup

Definition 6.1: Function

A **function** f from set A to set B, written $f : A \to B$, is a relation from A to B such that:

$$\forall a \in A,\ \exists! b \in B,\ (a, b) \in f$$

That is, every element of A is related to *exactly one* element of B.

Terminology:

- A is the **domain** of f
- B is the **codomain** of f
- For $(a, b) \in f$, we write $f(a) = b$; b is the **image** of a
- The **range** of f is $\{f(a) \mid a \in A\} \subseteq B$

Remark

Key distinction: The **codomain** is the set B specified in the definition $f : A \to B$.
The **range** is the set of actual outputs: $\{f(a) \mid a \in A\}$.
In general, range $\subseteq$ codomain, with equality when f is surjective.

Definition 6.2: Injective (One-to-One)

A function $f : A \to B$ is **injective** (or **one-to-one**) if distinct inputs produce distinct outputs:

$$\forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \to a_1 = a_2$$

Equivalently (contrapositive):

$$\forall a_1, a_2 \in A,\ a_1 \neq a_2 \to f(a_1) \neq f(a_2)$$

Injective Function

$f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 3$ is injective.
Proof: Suppose $f(a) = f(b)$. Then:

$$2a + 3 = 2b + 3 \quad \Rightarrow \quad 2a = 2b \quad \Rightarrow \quad a = b$$

Thus f is injective. □

Non-Injective Function

$g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ is **not** injective.
Counterexample: $g(2) = 4 = g(-2)$, but $2 \neq -2$. □

Definition 6.3: Surjective (Onto)

A function $f : A \to B$ is **surjective** (or **onto**) if every element of the codomain is an output:

$$\forall b \in B,\ \exists a \in A,\ f(a) = b$$

Equivalently, the range equals the codomain.

Surjective Function

$f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 3$ is surjective.
Proof: Let $b \in \mathbb{R}$ be arbitrary. We need $a \in \mathbb{R}$ such that $f(a) = b$.
Solving: $2a + 3 = b \Rightarrow a = \frac{b-3}{2} \in \mathbb{R}$.
Then $f(a) = 2 \cdot \frac{b-3}{2} + 3 = b - 3 + 3 = b$.
Thus f is surjective. □

Non-Surjective Function

$h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = x^2$ is **not** surjective.
Counterexample: $-1 \in \mathbb{R}$ (codomain), but there is no $x \in \mathbb{R}$ with $x^2 = -1$. □

Definition 6.4: Bijective (One-to-One Correspondence)

A function $f : A \to B$ is **bijective** if it is both injective and surjective.
Bijective functions establish a **one-to-one correspondence** between A and B.

Example

$f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 3$ is bijective (both injective and surjective, as shown above).

Definition 6.5: Composition of Functions

Let $f : A \to B$ and $g : B \to C$. The **composition** $g \circ f : A \to C$ is defined by:

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

Read: "g of f of a" — apply f first, then g.

Theorem 6.1: Properties of Composition

1. If f and g are both injective, then $g \circ f$ is injective.
2. If f and g are both surjective, then $g \circ f$ is surjective.
3. If f and g are both bijective, then $g \circ f$ is bijective.

Definition 6.6: Inverse Function

Let $f : A \to B$ be bijective. The **inverse function** $f^{-1} : B \to A$ is defined by:

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

Properties:

- $(f^{-1} \circ f)(a) = a$ for all $a \in A$
- $(f \circ f^{-1})(b) = b$ for all $b \in B$

Remark

Warning: The notation f^{-1} has two meanings:

1. **Inverse function** (only exists if f is bijective)
2. **Preimage** (exists for any function, defined below)

Context determines which is meant.

Definition 6.7: Image and Preimage

Let $f : A \to B$.
Image of a set: For $X \subseteq A$,

$$f(X) = \{f(a) \mid a \in X\} = \{b \in B \mid \exists a \in X, f(a) = b\}$$

Preimage of a set: For $Y \subseteq B$,

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

Remark

Important: $f^{-1}(Y)$ (preimage) exists for *any* function f, even if f is not bijective!

6.3 Worked Examples

6.3.1 Tutorial Example: Checking Injective and Surjective

Past Exam Question (AY 21/22 Q5b): $g(n) = 2n \bmod 3$

Question: Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(n) = 2n \bmod 3$.

(i) Is g injective?

(ii) Is g surjective?

(iii) What is the range of g?

Solution:
First, we understand g. For any $n \in \mathbb{Z}$:

$$g(n) = 2n \bmod 3 \in \{0, 1, 2\}$$

Specifically:

$$\begin{aligned} g(0) &= 0 \bmod 3 = 0 \\ g(1) &= 2 \bmod 3 = 2 \\ g(2) &= 4 \bmod 3 = 1 \\ g(3) &= 6 \bmod 3 = 0 \end{aligned}$$

(i) Is g injective?
No. We have $g(0) = 0 = g(3)$, but $0 \neq 3$.
Thus g is not injective. □
(ii) Is g surjective?
No. The codomain is $\mathbb{Z}$, but the range is $\{0, 1, 2\}$.

For example, $3 \in \mathbb{Z}$, but there is no $n \in \mathbb{Z}$ with $g(n) = 3$ (since $g(n) \in \{0, 1, 2\}$ always).
Thus g is not surjective. $\square$
(iii) What is the range of g?
The range of g is $\{0, 1, 2\}$, as shown by the calculations above. $\square$

6.3.2 Past Exam Example: Image and Preimage Inclusion

Past Exam Question (AY 21/22 Q5a): $f(f^{-1}(Y)) \subseteq Y$ and $X \subseteq f^{-1}(f(X))$

Question: Let $f : A \to B$ be a function, $X \subseteq A$, and $Y \subseteq B$. Prove:

(1) $f(f^{-1}(Y)) \subseteq Y$

(2) $X \subseteq f^{-1}(f(X))$

Solution:
(1) Prove $f(f^{-1}(Y)) \subseteq Y$:
Let $y \in f(f^{-1}(Y))$. By definition of image, there exists $a \in f^{-1}(Y)$ such that $y = f(a)$.
Since $a \in f^{-1}(Y)$, by definition of preimage, $f(a) \in Y$.
Thus $y = f(a) \in Y$.
Therefore $f(f^{-1}(Y)) \subseteq Y$. $\square$

(2) Prove $X \subseteq f^{-1}(f(X))$:
Let $x \in X$. Then $f(x) \in f(X)$ (by definition of image).
By definition of preimage, $x \in f^{-1}(f(X))$ (since $f(x) \in f(X)$).
Therefore $X \subseteq f^{-1}(f(X))$. $\square$

Remark

Note: In general, $f(f^{-1}(Y)) \subsetneq Y$ (strict inequality). Equality holds if and only if Y is contained in the range of f.
Similarly, $X \subsetneq f^{-1}(f(X))$ in general. Equality holds if and only if f is injective (restricted to X).

6.3.3 Additional Constructed Example: Composition Surjectivity

Constructed Example (from AY 20/21 Q6b): Composition of Surjective Functions

Question: Let $f : A \to B$ and $g : B \to C$ be surjective functions. Prove that $g \circ f : A \to C$ is surjective.

