MATHD022: Discrete Mathematics

Connor Petri

Spring 2025

Contents

1. The Language of Mathematics

1.1 Variables

Definition A **variable** is a symbol that is used as a placeholder when:

- The quantity has one of more values, but is not known.
  - For example: $2x^2 - x = 7$
- The quantity represents **any element** from a given set.
  - For example: The reciporical of any non-zero integer n is $\frac{1}{n}$.

Writing Sentences using Variables We can rewrite the following sentences using variables:

- Is there an integer n that has a remainder of 2 when it is divided by 5?
  - Is there an integer n such that $n\%5 = 2$?
- The cube root of any negative real number is negative.
  - For any real number s, if $s < 0$, then $\sqrt[3]{s} < 0$.

Types of Statements

- A **universal statement** is a statement that is true always true.
  - For example: **All** positive numbers are greater than 0.
- A **conditional statement** is a statement that is true if a certain condition is met.
  - For example: **If** 378 is divisible by 18, **then** 378 is divisible by 6.
- A **universal conditional statement** is a statement that is both conditional and universal.

  - For example: **For all** animals a, if a is a dog, **then** a is a mammal.
  - As a universal statement: **For all** dogs a, a is a mammal.
  - As a conditional statement: **If** a is a dog, **then** a is a mammal.

- An **existential statement** gives a property that is true for at least one thing.

  - **There is** a prime number that is even.

- A **universal existential statement** is a statement where the first part is universal and the second part is existential.

  - **Every** real number **has** an additive inverse.
  - **For all** real numbers r, **there is** an additive inverse $-r$.
  - **For all** real numbers r, **there is** a real number s such that $r+s = 0$.

- An **existential universal statement** is a statement where the first part is existential and the second part is universal.

  - **There is** a positive integer that is less than or equal to **every** positive integer.
  - **There is** a positive intefer m such that **every** positive integer is greater than or equal to m.
  - **There is** a positive integer m with the property that **for all** positive integers n, $m \leq n$.

1.2 Sets

Definition A **set** is a collection of objects.

Notation

- $x \in S$: x is an element of S.
- $x \notin S$: x is not an element of S.
- $S = \{1, 2, 3, \dots\}$: is **set roster notation.**

Axion of Extension A set is determined by what its elements are. Orders of elements or repeated elements can't be determine the set.
For example: $\{1, 2, 3\} = \{3, 2, 2, 1, 2, 3, 1\}$. There are 3 elements in both sets.

Common Sets

- $\mathbb{R}$: the set of all real numbers.
- $\mathbb{Z}$: $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ the set of all integers.
- $\mathbb{N}$: $\{1, 2, 3, \dots\}$ the set of all natural numbers.
- $\mathbb{Q}$: the set of all rational numbers.
- $\emptyset = \{\}$: the empty set, or null set.

The null set is a subset of every set.

Set Builder Notation Let S denote a set and let $x \in S$ be and element in S. $P(x)$ is a property that some elements of S satisfy.

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

A constains elements in S such that (—) P(x) is true.

Subsets

Definition Let A and B be sets. A is a **subset** ($\subseteq$) of B if every element of A is also an element of B.

Proper Subsets Let A and B be sets. A is a **proper subset** ($\subset$) of B if every element of A is also an element of B, **and** there is at least one element in B that is not in A.

Example Let $A = \mathbb{Z}^+, B = \{n \in \mathbb{Z} | 0 \leq n \leq 100\}, andC = \{100, 200, 300, 400, 500\}$.

- $B \subseteq A$ is false.
- $C \subset A$ is true.
- $C \subseteq B$ is false.
- $C \subseteq C$ is true.

Cartesian Product of sets Let A and B be sets. The **Cartesian product** of A and B, denoted $A \times B$, is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

Example Let $A = \{1, 2, 3\}$ and $B = u, v$.

$$A \times B = \{(1, u), (1, v), (2, u), (2, v), (3, u), (3, v)\}$$
$$A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

1.3 Relations and Functions

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

$$R \subseteq A \times B$$

- If (x,y) $\in R$, we say that x is related to y by R, denoted as xRy.
- **A** is in the **domain** of **R**
- **B** is the **codomain** of **R**

Example Let $A = \{1, 2, 3\}$ and $B = \{1, 2\}$ and define a relation R from A to B as follows:

$$\begin{aligned}(x, y) \in R \iff \frac{x+y}{2} \in \mathbb{Z}\\ R =& \{(1,1),(1,2),(2,1),(2,2),(3,1)\}\\ &\text{Domain of } R = \{1,2,3\}\\ &\text{Codomain of } R = \{1,2\}\end{aligned}$$

Functions

Definition Let A and B be two sets. A function F from A to B is a relation with domain A and co-domain B that satisfies the following properties:

- For every element $x \in A$, there is an element $y \in B$ such $(x, y) \in F$
- For every element $x \in A$ and $y, z \in B$:
  - If $(x, y) \in F$ and $(x, z) \in F$, then $y = z$

Example Let $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$. Which of the relations defined below are functions from A to B?

- $R = \{(2, 5), (4, 1), (4, 3), (6, 5)\}$
  - Not a function because 4 is related to 1 and 3. This is not a many-to-one relationship.
- For all $(x.y) \in A \times B, (x, y) \in S \iff y = x + 1$
  - $S = \{(2, 3), (4, 5)\}$ is a function from A to B.
- $T = \{(2, 5), (4, 1), (6, 1)\}$
  - T is a function from A to B as A has a many-to-one relationshop with B.

Equivalent Functions

Let A and B be two sets. Two functions f and g from A to B:

$$f = g \iff f(x) = g(x) \quad \forall \quad x \in A$$

2. The Logic of Compound Statements

2.1 Logical Form and Equivalence

Arguments

Definition An arguement is a sequence of statements aimed at demonstrating the truth of an assertion.

- The assertion at the end of the sequence is called the conclusion.
- The statements that support the conclusion are called premises.
- If the premises are true, the conclusion must also be true.

Example

- If student A is a math major or student A is a computer science major,
- Then student A will take Discrete Math.

Logical Statements

Definition A logical statement is a declarative sentence that is either true or false, but not both.

- Not p: $\neg p$
- p and/but q: $p \wedge q$
- p or q: $p \vee q$
- Neither p nor q: $\neg p \wedge \neg q$

Example h = healthy, w = wealthy, s = wise

- John is healthy and wealthy but not wise.
  - $(h \wedge w) \wedge \neg s$
- John is neither wealthy nor wise, but he is healthy
  - $(\neg w \wedge \neg s) \wedge h$

Equivalent Statements

Definition Two logical statements are equivalent if they have the same truth tables, denoted:

$$p \equiv q$$

De Morgan's Laws The negation ($\neg$) of an and statement is logically equivalent to the or statement of the negations. Similarly, the negation of an or statement is logically equivalent to the and statement of the negations.

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

Tautological and Condtradictory Statements

- A tautological statement is a statement that is always true.
- A contradictory statement is a statement that is always false.

2.2 Conditional Statements

Definition A Conditional statement is in the form "If p, then q" and is denoted as $p \implies q$ This is read as p implies q.

- p is the **hypothesis** of the statement.
- q is the **conclusion** of the statement.

Order of Operations

- (): parentheses
- $\neg$: negation
- $\wedge / \vee$: conjunction/disjunction
- $\implies$: implication

Equivalent of Conditional Statements

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

Example Find the negation of the following statement: "If my car is in the repair shop then I cannot go to class".

- Hypothesis (p): "My car is in the repair shop"
- Conclusion (q): "I cannot go to class"
- Convert: $p \implies q \equiv \neg p \vee q$
- Negation: $\neg(p \implies q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$
- Convert back: "My car is in the repair shop and I can go to class"

Negation vs Inverse The negation of a statement is NOT the same as the inverse of the statement.

- Negation: $\neg(p \implies q)$
- Inverse: $\neg p \implies \neg q$

Example If p is a square, then p is a rectangle.

- Hypothesis (p): "p is a square"
- Conclusion (q): "p is a rectangle"
- Negation: $\neg(p \implies q) \equiv p \wedge \neg q$
- Convert back: "p is a square and p is not a rectangle"
- Inverse: $\neg p \implies \neg q \equiv p \vee \neg q$
- Convert: "If p is not a square, then p is not a rectangle"

More statement types

- Contrapositive of $p \implies q \equiv \neg q \implies \neg p$
- Converse of $p \implies q \equiv q \implies p$
- Inverse of $p \implies q \equiv \neg p \implies \neg q$

Example If today is Easter then tomorrow is Monday.

- Hypothesis (p): "Today is Easter"
- Conclusion (q): "Tomorrow is Monday"
- Convert: $p \implies q$
- Contrapositive: $\neg q \implies \neg p \equiv$ If tomorrow is not Monday, then today is not Easter
- Converse: $q \implies p \equiv$ If tomorrow is Monday, then today is Easter
- Inverse: $\neg p \implies \neg q \equiv$ If today is not Easter, then tomorrow is not Monday

Biconditional Statements A biconditional statement is in the form ”p if and only if q” and is denoted as $p \iff q$. This is read as p if and only if q.

$$p \iff q \equiv (p \implies q) \wedge (q \implies p) \tag{1}$$

Sufficient and Necessary Conditions If r and s are statements:

- r is a **sufficient condition** for s if $r \implies s$.
- r is a **necessary condition** for s if $s \implies r$ or $s \implies r$.
- r is a **necessary and sufficient condition** for s if $r \iff s$.