Solution:
Let $c \in C$ be arbitrary. We must find $a \in A$ such that $(g \circ f)(a) = c$.

Since g is surjective, there exists $b \in B$ such that $g(b) = c$.
Since f is surjective, there exists $a \in A$ such that $f(a) = b$.
Then:

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Thus every $c \in C$ is in the range of $g \circ f$, so $g \circ f$ is surjective. □

6.4 Common Mistakes & Exam Tips

Common Mistake

Mistake 1: Confusing injective and surjective
Injective: different inputs → different outputs (one-to-one)
Surjective: every output is achieved (onto)
To disprove injective: find two different inputs with the same output.
To disprove surjective: find an element of the codomain that is not an output.

Common Mistake

Mistake 2: Forgetting the difference between range and codomain
The **codomain** is part of the definition: $f : A \to B$ has codomain B.
The **range** is the set of actual outputs: $\{f(a) \mid a \in A\}$.
f is surjective $\iff$ range = codomain.

Common Mistake

Mistake 3: Confusing f^{-1} (inverse function) with f^{-1} (preimage)
Inverse function: only exists if f is bijective; maps $B \to A$.
Preimage: exists for any function; maps subsets of B to subsets of A.
Context determines which is meant!

Exam Tip

Exam Strategy for Proving Injective:
Method 1 (Direct): Assume $f(a_1) = f(a_2)$. Show $a_1 = a_2$ through algebraic manipulation.
Method 2 (Contrapositive): Assume $a_1 \neq a_2$. Show $f(a_1) \neq f(a_2)$.
To disprove: Find one counterexample where $f(a_1) = f(a_2)$ but $a_1 \neq a_2$.

Exam Tip

Exam Strategy for Proving Surjective:
Method: Let $b \in B$ be arbitrary. Construct (or show existence of) $a \in A$ such that $f(a) = b$.
Often this involves solving $f(a) = b$ for a.

To disprove: Find one element $b \in B$ (codomain) that is not in the range.

Exam Tip

Exam Strategy for Composition:

- $(g \circ f)(a) = g(f(a))$ — apply f first, then g
- If both injective, composition is injective
- If both surjective, composition is surjective
- Composition is generally not commutative: $g \circ f \neq f \circ g$

6.5 Topic Summary

Functions Quick Reference

Core Definitions:

- Function $f : A \to B$: each $a \in A$ maps to exactly one $b \in B$
- Domain: A; Codomain: B; Range: $\{f(a) \mid a \in A\} \subseteq B$
- Injective: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ (one-to-one)
- Surjective: $\forall b \in B, \exists a \in A, f(a) = b$ (onto)
- Bijective: both injective and surjective

Image and Preimage:

$$f(X) = \{f(a) \mid a \in X\} \quad (X \subseteq A)$$
$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\} \quad (Y \subseteq B)$$

Key Properties:

- $f(f^{-1}(Y)) \subseteq Y$ (equality iff $Y \subseteq \text{range}(f)$)
- $X \subseteq f^{-1}(f(X))$ (equality iff f is injective on X)
- Composition: $(g \circ f)(a) = g(f(a))$
- If f, g both injective/surjective/bijective, so is $g \circ f$

Inverse Function:

- Exists iff f is bijective
- $f^{-1}(f(a)) = a$ and $f(f^{-1}(b)) = b$

Proof Strategies:

- Injective: assume $f(a_1) = f(a_2)$, prove $a_1 = a_2$
- Surjective: for arbitrary $b \in B$, construct a with $f(a) = b$
- To disprove: give one counterexample

7 Mathematical Induction

7.1 Overview

Mathematical induction is one of the most powerful proof techniques in discrete mathematics and number theory. It allows us to prove statements about all natural numbers (or integers beyond a certain point) by establishing a base case and showing that truth ”propagates” from one integer to the next.

Why this matters:

- Induction is essential for proving formulas for sums, products, and recursive sequences
- It’s the foundation for proving correctness of recursive algorithms
- Strong induction extends the technique to problems involving recurrence relations
- The well-ordering principle (equivalent to induction) underpins many fundamental theorems

Connection to later topics: Induction appears throughout computer science (loop invariants, algorithm correctness), combinatorics (counting arguments), and analysis (proving inequalities). It’s closely related to recursive thinking.

7.2 Definitions & Setup

Definition 7.1: Principle of Mathematical Induction (Weak Form)

Let $P(n)$ be a statement about integers $n \geq n_0$. To prove $P(n)$ is true for all $n \geq n_0$:
Step 1 (Base Case): Prove $P(n_0)$ is true.
Step 2 (Inductive Step): Assume $P(k)$ is true for some arbitrary $k \geq n_0$ (the **inductive hypothesis**). Prove that $P(k+1)$ is true.
Conclusion: By the principle of mathematical induction, $P(n)$ is true for all $n \geq n_0$.

Remark

Intuition: Think of dominoes standing in a line.

- **Base case:** The first domino falls
- **Inductive step:** If any domino falls, the next one falls
- **Conclusion:** All dominoes fall

The inductive step is like proving: ”For any domino k, if domino k falls, then domino $k+1$ falls.”

Definition 7.2: Principle of Strong Induction

Let $P(n)$ be a statement about integers $n \geq n_0$. To prove $P(n)$ is true for all $n \geq n_0$:
Step 1 (Base Cases): Prove $P(n_0), P(n_0+1), \dots, P(n_0+m)$ are true (as many base cases as needed).
Step 2 (Strong Inductive Step): Assume $P(n_0), P(n_0+1), \dots, P(k)$ are all true for some arbitrary $k \geq n_0+m$ (the **strong inductive hypothesis**). Prove that $P(k+1)$ is true.
Conclusion: By strong mathematical induction, $P(n)$ is true for all $n \geq n_0$.

Remark

Difference from weak induction:
Weak induction: Assume only $P(k)$ to prove $P(k+1)$
Strong induction: Assume $P(n_0), P(n_0+1), \dots, P(k)$ (all previous cases) to prove $P(k+1)$
Strong induction is useful when $P(k+1)$ depends on multiple previous values, such as in recurrence relations.

7.3 Proof Templates

7.3.1 Template for Weak Induction

Weak Induction Template

Statement: For all $n \geq n_0$, $P(n)$ holds.
Proof by Mathematical Induction:
Let $P(n)$ denote the statement: [write explicit statement].
Base case ($n = n_0$):
[Verify $P(n_0)$ directly by computation.]
Thus $P(n_0)$ is true.
Inductive step:
Assume $P(k)$ is true for some $k \geq n_0$. That is, assume [state $P(k)$ explicitly].
We prove $P(k+1)$ is true, i.e., [state $P(k+1)$ explicitly].
[Use the inductive hypothesis to prove $P(k+1)$.]
Thus $P(k+1)$ holds.
Conclusion:
By the principle of mathematical induction, $P(n)$ is true for all $n \geq n_0$. □

7.3.2 Template for Strong Induction

Strong Induction Template

Statement: For all $n \geq n_0$, $P(n)$ holds.
Proof by Strong Induction:
Let $P(n)$ denote the statement: [write explicit statement].
Base cases:
[Verify $P(n_0), P(n_0+1), \ldots$ as needed.]
Inductive step (strong form):
Assume $P(n_0), P(n_0+1), \ldots, P(k)$ are all true for some $k \geq [\textit{threshold}]$. That is, assume [state assumptions explicitly].
We prove $P(k+1)$ is true.
[Use one or more of the previous cases $P(n_0), \ldots, P(k)$ to prove $P(k+1)$.]
Thus $P(k+1)$ holds.
Conclusion:
By strong mathematical induction, $P(n)$ is true for all $n \geq n_0$. □

7.4 Worked Examples

7.4.1 Tutorial Example: Summation Formula

Past Exam Question (AY 24/25 Q3a): Summation Identity

Question: Use mathematical induction to prove that for every integer $n \geq 1$,

$$\sum_{j=1}^{3n} j(j-1) = n(9n^2-1).$$

Solution:
Let $P(n)$ denote the statement

$$\sum_{j=1}^{3n} j(j-1) = n(9n^2-1), \quad n \geq 1.$$

Base case ($n = 1$):

$$\text{LHS} = \sum_{j=1}^{3} j(j-1) = 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 2 = 0 + 2 + 6 = 8$$
$$\text{RHS} = 1 \cdot (9 \cdot 1^2 - 1) = 9 - 1 = 8$$

So $P(1)$ is true.
Inductive step:

Assume $P(k)$ is true for some $k \geq 1$, i.e.,

$$\sum_{j=1}^{3k} j(j-1) = k(9k^2-1).$$

We prove $P(k+1)$:

$$\begin{aligned}
\sum_{j=1}^{3(k+1)} j(j-1) &= \sum_{j=1}^{3k+3} j(j-1) \\
&= \sum_{j=1}^{3k} j(j-1) + (3k+1)(3k) + (3k+2)(3k+1) + (3k+3)(3k+2) \\
&= k(9k^2-1) + (3k+1)(3k) + (3k+2)(3k+1) + (3k+3)(3k+2) \\
&\qquad\qquad\qquad\qquad [\text{by inductive hypothesis}]
\end{aligned}$$

Now we simplify the three new terms:

$$\begin{aligned}
&(3k+1)(3k) + (3k+2)(3k+1) + (3k+3)(3k+2) \\
&= (3k+1)\cdot 3k + (3k+2)(3k+1+3k+3) \\
&= (3k+1)\cdot 3k + (3k+2)(6k+4) \\
&= 9k^2 + 3k + 18k^2 + 12k + 12k + 8 \\
&= 27k^2 + 27k + 8
\end{aligned}$$

Thus:

$$\begin{aligned}
\sum_{j=1}^{3k+3} j(j-1) &= k(9k^2-1) + 27k^2 + 27k + 8 \\
&= 9k^3 - k + 27k^2 + 27k + 8 \\
&= 9k^3 + 27k^2 + 26k + 8
\end{aligned}$$

We need this to equal $(k+1)(9(k+1)^2-1)$. Let's compute the RHS for $n = k+1$:

$$\begin{aligned}
(k+1)(9(k+1)^2-1) &= (k+1)(9(k^2+2k+1)-1) \\
&= (k+1)(9k^2+18k+9-1) \\
&= (k+1)(9k^2+18k+8) \\
&= 9k^3 + 18k^2 + 8k + 9k^2 + 18k + 8 \\
&= 9k^3 + 27k^2 + 26k + 8
\end{aligned}$$

This matches our LHS, so $P(k+1)$ is true.
Conclusion:

By mathematical induction, $\displaystyle\sum_{j=1}^{3n} j(j-1) = n(9n^2-1)$ for all $n \geq 1$. □

7.4.2 Past Exam Example: Divisibility

Past Exam Question (AY 21/22 Q3b): Divisibility by 21

Question: Prove that for every positive integer m,

$$4^{m+1} + 5^{2m-1}$$

is divisible by 21.

Solution by Induction:
Let $P(m)$ be the statement: $21 \mid (4^{m+1} + 5^{2m-1})$ for $m \geq 1$.
Base case ($m = 1$):

$$4^{1+1} + 5^{2\cdot 1-1} = 4^2 + 5^1 = 16 + 5 = 21$$

Since $21 = 21 \cdot 1$, we have $21 \mid 21$. Thus $P(1)$ is true.
Inductive step:
Assume $P(k)$ is true for some $k \geq 1$. Then there exists an integer x such that

$$4^{k+1} + 5^{2k-1} = 21x.$$

Consider $P(k+1)$:

$$\begin{aligned}
4^{(k+1)+1} + 5^{2(k+1)-1} &= 4^{k+2} + 5^{2k+1} \\
&= 4 \cdot 4^{k+1} + 25 \cdot 5^{2k-1} \\
&= 4 \cdot 4^{k+1} + 4 \cdot 5^{2k-1} + 21 \cdot 5^{2k-1} \\
&= 4(4^{k+1} + 5^{2k-1}) + 21 \cdot 5^{2k-1} \\
&= 4 \cdot 21x + 21 \cdot 5^{2k-1} \qquad \text{[by inductive hypothesis]} \\
&= 21(4x + 5^{2k-1})
\end{aligned}$$

Since $4x + 5^{2k-1} \in \mathbb{Z}$, we have $21 \mid (4^{k+2} + 5^{2k+1})$. Thus $P(k+1)$ is true.
Conclusion:
By mathematical induction, $4^{m+1} + 5^{2m-1}$ is divisible by 21 for all positive integers m.
□

7.4.3 Past Exam Example: Strong Induction on Recurrence

Past Exam Question (AY 22/23 Q3b): Strong Induction on Recurrence Relation

Question: Define the sequence $\{a_n\}_{n=0}^{\infty}$ by $a_0 = 1$, $a_1 = 2$, $a_2 = 3$ and

$$a_n = a_{n-1} + 3a_{n-3} + 1 \quad \text{for all } n \geq 3.$$

Prove that $a_n \leq 2^n$ for all $n \geq 0$.

Solution by Strong Induction:

Let $P(n)$ be the statement: $a_n \leq 2^n$.
Base cases:

$$\begin{aligned} P(0): &\quad a_0 = 1 \leq 2^0 = 1 \quad \checkmark \\ P(1): &\quad a_1 = 2 \leq 2^1 = 2 \quad \checkmark \\ P(2): &\quad a_2 = 3 \leq 2^2 = 4 \quad \checkmark \end{aligned}$$

Inductive step (strong form):
Assume $P(0), P(1), \dots, P(k-1)$ all hold for some $k \geq 3$. That is,

$$a_j \leq 2^j \quad \text{for } j = 0, 1, \dots, k-1.$$

We prove $P(k)$. From the recurrence relation:

$$a_k = a_{k-1} + 3a_{k-3} + 1$$

By the inductive hypothesis applied to $k-1$ and $k-3$ (both $< k$):

$$a_k \leq 2^{k-1} + 3 \cdot 2^{k-3} + 1$$

Now simplify:

$$3 \cdot 2^{k-3} = 2^{k-2} + 2^{k-3}$$

so

$$a_k \leq 2^{k-1} + 2^{k-2} + 2^{k-3} + 1$$

Since $k \geq 3$, we have $1 \leq 2^{k-3}$, hence:

$$a_k \leq 2^{k-1} + 2^{k-2} + 2^{k-3} + 2^{k-3} = 2^{k-3}(4 + 2 + 1 + 1) = 2^{k-3} \cdot 8 = 2^k$$

Thus $P(k)$ holds.
Conclusion:
By strong mathematical induction, $a_n \leq 2^n$ for all $n \geq 0$. □

7.4.4 Additional Constructed Example: Factorial Inequality

Constructed Example: Proving $2^n \leq n!$ for $n \geq 4$

Question: Prove that $2^n \leq n!$ for all integers $n \geq 4$.