2.3 Valid and Invalid Arguments

Definition An **argument** is a sequence of statements, and an **argument form** is a sequence of statement form.

- The final statement or statement form is called the **conclusion**. The symbol $\therefore$ (therefore) is used to denote the conclusion.
- All the preceding statements or statement forms are called **premises**, or assumptions or hypotheses.
- An argument form is **valid** means if all premises are true, then the conclusion must also be true.

Example Determine whether the following argument form is valid or invalid:

$$\begin{aligned} p &\implies q \vee \neg r \\ q &\implies p \wedge r \\ \therefore p &\implies r \end{aligned}$$

p	q	r	$p \implies (q \vee \neg r)$	$q \implies (p \wedge r)$	$p \implies r$	Valid?
T	T	T	T	T	T	Valid
T	T	F	F	T	F	Invalid
T	F	T	T	F	T	Invalid
T	F	F	F	F	F	Invalid
F	T	T	T	F	T	Invalid
F	T	F	T	F	T	Invalid
F	F	T	T	F	T	Invalid
F	F	F	T	F	T	Invalid

Therefore the argument form is invalid.

Syllogisms

Definition An argument form with two premisies are called syllogism. The firest and second premises are called the major premise and minor premise respectively.

Modus Ponens Modus Ponens is a valid argument form that can be expressed as:

$$\begin{aligned} p &\implies q \\ p & \\ \therefore q & \end{aligned}$$

This means that if $p \implies q$ (if p then q) is true, and p is true, then we can conclude that q must also be true.

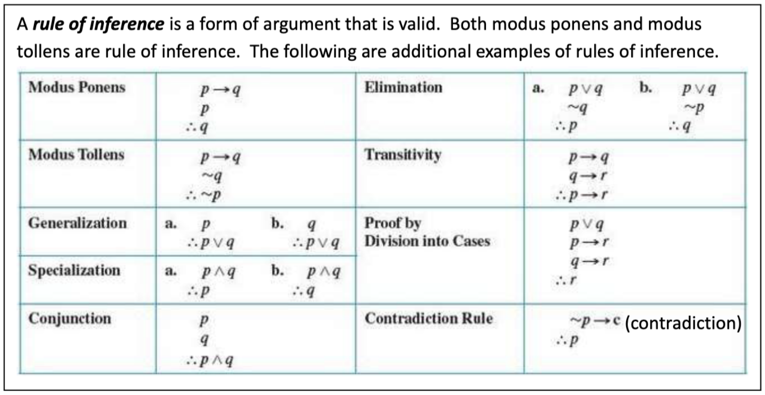
Example If there are more pigeons than there are pigeonholes, then at least two pigeons roost in the same hole.
There are more pigeons than there are pigeonholes.
$\therefore$ At least two pigeons roost in the same hole.

Modus Tollens Modus Tollens is a valid argument form that can be expressed as:

$$\begin{aligned} p &\implies q \\ \neg q & \\ \therefore \neg p & \end{aligned}$$

This means that if $p \implies q$ (if p then q) is true, and q is false, then we can conclude that p must also be false.

Rules of Inference A rule of inference is a form of argument that is valid. Both modus ponens and modus tollens are rules of inference. The following are additional examples of rules of inference:



A ***rule of inference*** is a form of argument that is valid. Both modus ponens and modus tollens are rule of inference. The following are additional examples of rules of inference.

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \to c$ (contradiction) $\therefore p$

Prove by Detachment
Prove by contrapositive
Disjunctive of syllogism
Law of Syllogism

Contradictions

Definition A contradiction is a statement that is always false.

$$\begin{aligned} &\neg p \implies c \\ &\therefore p \end{aligned}$$

2 column rule The 2 column rule is a way to prove by contradiction. For example with knights and knaves. Knights always tell the truth and knaves always lie:

- A says B is a knight
- B says A and I are of opposite types

Suppose A is a knight:

What A says must be true	By the definition of a knight
B is a knight	by given (what A says)
What B says must be true	By the definition of a knight
A and B are of opposite types	by given (what B says)
Contradiction	A is not a knight or A is a knave
The supposition is false	by rule of contradiction
A is not a knight or A is a knave	by negation of supposition.

3. The Logic of Quantified Statements

3.1 Predicates and Quantified Statements (Part 1)

Predicates

Definition A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. For example: "$P(x)$: x is a positive integer" is a predicate. The statement $P(3)$ is true, while $P(-2)$ is false.

Domain of a Predicate The Domain of a predicate is the set of all values that can be substituted for the variable.

Example Let $P(x)$ be the predicate "$x^2 > x$." The domain of $P(x)$ is $\mathbb{R}$.

$$\begin{aligned} P(\frac{1}{2}):&\quad (\frac{1}{2})^2 > \frac{1}{2} && = False \\ P(-\frac{1}{2}):&\quad (-\frac{1}{2})^2 > -\frac{1}{2} && = True \\ P(2):&\quad 2^2 > 2 && = True \end{aligned}$$

Truth Sets

Definition If $P(x)$ is a predicate with domain D, the truth set of $P(x)$ is the set of all elements in D for which $P(x)$ is true when they are substituted for x. The truth set of $P(x)$ is denoted by:

$$\{x \in D \ni P(x)\} \subseteq D$$

Example Let $P(x)$ be the predicate "$n^2 \leq 30$" with domain $\mathbb{Z}$. The truth set of $P(x)$ is:

$$\{x \in \mathbb{Z} \ni P(x)\} = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$$

Quantified Statements

Definition A quantified statement is a statement that contains a quantifier. The two most common quantifiers are:

- **Universal Quantifier** $\forall$ (for all)
- **Existential Quantifier** $\exists$ (there exists)

Universal Statements Let $P(x)$ be a predicate with domain D. A univseral statment is a statement of the form "$\forall x \in D, P(x)$" which is read as "for all x in D, $P(x)$ is true."

- It is defined to be true if and only if $P(x)$ is true for all x in D.
- It is defined to be false if and only if $P(x)$ is false for at least one x in D.
- The value of x for which $P(x)$ is false is called a counterexample.

Example Let $D = \{1, 2, 3\}$, and show that the statement "$\forall x \in D, x^2 \geq x$" is true.

$$\begin{aligned} &1^2 \geq 1 \text{ is true} \\ &2^2 \geq 2 \text{ is true} \\ &3^2 \geq 3 \text{ is true} \\ \therefore \quad &\forall x \in D, x^2 \geq x \text{ is true.} \end{aligned}$$

Existential Statements Let $P(x)$ be a predicate with domain D. An existential statement is a statement of the form "$\exists x \in D \ni P(x)$" which is read as "there exists an x in D such that $P(x)$ is true."

- It is defined to be true if and only if $P(x)$ is true for at least one x in D.
- It is defined to be false if and only if $P(x)$ is false for all x in D.
- The value of x for which $P(x)$ is true is called a witness.

Example Show that the statement "$\exists x \in \mathbb{Z} \ni \frac{1}{x} = x$" is true.

$$x = 1 : \frac{1}{1} = 1 \text{ is true}$$
$$\therefore \quad \exists x \in \mathbb{Z} \ni \frac{1}{x} = x \text{ is true.}$$

Universal Conditional Statements A universal conditional statement is a statement of the form "$\forall x \in D, P(x) \implies Q(x)$" which is read as "for all x in D, if $P(x)$ is true, then $Q(x)$ is true."

3.2 Predicates and Quantified Statements (Part 2)

Negations of Quantified Statements

Negation of a Universal Statement

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

Negation of an Existential Statement

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

Negation of a Universal Conditional Statement

$$\neg(\forall x \in D, P(x) \implies Q(x)) \equiv \exists x \in D \ni P(x) \wedge \neg Q(x)$$

Consider the statement: $\forall x \in D, P(x) \implies Q(x)$.

$$\begin{aligned} \text{It's contrapositive is:} \quad & \forall x \in D, \neg Q(x) \implies \neg P(x) \\ \text{It's converse is:} \quad & \forall x \in D, Q(x) \implies P(x) \\ \text{It's inverse is:} \quad & \forall x \in D, \neg P(x) \implies \neg Q(x) \end{aligned}$$

3.3 Statements with Multiple Quantifiers

Consider the statement: $\forall x \in D, \exists y \in E \ni P(x,y)$. To show the truth of the statement, we must show that for every x in D, there exists a y in D such that $P(x,y)$ is true.