Solution:
Let $P(n)$ be the statement: $2^n \leq n!$ for $n \geq 4$.
Base case ($n = 4$):

$$2^4 = 16, \quad 4! = 24, \quad 16 \leq 24 \quad \checkmark$$

Inductive step:
Assume $P(k)$ is true for some $k \geq 4$, i.e., $2^k \leq k!$.

Consider $P(k+1)$:

$$2^{k+1} = 2 \cdot 2^k \leq 2 \cdot k! \quad \text{[by inductive hypothesis]}$$

Since $k \geq 4$, we have $k+1 \geq 5 > 2$, so:

$$2 \cdot k! < (k+1) \cdot k! = (k+1)!$$

Therefore $2^{k+1} < (k+1)!$, so $P(k+1)$ holds.
Conclusion:
By mathematical induction, $2^n \leq n!$ for all $n \geq 4$. □

7.5 Common Mistakes & Exam Tips

Common Mistake

Mistake 1: Not stating $P(n)$ explicitly
You MUST write down what $P(n)$ is at the start of your proof. This clarifies exactly what you're proving.
Wrong: "We prove by induction..."
Correct: "Let $P(n)$ denote the statement: [explicit formula/claim]."

Common Mistake

Mistake 2: Forgetting to verify the base case
The base case is NOT optional! Even if it seems trivial, you must verify it explicitly. Without the base case, the dominoes never start falling!

Common Mistake

Mistake 3: Not using the inductive hypothesis
In the inductive step, you MUST use the assumption that $P(k)$ is true.
If your proof of $P(k+1)$ doesn't use $P(k)$, you're not doing induction correctly!

Common Mistake

Mistake 4: Using weak induction when strong induction is needed
If the recurrence relation depends on multiple previous terms (e.g., $a_n = a_{n-1} + a_{n-3}$), you need **strong induction**, not weak induction.
Weak induction only gives you $P(k)$; strong induction gives you $P(0), P(1), \ldots, P(k)$.

Exam Tip

Exam Strategy for Induction Proofs:

1. **Clearly state** $P(n)$ at the beginning
2. **Verify the base case(s)** explicitly by direct computation
3. **State the inductive hypothesis** clearly: ”Assume $P(k)$ is true for some $k \geq n_0$...”
4. **State what you need to prove**: ”We prove $P(k+1)$...”
5. **Use the inductive hypothesis** explicitly in your derivation
6. **Conclude** by citing the principle of mathematical induction

Exam Tip

When to Use Strong Induction:

- Recurrence relations with multiple previous terms (e.g., Fibonacci: $F_n = F_{n-1} + F_{n-2}$)
- Proving statements about divisibility or factorization
- Problems involving the Fundamental Theorem of Arithmetic
- Any situation where $P(k+1)$ naturally depends on multiple previous cases, not just $P(k)$

7.6 Topic Summary

Mathematical Induction Quick Reference

Weak Induction:

1. Base case: Verify $P(n_0)$
2. Inductive step: Assume $P(k)$, prove $P(k+1)$
3. Conclusion: $P(n)$ true for all $n \geq n_0$

Strong Induction:

1. Base cases: Verify $P(n_0), P(n_0+1), \ldots$
2. Inductive step: Assume $P(n_0), \ldots, P(k)$, prove $P(k+1)$
3. Conclusion: $P(n)$ true for all $n \geq n_0$

Common Applications:

- Summation formulas: $\displaystyle\sum_{i=1}^{n} f(i) = g(n)$
- Divisibility: $d \mid f(n)$ for all $n \geq n_0$
- Inequalities: $f(n) \leq g(n)$ for all $n \geq n_0$
- Recurrence relations: a_n satisfies certain bounds

Critical Steps:

- **Always** state $P(n)$ explicitly
- **Always** verify base case(s)
- **Always** use the inductive hypothesis in the inductive step
- **Always** conclude by citing the principle of induction

Common Traps:

- Forgetting base case
- Not using inductive hypothesis
- Using weak induction when strong is needed
- Circular reasoning (assuming what you want to prove)

8 Complex Numbers and Roots of Unity

8.1 Overview

Complex numbers extend the real numbers to include solutions to equations like $x^2 + 1 = 0$. In MH1300, we focus on the polar (exponential) form of complex numbers and finding nth roots, particularly roots of unity.

Why this matters:

- Complex numbers are essential in electrical engineering, signal processing, and quantum mechanics
- Polar form simplifies multiplication, division, and exponentiation
- Roots of unity have deep connections to group theory, Fourier analysis, and cyclotomic polynomials
- De Moivre's theorem is a powerful tool for computing powers and roots

Connection to later topics: Complex exponentials underpin Fourier transforms. Roots of unity form cyclic groups in abstract algebra. The geometry of complex numbers connects to linear algebra and differential equations.

8.2 Definitions & Setup

Definition 8.1: Complex Numbers

A **complex number** is a number of the form

$$z = a + bi$$

where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$ (i.e., $i^2 = -1$).
Terminology:

- $a = \text{Re}(z)$ is the **real part**
- $b = \text{Im}(z)$ is the **imaginary part**
- If $b = 0$, z is real; if $a = 0$ and $b \neq 0$, z is **purely imaginary**

Definition 8.2: Polar (Exponential) Form

Any complex number $z = a + bi$ can be written in **polar form**:

$$z = re^{i\theta} = r(\cos\theta + i\sin\theta)$$

where:

- $r = |z| = \sqrt{a^2 + b^2}$ is the **modulus** (or absolute value)

- $\theta = \arg(z)$ is the **argument** (or angle), with $-\pi < \theta \leq \pi$

Conversion formulas:

$$\begin{aligned} a &= r\cos\theta \\ b &= r\sin\theta \\ r &= \sqrt{a^2+b^2} \\ \theta &= \begin{cases} \arctan(b/a) & \text{if } a > 0 \\ \arctan(b/a) + \pi & \text{if } a < 0, b \geq 0 \\ \arctan(b/a) - \pi & \text{if } a < 0, b < 0 \\ \pi/2 & \text{if } a = 0, b > 0 \\ -\pi/2 & \text{if } a = 0, b < 0 \end{cases} \end{aligned}$$

Theorem 8.1: De Moivre's Theorem

If $z = re^{i\theta}$, then for any integer n:

$$z^n = r^n e^{in\theta} = r^n(\cos(n\theta) + i\sin(n\theta))$$

Definition 8.3: nth Roots

The n**th roots** of a complex number $w = \rho e^{i\alpha}$ are:

$$z_k = \rho^{1/n} e^{i(\alpha+2\pi k)/n}, \quad k = 0, 1, 2, \ldots, n-1$$

There are exactly n distinct nth roots.

Definition 8.4: Roots of Unity

The n**th roots of unity** are the solutions to $z^n = 1$:

$$z_k = e^{2\pi ik/n}, \quad k = 0, 1, 2, \ldots, n-1$$

These are equally spaced around the unit circle in the complex plane.

8.3 Worked Examples

8.3.1 Tutorial Example: Finding nth Roots

Past Exam Question (AY 21/22 Q6a): Sixth Roots of Unity

Question: Find all sixth roots of unity. That is, find all complex numbers z satisfying $z^6 - 1 = 0$. Leave your answer in terms of $re^{i\theta}$.

Solution:
We need to solve $z^6 = 1$.
Write 1 in polar form: $1 = e^{i\cdot 0}$ (modulus $r = 1$, argument $\theta = 0$).
Using the nth root formula with $n = 6$, $\rho = 1$, $\alpha = 0$:

$$z_k = 1^{1/6} e^{i(0+2\pi k)/6} = e^{i\pi k/3}, \quad k = 0, 1, 2, 3, 4, 5$$

Thus the six roots are:

$$\begin{aligned}
z_0 &= e^{i\cdot 0} = 1 \\
z_1 &= e^{i\pi/3} \\
z_2 &= e^{i2\pi/3} \\
z_3 &= e^{i\pi} = -1 \\
z_4 &= e^{i4\pi/3} \\
z_5 &= e^{i5\pi/3}
\end{aligned}$$

These are the six sixth roots of unity, equally spaced around the unit circle with angular separation $\pi/3$ (or 60). □

8.3.2 Past Exam Example: Fifth Roots of a Complex Number

Past Exam Question (AY 22/23 Q6): Fifth Roots of Complex Number

Question: Find all fifth roots of $32i$ in polar form.

Solution:
First, write $32i$ in polar form.
Modulus: $|32i| = 32$
Argument: Since $32i = 0 + 32i$, we have $a = 0$, $b = 32 > 0$, so $\arg(32i) = \pi/2$.
Thus $32i = 32e^{i\pi/2}$.
Using the nth root formula with $n = 5$, $\rho = 32$, $\alpha = \pi/2$:

$$z_k = 32^{1/5} e^{i(\pi/2+2\pi k)/5}, \quad k = 0, 1, 2, 3, 4$$

Since $32 = 2^5$, we have $32^{1/5} = 2$.

Thus:

$$\begin{aligned} z_0 &= 2e^{i\pi/10} \\ z_1 &= 2e^{i(\pi/2+2\pi)/5} = 2e^{i\pi/2} \cdot e^{i2\pi/5} = 2e^{i(\pi/2+2\pi/5)} = 2e^{i9\pi/10} \\ z_2 &= 2e^{i(\pi/2+4\pi)/5} = 2e^{i17\pi/10} \\ z_3 &= 2e^{i(\pi/2+6\pi)/5} = 2e^{i5\pi/2} = 2e^{i\pi/2} \quad \text{(reducing mod } 2\pi) \\ z_4 &= 2e^{i(\pi/2+8\pi)/5} = 2e^{i33\pi/10} \end{aligned}$$

Actually, let's compute more carefully:

$$z_k = 2e^{i(\pi+4\pi k)/10} = 2e^{i\pi(1+4k)/10}, \quad k = 0, 1, 2, 3, 4$$

So:

$$\begin{aligned} z_0 &= 2e^{i\pi/10} \\ z_1 &= 2e^{i5\pi/10} = 2e^{i\pi/2} \\ z_2 &= 2e^{i9\pi/10} \\ z_3 &= 2e^{i13\pi/10} \\ z_4 &= 2e^{i17\pi/10} \end{aligned}$$

These are the five fifth roots of $32i$, each with modulus 2, equally spaced around a circle of radius 2. □

8.4 Common Mistakes & Exam Tips

Common Mistake

Mistake 1: Forgetting all n roots
The equation $z^n = w$ has **exactly** n complex solutions (counting multiplicity).
Don't just find one root and stop! Use the formula with $k = 0, 1, \ldots, n-1$.

Common Mistake

Mistake 2: Incorrect argument calculation
The argument θ must be in the range $-\pi < \theta \leq \pi$ (or $0 \leq \theta < 2\pi$, depending on convention).
Be careful with the quadrant when computing $\arctan(b/a)$!

Common Mistake

Mistake 3: Not simplifying the modulus
If $w = 32 = 2^5$, then $w^{1/5} = 2$, not $32^{1/5}$ left unsimplified.

Always simplify perfect nth powers.

Exam Tip

Exam Strategy for Finding nth Roots:

1. **Convert to polar form:** Write $w = \rho e^{i\alpha}$ (find ρ and α)
2. **Apply the formula:** $z_k = \rho^{1/n} e^{i(\alpha+2\pi k)/n}$ for $k = 0, 1, \ldots, n-1$
3. **Simplify:** Compute $\rho^{1/n}$ explicitly if possible; simplify angles
4. **List all n roots** clearly

Exam Tip

Special Case: Roots of Unity
For $z^n = 1$ (roots of unity):

$$z_k = e^{2\pi i k/n}, \quad k = 0, 1, \ldots, n-1$$

These lie on the unit circle, equally spaced with angular separation $2\pi/n$.

8.5 Topic Summary

Complex Numbers Quick Reference

Forms:

- Rectangular: $z = a + bi$
- Polar: $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$
- Conversion: $r = \sqrt{a^2 + b^2}$, $\theta = \arg(z)$

De Moivre's Theorem:

$$(re^{i\theta})^n = r^n e^{in\theta}$$

nth Roots of $w = \rho e^{i\alpha}$:

$$z_k = \rho^{1/n} e^{i(\alpha + 2\pi k)/n}, \quad k = 0, 1, \ldots, n-1$$

nth Roots of Unity ($z^n = 1$):

$$z_k = e^{2\pi i k/n}, \quad k = 0, 1, \ldots, n-1$$

Key Facts:

- There are exactly n distinct nth roots
- Roots of unity are equally spaced on the unit circle
- Always simplify $\rho^{1/n}$ when possible

9 Special Topics: Floor, Ceiling, and Archimedean Property

9.1 Overview

This chapter covers several special topics that appear frequently in MH1300 exams but don't fit neatly into the other categories: floor and ceiling functions, the absolute value function, and the Archimedean property of real numbers.

9.2 Floor and Ceiling Functions

Definition 9.1: Floor and Ceiling Functions

For any real number x:
Floor function: $\lfloor x \rfloor$ is the greatest integer less than or equal to x.

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$$

Equivalently: $\lfloor x \rfloor$ is the unique integer satisfying

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

Ceiling function: $\lceil x \rceil$ is the smallest integer greater than or equal to x.