Example Let $D = \{1,2,3\}$ and $P(x,y)$ be the predicate "$x+y = 4$". Show that the statement $\forall x \in D, \exists y \in D \ni P(x,y)$ is true.

$$\begin{aligned} x = 1: &\quad \exists y \in D \ni 1 + y = 4 \implies y = 3 \\ x = 2: &\quad \exists y \in D \ni 2 + y = 4 \implies y = 2 \\ x = 3: &\quad \exists y \in D \ni 3 + y = 4 \implies y = 1 \\ \therefore &\quad \forall x \in D, \exists y \in D \ni P(x,y) \text{ is true.} \end{aligned}$$

Consider the statement: $\exists x \in D \ni \forall y \in D, P(x,y)$. To show the truth of the statement, we must show that there exists an x in D such that for every y in D, $P(x,y)$ is true.

Example Let $D = \{1,2,3\}$ and $P(x,y)$ be the predicate "$x+y = 4$". Show that the statement $\exists x \in D \ni \forall y \in P, P(x,y)$ is false.

$$\begin{aligned} x = 1: &\quad \forall y \in D, 1 + y = 4 \implies y = 3 \\ x = 2: &\quad \forall y \in D, 2 + y = 4 \implies y = 2 \\ x = 3: &\quad \forall y \in D, 3 + y = 4 \implies y = 1 \\ \therefore &\quad \exists x \in D \ni \forall y \in D, P(x,y) \text{ is false.} \end{aligned}$$

Negation of Multiply-Quantified Statements

$$\begin{aligned} \neg(\forall x \in D, \exists y \in E \ni P(x,y)) &\equiv \exists x \in D \ni \forall y \in E, \neg P(x,y)) \\ \neg(\exists x \in D, \ni \forall y \in E, P(x,y)) &\equiv \forall x \in D, \exists y \in E \ni \neg P(x,y) \end{aligned}$$

3.4 Arguments with Quantified Statements

Universal Model Ponens (Direct Proof)

$\forall x, P(x) \implies Q(x)$ If x makes P(x) true, then x makes Q(x) true.
$P(a)$ Input a makes P(a) true.
$\therefore\ Q(a)$ Therefore a makes Q(a) true.

Example Let $P(x)$ be the predicate "x is a prime number" and $Q(x)$ be the predicate "x is an odd number".

$\forall x, P(x) \implies Q(x)$ If x is a prime number, then x is an odd number.
$P(3)$ 3 is a prime number,
$\therefore\ Q(3)$ therefore 3 is an odd number.

Universal Modus Tollens (Prove by Contradiction)

$\forall x, P(x) \implies Q(x)$ If x makes P(x) true, then x makes Q(x) true.
$\neg Q(a)$ Input a makes Q(a) false.
$\therefore\ \neg P(a)$ Therefore a does not make P(a) true.

Example Consider the statement "All irrational numbers are real numbers.":

$\forall x \in \mathbb{R} - \mathbb{Q}, x \in \mathbb{R}$ If x is an irrational number, then x is a real number.
$\frac{1}{0} \notin \mathbb{R}$ $\frac{1}{0}$ is not a real number,
$\therefore\ \frac{1}{0} \notin \mathbb{R} - \mathbb{Q}$ therefore $\frac{1}{0}$ is not an irrational number.

Converse and Inverse Errors

Converse Error

$\forall x, P(x) \implies Q(x)$ $Q(a) \therefore\ P(a)$(Invalid Arguement)

Inverse Error

$$\forall x, P(x) \implies Q(x) \qquad \neg P(a) \therefore \quad \neg Q(a)\text{(Invalid Arguement)}$$

4. Elementary Number Theory and Methods of Proof

4.1 Direct Proof and Counterexample

Definitions Let P(n) be the predicate ”n is an even number”.

$$\forall n \in \mathbb{Z}, P(n) \iff \exists k \in \mathbb{Z} \ni n = 2k.$$
$$\forall n \in \mathbb{Z}, \neg P(n) \iff \exists k \in \mathbb{Z} \ni n = 2k+1.$$

Example Is -301 even or odd?

$$-301 = 2k+1 \text{ for } k = -151$$

Example If $a, b \in \mathbb{Z}$, is $6a^2b$ even?

$$\begin{aligned} & \exists a, b \in \mathbb{Z} \ni 6a^2b = 2(k)+1 \\ & 6a^2b = 2(3a^2b) \text{ for } k = 3a^2b \\ \therefore\ & 6a^2b \text{ is even.} \end{aligned}$$

Prime and Composite Number Definition Let P(n) be the predicate ”n is a prime number”.

$$\forall n \in \mathbb{Z}_{>1}, P(n) \iff \forall r, s \in \mathbb{Z}_{>1}, n = rs \implies r = n \vee s = n$$
$$\forall n \in \mathbb{Z}_{>1}, \neg P(n) \iff \exists r, s \in \mathbb{Z}_{>1} \ni n = rs \wedge 1 < r < n \wedge 1 < s < n$$

Constructive Proof of Existential Statement

$$\exists xinD \ni Q(x)$$

- Find an x in D that makes !(x) true.
- Give a set of directions for finding such an x in D

Example Prove there is and even integer n such that n can be written in two ways as a sum of two prime numbers.

$$\begin{aligned} &\text{Let } n = 10, \\ &\quad 10 = 3 + 7 \\ &\quad 10 = 5 + 5 \\ &\therefore \quad \text{the statement is true.} \end{aligned}$$

Disproving Universal Statement by Counterexample

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

- Find an x in D that makes P(x) true, but Q(x) false.