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}$$

Equivalently: $\lceil x \rceil$ is the unique integer satisfying

$$\lceil x \rceil - 1 < x \leq \lceil x \rceil$$

Example

$$\begin{gathered}\lfloor 3.7 \rfloor = 3, \quad \lceil 3.7 \rceil = 4 \\ \lfloor -2.3 \rfloor = -3, \quad \lceil -2.3 \rceil = -2 \\ \lfloor 5 \rfloor = 5, \quad \lceil 5 \rceil = 5 \\ \lfloor -4 \rfloor = -4, \quad \lceil -4 \rceil = -4\end{gathered}$$

Theorem 9.1: Key Properties

For any real x:

1. $\lfloor -x \rfloor = -\lceil x \rceil$

2. $\lceil -x \rceil = -\lfloor x \rfloor$

3. If x is an integer, then $\lfloor x \rfloor = \lceil x \rceil = x$

4. $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{if } x \in \mathbb{Z} \\ -1 & \text{if } x \notin \mathbb{Z} \end{cases}$

9.2.1 Worked Example

Past Exam Question (AY 24/25 Q4c): Floor and Ceiling Identities

Question: Prove or disprove:

(i) For every real number x, $\lfloor -x \rfloor = -\lceil x \rceil$

(ii) For every real number x, $\lfloor -x \rfloor = -\lfloor x \rfloor$

Solution:
(i) Claim: $\lfloor -x \rfloor = -\lceil x \rceil$ *for all* $x \in \mathbb{R}$.
Proof: By definition of floor and ceiling:

$$\lfloor -x \rfloor \le -x < \lfloor -x \rfloor + 1$$

$$\lceil x \rceil - 1 < x \le \lceil x \rceil$$

Negating the second inequality:

$$-\lceil x \rceil \le -x < -\lceil x \rceil + 1$$

Comparing with the first, we see that both $\lfloor -x \rfloor$ and $-\lceil x \rceil$ are integers satisfying

$$n \le -x < n + 1$$

By uniqueness of the floor function, $\lfloor -x \rfloor = -\lceil x \rceil$. □

(ii) Claim: $\lfloor -x \rfloor = -\lfloor x \rfloor$ *is* ***false*** *in general.*
Counterexample: Take $x = 1/2$.

$$\lfloor -x \rfloor = \lfloor -1/2 \rfloor = -1$$

$$-\lfloor x \rfloor = -\lfloor 1/2 \rfloor = -0 = 0$$

Since $-1 \neq 0$, the equality fails. □

9.3 Archimedean Property

Definition 9.2: Archimedean Property of $\mathbb{R}$

The real numbers $\mathbb{R}$ satisfy the **Archimedean property**:
For any real numbers a, b with $a > 0$, there exists a positive integer n such that $na > b$.
Intuition: No matter how small $a > 0$ is, if you add it to itself enough times, you can exceed any given b.

Past Exam Question (AY 22/23 Q4b): Characterizing Archimedean Property

Question: A set $S \subseteq \mathbb{R}$ is said to have the Archimedean property if for every $a, b \in S$ there is a positive integer n such that $na > b$. Find a necessary and sufficient condition for S to have the Archimedean property.

Solution:
Claim: S has the Archimedean property if and only if $S \subseteq (0, \infty)$.
Sufficiency (⇒): Suppose $S \subseteq (0, \infty)$. Let $a, b \in S$. Then $a, b > 0$.
If $a \geq b$, take $n = 1$: $na = a \geq b$.
If $a < b$, let $k = \lfloor b/a \rfloor$. Then $k \leq b/a < k + 1$, so $b < a(k + 1)$.
Let $n = k + 1$ (a positive integer). Then $na > b$. ✓
Necessity (⇐): Suppose S has the Archimedean property. We show $S \subseteq (0, \infty)$.
Assume for contradiction that there exists $c \in S$ with $c \leq 0$.
Take $a = c$ and $b = c$ (both in S). By the Archimedean property, there exists $n \in \mathbb{Z}^+$ such that

$$na > b \quad \Rightarrow \quad nc > c$$

But since $n \geq 1$ and $c \leq 0$, we also have $nc \leq c$. Thus $c < nc \leq c$, a contradiction.
Therefore S contains no non-positive elements, so $S \subseteq (0, \infty)$. □

9.4 Topic Summary

Special Topics Quick Reference

Floor & Ceiling:

- $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$
- $\lceil x \rceil - 1 < x \leq \lceil x \rceil$
- $\lfloor -x \rfloor = -\lceil x \rceil$
- $\lceil -x \rceil = -\lfloor x \rfloor$
- $\lfloor x \rfloor + \lfloor -x \rfloor \in \{0, -1\}$

Archimedean Property:

- For $a > 0$ and any b, $\exists n \in \mathbb{Z}^+$ with $na > b$
- A set S has the Archimedean property iff $S \subseteq (0, \infty)$

A TI-84 Plus CE: Automated Truth Table Generator

Purpose

The following program automatically generates an 8-row truth table for three propositional variables `A`, `B`, `C`. The TI-84 Plus CE evaluates your logical expression using the built-in `not`, `and`, `or`, and the numerical biconditional `=`. The results are stored in lists `L1--L4`, which can be viewed directly via

`STAT` → `1:Edit`.

Typing the program once (before the exam) ensures instant truth-table computation.

Full Program: Three-Variable Truth Table (A,B,C)

Below is the exact program. Every line is intentionally short and CE-compatible.

PROGRAM:A (3-Variable Truth Table)

```
PROGRAM:A
ClrTable
Input "",Str1
0→X
For(A,0,1)
 For(B,0,1)
  For(C,0,1)
   X+1→X
   A→L1(X)
   B→L2(X)
   C→L3(X)
   expr(Str1)→L4(X)
  End
 End
End
Stop
```

How to Type Each Command (TI-84 Plus CE Exact Keys)

1. `ClrTable`: `2nd` → `WINDOW` (scroll to `ClrTable`)

2. `Input`: Press `PRGM` → `I/O` → `1:Input`

3. `Str1`: `VARS` → `7:String` → `1:Str1`

4. `0`→ `X`: type `0`, press `STO`→, then `X,T,,n` key

5. `For(...):`
   - Press the number `4` (because `For` is PRGM command #4).
   - Or use: `PRGM` → `7:For`
6. `End`: press `7` (or `PRGM` → `8:End`)
7. `Stop`: press `G` (letter G), or manually:

   `PRGM` → `0:Stop`

8. `L1, L2, L3, L4: 2nd` → `1`, `2`, `3`, `4`
9. `expr(: 2nd` → `CATALOG`, then scroll to `expr(`

Using the Program

1 Run with:

`PRGM` → `A` → `ENTER`.

2 When prompted `""`, type any logical formula using variables `A`, `B`, `C`. Examples:

`not(A) or (B and C)`, `A=B`, `not(A) or (B or C)`.

3 View output with:

`STAT` → `1:Edit`.

4 The lists show:

$$L1 = A, \quad L2 = B, \quad L3 = C, \quad L4 = \text{formula truth values.}$$

Quick Self-Test (Highly Recommended)

Use the formula:

`not(A) or A`

A tautology. `L4` should contain eight **1**'s.

Then test:

`A=B`

`L4` should be:

$$1, 1, 0, 0, 0, 0, 1, 1.$$

Expanding to Four Variables (A,B,C,D)

To create a 4-variable, 16-row truth table, simply add a fourth loop:

PROGRAM:T4 (4-Variable Truth Table)

```
ClrTable
Input "",Str1
0→X
For(A,0,1)
 For(B,0,1)
  For(C,0,1)
   For(D,0,1)
    X+1→X
    A→L1(X)
    B→L2(X)
    C→L3(X)
    D→L4(X)
    expr(Str1)→L5(X)
   End
  End
 End
End
Stop
```

Notes:

- Output lists shift: `L1--L4` store variables, `L5` stores truth values.
- All typing rules and key locations are identical.