Method of Exhaustion of Proving Universal Statement

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

- Check all x in D to make sure that when P(x) is true, Q(x) is false.

Direct Proof of Universal Statement

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

- Suppose x is an arbitrary element in D for which the hypothesis P(x) is true.
- Using definitions or previously established results and rules to conclude Q(x) is true.

Example Prove the statement ”the sum of any two even integers is even.”

$$\begin{aligned} & \text{Suppose a and b are two even integers} \\ \therefore \quad & a = 2k, \exists k_1 \in \mathbb{Z} \\ \therefore \quad & b = 2k, \exists k_2 \in \mathbb{Z} \\ \therefore \quad & a + b = 2k_1 + 2k_2 \\ \therefore \quad & a + b = 2(k_1 + k_2) \\ \therefore \quad & a + b \text{ is even} \end{aligned}$$

4.2 Skipped

4.3 Rational Numbers

Definitions

- A real number r is rational if and only if $\exists a, b \in \mathbb{Z}$ such that $r = \frac{a}{b} \wedge b \neq 0$.
- A real number that is not rational is irrational.

Example Is 320.5492492492... a rational number? (The 492 repeats). We can split the number into two parts: 320.5 and 0.0492492...

First we rewrite 320.5 as a fraction:

$$320.5 = \frac{3205}{10}$$

Then we rewrite 0.0492492... as a fraction:

$$10000(0.0492492...) - 10(0.0492492...) = 492.492... = 0.492492... = 492$$

$$\Rightarrow \quad 10000x - 10x = 492$$

$$\Rightarrow \quad 9990x = 492$$

$$\Rightarrow \quad x = \frac{492}{9990}$$

Now we can combine the two fractions:

$$320.5492492... = \frac{3205}{10} + \frac{492}{9990}$$

$$\Rightarrow \quad \frac{3205 \cdot 999}{10 \cdot 999} + \frac{492 \cdot 1}{9990}$$

$$\Rightarrow \quad \frac{3205 \cdot 999 + 492}{9990}$$

$$\Rightarrow \quad \frac{3199995 + 492}{9990}$$

$$\Rightarrow \quad \frac{3200487}{9990}$$

$\therefore$ 320.5492492... is rational.

Zero Product Property

Theorem If neither of two real numbers is zero, then their product is nonzero. The contrapositive of this theorem is also true: If the product of two real numbers is zero, then at least one of the two numbers is zero.

$$\begin{aligned}
&\text{Let } a, b \in \mathbb{Q}\\
&\text{If } ab = 0 \Rightarrow a = 0 \vee b = 0\\
&\text{If } ab \neq 0 \Rightarrow a \neq 0 \wedge b \neq 0
\end{aligned}$$

Example

$$\begin{aligned}
&\text{Let } a, b \in \mathbb{Q} : && \\
\therefore\quad & a = \frac{n_1}{d_1}, \exists n_1, d_1 \in \mathbb{Z} \wedge d_1 \neq 0 && \text{Definition of rational numbers.}\\
\therefore\quad & b = \frac{n_2}{d_2}, \exists n_1, d_1 \in \mathbb{Z} \wedge d_2 \neq 0 && \\
\therefore\quad & a + b = \frac{n_1}{d_1} + \frac{n_2}{d_2} && \text{Substitution principle.}\\
\therefore\quad & a + b = \frac{n_1 d_2 + n_2 d_1}{d_1 d_2} && \\
\therefore\quad & d_1 d_2 \neq 0 && \text{Zero product property}\\
\therefore\quad & a + b \text{ is rational} &&
\end{aligned}$$

Corollaries

Definition A corollary is a statement whose truth can be immediately deduced from a theorem that has already been proven.

Example Prove that the product of two rational numbers is rational.

$$\begin{aligned}
&\text{Let } a, b \in \mathbb{Q}: \\
\therefore\quad & a = \frac{n}{m}, \exists n, m \in \mathbb{Z} \land m \neq 0 && \text{Definition of rational numbers.} \\
\therefore\quad & b = \frac{s}{t}, \exists s, t \in \mathbb{Z} \land t \neq 0 \\
\therefore\quad & a \cdot b = \frac{n}{m} \cdot \frac{s}{t}, m \neq 0 \land t \neq 0 \\
\therefore\quad & ab = \frac{ns}{mt}, mt \neq 0 && \text{Zero product property.} \\
\therefore\quad & ab \in \mathbb{Q}
\end{aligned}$$

Example Prove or disprove by counterexample the following statement: "The quotient of any 2 rational numbers is rational."

$$\begin{aligned}
& \forall p, q \in \mathbb{Q}, \frac{p}{q} \in \mathbb{Q} && \text{Statement} \\
& \text{Let } p = 1, q = 0 \\
\therefore\quad & \frac{p}{q} \notin \mathbb{Q} \\
\therefore\quad & \exists p, q \in \mathbb{Q} \ni \frac{p}{q} \notin \mathbb{Q}
\end{aligned}$$

Example Prove or disprove by counterexample the following statement: $\forall a, b \in \mathbb{R}, a < b \implies a < \frac{a+b}{2} < b$.

$$\begin{aligned}
\therefore\quad & a < b \implies a + b < 2b \\
\because\quad & \frac{1}{2} > 0 \\
\therefore\quad & a < b \land \frac{1}{2} > 0 \implies \frac{a+b}{2} < \frac{b}{2} \\
\therefore\quad & a < b \implies 2a < b + a \\
\because\quad & \frac{1}{2} > 0 \\
\therefore\quad & a < b \land \frac{1}{2} > 0 \implies a < \frac{a+b}{2} \\
\therefore\quad & a < \frac{a+b}{2} \land \frac{a+b}{2} < b \equiv a < \frac{a+b}{2} < b
\end{aligned}$$

4.4 Divisibility

Definitions If n and d are integers and d $\neq$ 0, then n is divisible by d if and only if n = dk for some integer k.

- Notation: $d|n$ is read "d divides n".
  - $d|n \iff \exists k \in \mathbb{Z} \ni n = dk$
  - Note that the factor comes first in this notation.

It is equivalent to the following statements:

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

Example Prove the following statement: $\forall a, b, c \in \mathbb{Z}, a|b \wedge a|c \implies a|(b+c)$.

	Suppose $a, b, c \in \mathbb{Z} \wedge a|b \wedge a|c$	
$\therefore$	$b = ak, \exists k \in \mathbb{Z}$	Definition of Divisibility
$\therefore$	$c = am, \exists m \in \mathbb{Z}$	
$\therefore$	$b + c = a(k+m)$	Substitution and distributive
$\therefore$	$k + m \in \mathbb{Z}$	Integers are closed under addition
$\therefore$	$a|(b+c)$	Def. of divisibility

Divisibility Theorems

Positive Divisor of a Positive Integer Theorem

$$\forall a, b \in \mathbb{Z}, a > 0 \wedge b > 0 \wedge a|b \implies a \leq b.$$

Divisors of 1 Theroem The only divisors of 1 are 1 and -1.

Transistivity of Divisibility Theorem

$$\forall a, b, c \in \mathbb{Z}, a|b \wedge b|c \implies a|c$$

Divisible by a Prime Theorem Any integers n ¿ 1 is divisible by a prime number.

Unique Factorization of Integers Theorem Given any integers n ¿ 1, there exists k many distinct prime numbers $(p_1, \ldots, p_k)$ and k many positive integers $(e_1, \ldots, e_k)$, where k is a positive integer, such that:

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

Example If $a = \prod_{i=1}^{k} p_i^{e_i}$, find the standard factored form of a^2:

$$\begin{aligned} a^2 &= \prod_{i=1}^{k} p_i^{e_i} \cdot \prod_{i=1}^{k} p_i^{e_i} \\ &= (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \cdot (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\ &= p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k} \\ &= \prod_{i=1}^{k} p_i^{2e_i} \end{aligned}$$

4.5 The Quotient-Remainder Theorem

Theorem

$$\forall n \in \mathbb{Z}, \forall d \in \mathbb{Z}^+, \exists q, r \in \mathbb{Z} \ni n = dq + r \land 0 \leq r < d$$

Definition Given any integer n and any positive integer d:

$$n \div d = q$$
$$n \mod d = r$$

Example If today is tuesday, what day of the week will it be in 365 days?

$$365 \mod 7 = 1 \text{Tuesday} + 1 \text{ day} = \text{Wednesday}$$

The Parity Property

Definition We call the fact that any integer is either even or odd the parity property.