When to Type This Program

It is highly recommended to type this program:

after your GC-calculator check but before the exam begins.

This ensures both compliance and readiness. Afterwards, evaluating any MH1300 truth table takes less than 5 seconds.

B Cheatsheet Guide

A dedicated two–page MH1300 examination cheatsheet is provided as a standalone PDF and appended after this section. It has been designed with two objectives in mind:

- to serve as a **rapid visual reference** for core concepts, identities, and proof structures;
- to provide a **compact space** for students to record year-specific results and theorems introduced in class.

Important: Although the MH1300 syllabus is consistent across years, instructors may introduce:

- additional lemmas or identities,
- alternative forms of standard theorems,
- specific proof strategies highlighted during lectures,
- clarifications or strengthened versions of earlier results.

Blank regions have therefore been intentionally built into the cheatsheet layout. Students are strongly encouraged to **copy down these instructor-specific theorems or results** into the designated spaces to complete the sheet for their academic year.

Integrated Past-Year References. The cheatsheet embeds **selected past-year final examination snippets** directly into the background layer. This allows you to recognise common structural patterns at a glance—such as typical induction tasks, standard equivalence proofs, usual modular arithmetic manipulations, and common relation/function classification questions.

Printing Recommendations. To preserve sharpness of the embedded diagrams and faint background overlays, it is recommended to **print the cheatsheet at 600 DPI or higher**.

How to Use the Cheatsheet Effectively:

1. **Fill in the blank theorem areas early**. These will form your personalised quick-reference scaffold.
2. **Annotate frequently used proof templates** (contrapositive, induction, injectivity/surjectivity tests, divisibility proofs).
3. **Review the embedded past-year patterns** to reinforce the typical structure of MH1300 questions.

QRS@NTU

Sets

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (natural numbers)

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ (positive integers)

$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$ (rational numbers)

$\mathbb{R}$ = real numbers

$\mathbb{C}$ = complex numbers

Logical Form and Equivalences

Notation	Name	Read as	Ti84
$\sim p$ or $\neg p$	Negation	not p	`not(p)`
$p \wedge q$	Conjunction	p and q	`p and q`
$p \vee q$	Disjunction	p or q	`p or q`
$p \to q$	Conditional	if p then q	`not(p) or q`
$p \leftrightarrow q$	Biconditional	p iff q	`p = q`

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

Statements: true or false but not both.
Tautology: always true (T).
Contradiction: always false (F).

Commutative:	$p \wedge q \equiv q \wedge p, \quad p \vee q \equiv q \vee p$
Associative:	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r),$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive:	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r),$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Identity:	$p \wedge T \equiv p, \quad p \vee F \equiv p$
Negation:	$p \vee \neg p \equiv T, \quad p \wedge \neg p \equiv F$
Double negation:	$\neg(\neg p) \equiv p$
Idempotent:	$p \wedge p \equiv p, \quad p \vee p \equiv p$
Universal bound:	$p \vee T \equiv T, \quad p \wedge F \equiv F$
De Morgan:	$\neg(p \vee q) \equiv \neg p \wedge \neg q,$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption:	$p \vee (p \wedge q) \equiv p, \quad p \wedge (p \vee q) \equiv p$
Negations of T and F:	$\neg T \equiv F, \quad \neg F \equiv T$

Ti84 Program

```
PROGRAM:A          A→L1(X)
ClrTable           B→L2(X)
Input "",Str1      C→L3(X)
0→X                expr(Str1)→L4(X)
For(A,0,1)         End
For(B,0,1)         End
For(C,0,1)         End
X+1→X              Stop
```

Conditional Statements

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

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

Contrapositive: $p \to q \equiv \neg q \to \neg p$

Converse: $q \to p$

Inverse: $\neg p \to \neg q$

"p only if q" $\equiv p \to q \equiv \neg q \to \neg p$

"p if q" $\equiv q \to p$

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

r sufficient for s: $r \to s$

r necessary for s: $s \to r \equiv \neg r \to \neg s$

r necessary and sufficient for s: $r \leftrightarrow s$

Quantified Statements

Universal: $\forall x \in D, Q(x)$ — true if $Q(x)$ is true for every x in D.
Existential: $\exists x \in D$ such that $Q(x)$ — true if $Q(x)$ is true for at least one x in D.
Negations:

$$\neg(\forall x \in D, Q(x)) \equiv \exists x \in D \text{ such that } \neg Q(x)$$

$$\neg(\exists x \in D \text{ such that } Q(x)) \equiv \forall x \in D, \neg Q(x)$$

$$\neg(\forall x, P(x) \to Q(x)) \equiv \exists x \text{ such that } P(x) \wedge \neg Q(x)$$

Methods of Proof

Direct Proof Techniques:

- **Direct proof**: Assume hypothesis, derive conclusion
- **Proof by exhaustion**: Check all possible cases
- **Proof by cases**: Divide into exhaustive, mutually exclusive cases
- **Element method**: For sets, take arbitrary element and show property holds

Indirect Proof Techniques:

- **Proof by contradiction**: Assume negation of conclusion, derive contradiction
- **Proof by contraposition**: To prove $p \to q$, prove $\neg q \to \neg p$
- **Counterexample**: Find one example where universal statement fails

Valid Inference Rules:

Rule	Statement	Result
Modus Ponens	$p \to q,\ p$	q
Modus Tollens	$p \to q,\ \neg q$	$\neg p$
Generalization	p	$p \vee q$
Specialization	$p \wedge q$	p
Conjunction	$p,\ q$	$p \wedge q$
Disjunctive Syllogism	$p \vee q,\ \neg q$	p
Hypothetical Syllogism	$p \to q,\ q \to r$	$p \to r$
Proof by Cases	$p \vee q,\ p \to r,\ q \to r$	r

Common Fallacies (Invalid Inferences):

Fallacy	Statement	Invalid Result
Converse Error	$p \to q,\ q$	p
Inverse Error	$p \to q,\ \neg p$	$\neg q$

Mathematical Induction

Standard Induction: To prove $P(n)$ for all $n \geq a$:

1. Base case: Prove $P(a)$
2. Inductive step: Prove $\forall k \geq a,\ P(k) \Rightarrow P(k+1)$

Strong Induction: To prove $P(n)$ for all $n \geq a$:

1. Base cases: Prove $P(a), P(a+1), \ldots, P(b)$ for some $b \geq a$
2. Inductive step: If $P(i)$ holds for all $a \leq i \leq k$ (where $k \geq b$), then $P(k+1)$ holds

Elementary Number Theory

Basic Definitions:

- **Even**: $n = 2k$ for some integer k
- **Odd**: $n = 2k + 1$ for some integer k
- **Prime**: $n > 1$ and only positive divisors are 1 and n
- **Composite**: $n > 1$ and $n = ab$ with $1 < a, b < n$
- **Rational**: $r = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$

Parity Facts:

- Even $\pm$ even = even; odd $\pm$ odd = even; even $\pm$ odd = odd
- Even $\times$ any = even; odd $\times$ odd = odd

Divisibility: $d \mid n \iff \exists k \in \mathbb{Z}$ such that $n = dk$
Properties:

- If $a \mid b$ and $b \mid c$, then $a \mid c$ (transitivity)
- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$

Division Algorithm &Special Functions

Quotient-Remainder Theorem: For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, $\exists$ unique $q, r \in \mathbb{Z}$:

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

Notation: $q = n$ div d (quotient), $r = n$ mod d (remainder)

Absolute Value: $|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$

Properties: $-|x| \le x \le |x|$, $|-x| = |x|$, $|x+y| \le |x| + |y|$

Floor & Ceiling:

- **Floor:** $\lfloor x \rfloor = n$ where $n \le x < n+1$ (largest integer $\le x$)
- **Ceiling:** $\lceil x \rceil = n$ where $n-1 < x \le n$ (smallest integer $\ge x$)

Important Theorems & Formulas

Binomial Theorem:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \quad \text{where} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Factorization: $p^n - q^n = (p-q)(p^{n-1} + p^{n-2}q + \cdots + q^{n-1})$

Floor Function:

$$\lfloor n \rfloor = \begin{cases} \dfrac{n}{2}, & n \text{ even,} \\ \dfrac{n-1}{2}, & n \text{ odd.} \end{cases}$$

Quotient–Remainder (Integer Division): For $n \in \mathbb{N}$, $d \in \mathbb{N}^+$,

$$n = dq + r, \qquad 0 \le r < d.$$

Remainder Formula:

$$q = \left\lfloor \frac{n}{d} \right\rfloor, \qquad r = n - d \left\lfloor \frac{n}{d} \right\rfloor.$$

Well-Ordering Principle Every non-empty subset of $\mathbb{N}$ (or $\mathbb{Z}_{\ge 0}$) has a least element. That is, if $A \subseteq \mathbb{N}$ and $A \neq \emptyset$, then $\exists m \in A$ such that

$$m \le a \quad \text{for all } a \in A.$$

Key Results:

- $\sqrt{2}$ is irrational
- There are infinitely many prime numbers
- Fundamental Theorem of Arithmetic: Every integer > 1 has unique prime factorization

Complex Numbers

Definition: $z = a + bi$ where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$.
$a = \mathrm{Re}(z)$ (real part), $b = \mathrm{Im}(z)$ (imaginary part)

Basic Operations: For $z = a + bi$ and $w = c + di$:

$$z + w = (a+c) + (b+d)i$$

$$z \cdot w = (ac - bd) + (ad + bc)i$$

$$\bar{z} = a - bi \quad \text{(complex conjugate)}$$

$$|z| = \sqrt{a^2 + b^2} \quad \text{(modulus)}$$

$$z \cdot \bar{z} = |z|^2 = a^2 + b^2$$

Polar Form: $z = r(\cos\theta + i\sin\theta) = re^{i\theta}$
where $r = |z|$ and $\theta = \arg(z)$

Key Formulas:

- **Euler's Formula:** $e^{i\theta} = \cos\theta + i\sin\theta$
- **De Moivre's Theorem:** $(re^{i\theta})^n = r^n e^{in\theta} = r^n(\cos(n\theta) + i\sin(n\theta))$
- **nth Roots:** $z^{1/n} = r^{1/n} e^{i(\theta + 2\pi k)/n}$ for $k = 0, 1, \ldots, n-1$

Useful Properties:

- $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- $|z \cdot w| = |z| \cdot |w|$, $|z/w| = |z|/|w|$ (for $w \neq 0$)
- $z^{-1} = \frac{\bar{z}}{|z|^2}$ (for $z \neq 0$)

Set Theory

Operations (relative to universe U):

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\},$$
$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\},$$
$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\} = A \cap B^c,$$
$$A^c = \{x \in U \mid x \notin A\}.$$

Membership rules:

- $x \in A \cup B \iff x \in A \text{ or } x \in B$
- $x \in A \cap B \iff x \in A \text{ and } x \in B$
- $x \in A - B \iff x \in A \text{ and } x \notin B$
- $x \in A^c \iff x \notin A$

Basic properties:

- $A \cap B \subseteq A$, $A \cap B \subseteq B$
- $A \subseteq A \cup B$, $B \subseteq A \cup B$
- If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$
- $A \subseteq B \iff A \cap B = A \iff A \cup B = B$
- $\emptyset \subseteq A$ for all sets A

Set identities:

Commutative: $A \cup B = B \cup A, \quad A \cap B = B \cap A$

Associative: $(A \cup B) \cup C = A \cup (B \cup C),$
$(A \cap B) \cap C = A \cap (B \cap C)$

Distributive: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Identity: $A \cup \emptyset = A, \quad A \cap U = A$

Complement: $A \cup A^c = U, \quad A \cap A^c = \emptyset$

Double comp.: $(A^c)^c = A$

Idempotent: $A \cup A = A, \quad A \cap A = A$

Univ. bound: $A \cup U = U, \quad A \cap \emptyset = \emptyset$

De Morgan: $(A \cup B)^c = A^c \cap B^c, \quad (A \cap B)^c = A^c \cup B^c$

Absorption: $A \cup (A \cap B) = A, \quad A \cap (A \cup B) = A$

Difference: $A - B = A \cap B^c$.

Partition: Non-empty sets $\{A_1, \ldots, A_n\}$ partition A if $A = A_1 \cup \cdots \cup A_n$ and $A_i \cap A_j = \emptyset$ for $i \neq j$.

Power set: $\mathcal{P}(A) = \{S \mid S \subseteq A\}$, $\quad |\mathcal{P}(A)| = 2^{|A|}$.

Cartesian product: $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Functions

A function $f : X \to Y$ assigns each $x \in X$ exactly one $y \in Y$.

Domain: X **Codomain:** Y **Range:** $f(X) = \{f(x) \mid x \in X\}$

Image of $A \subseteq X$: $f(A) = \{f(x) \mid x \in A\}$ **Preimage of $B \subseteq Y$:** $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$

Injective (1–1): $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ **Surjective (onto):** $\forall y \in Y, \exists x \in X : f(x) = y$ **Bijective:** injective + surjective

Inverse (if bijective): $f^{-1} : Y \to X$ with $f^{-1}(f(x)) = x$ and $f(f^{-1}(y)) = y$.

Composition: $(g \circ f)(x) = g(f(x))$ Associative; preserves injective/onto when both components are.

Relations

A relation R from A to B is a subset of $A \times B$. Write $xRy \iff (x, y) \in R$.

Inverse: $R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}$.

Composition: If $R \subseteq A \times B$ and $S \subseteq B \times C$:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in R \text{ and } (b, c) \in S\}.$$

Properties on set A:

- **Reflexive:** $\forall x \in A, (x, x) \in R$
- **Symmetric:** $\forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$
- **Transitive:** $\forall x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$

Equivalence relation: Reflexive, symmetric, and transitive.

Transitive closure R^t of R:

- R^t is transitive
- $R \subseteq R^t$
- If S is transitive and $R \subseteq S$, then $R^t \subseteq S$ (minimality)