(Method of Proof by Division Into Cases) To prove a statement of the form "If $A_1 or A_2 \ldots or A_n$, then C."

Example The product of two consecutive integers is even.

$\exists n \in \mathbb{Z}$

Case 1: $2|n$

$$\begin{aligned}
&\therefore \quad 2|n \implies \exists k \in \mathbb{Z} \ni n = 2k \implies n+1 = 2k+1 \\
&\therefore \quad n(n+1) = 2k(2k+1) = 2(2k^2+k) \\
&\therefore \quad k \in \mathbb{Z} \implies 2k^2+k \in \mathbb{Z} \\
&\therefore \quad n(n+1) = 2(2k^2+k) \wedge 2k^2+k \in \mathbb{Z} \implies [2|n(n+1)]
\end{aligned}$$

Case 2: $\neg(2|n)$

$$\begin{aligned}
&\therefore \quad \neg(2|n) \implies \exists k \in \mathbb{Z} \ni n = 2k+1 \implies n+1 = 2k+2 \\
&\therefore \quad n(n+1) = (2k+1)(2k+2) = 2(2k^2+3k+1) \\
&\therefore \quad k \in \mathbb{Z} \implies 2k^2+3k+1 \in \mathbb{Z} \\
&\therefore \quad n(n+1) = 2(2k^2+3k+1) \wedge 2k^2+3k+1 \in \mathbb{Z} \implies [2|n(n+1)] \\
&\therefore \quad [2|n(n+1)]
\end{aligned}$$

Absolute Value

Definition For any real number x, the absolute value of x, delotes —x—, is defined as:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Lemma

$$\forall r \in \mathbb{R}, -|r| \leq r \leq |r|$$
$$\forall r \in \mathbb{R}, |-r| = |r|$$

The Triangle Inequality

$$\forall x, y \in \mathbb{R}, |x+y| \leq |x| + |y|$$

4.6 Skipped

4.7 Contradiction and Contraposition

Method of Proof by Contradiction

- Suppose the opposite of the to-be proved conclusion.
- Show that this supposition leads logically to a contradiction (a statement that is always false).
- Conclude that the statement to be broved is true.

Example Prove the theorem by contradiction: ”There is no greatest integer.”

$$\begin{array}{rll}
\text{Suppose:} & \exists m \in \mathbb{Z} \ni \forall n \in \mathbb{Z}, n \leq m & \text{Opposite of theorem} \\
\therefore & \exists n \in \mathbb{Z} \ni n = m + 1 & \\
\therefore & \nexists m \in \mathbb{Z} \ni \forall n \in \mathbb{Z}, n \leq m &
\end{array}$$

Example Prove the theorem by contradiction: ”The square root of any irrational number is irrational.”

$$\begin{array}{rlr}
\text{Theorem:} & \forall n \notin \mathbb{Q}, \sqrt{n} \notin \mathbb{Q} & \text{Theorem} \\
\text{Suppose:} & \forall n \notin \mathbb{Q}, \sqrt{n} \in \mathbb{Q} & \text{Opposite of theorem} \\
\therefore & \sqrt{n} \in \mathbb{Q} \implies \exists a, b \in \mathbb{Z} \ni \sqrt{n} = \dfrac{a}{b} \land b \neq 0 & \text{Definition of rational numbers} \\
\therefore & \sqrt{n} = \dfrac{a}{b} \implies n = \dfrac{a^2}{b^2} & \text{Squaring both sides} \\
\therefore & a, b \in \mathbb{Z} \implies a^2, b^2 \in \mathbb{Z} & \text{Integers are closed under squaring} \\
\therefore & n = \dfrac{a^2}{b^2} \land a^2, b^2 \in \mathbb{Z} \implies n \in \mathbb{Q} & \text{Definition of rational numbers} \\
\therefore & n \in \mathbb{Q} \land n \notin \mathbb{Q} & \text{Contradiction} \\
\therefore & \text{The assumption is false, and the theorem is true.} &
\end{array}$$

Example Prove the theorem by contradiction: ”The sum of any rational number and any irrational number is irrational.”

Theorem: $\forall n \in \mathbb{Q}, \forall m \notin \mathbb{Q}, n + m \notin \mathbb{Q}$

$$\begin{array}{rll}
\text{Suppose:} & \forall n \in \mathbb{Q}, \forall m \notin \mathbb{Q}, n + m \in \mathbb{Q} & \text{Opposite of theorem} \\
\therefore & n + b \in \mathbb{Q} \implies \exists a, b \in \mathbb{Z} \ni n + m = \dfrac{a}{b} \wedge b \neq 0 & \text{Definition of rational numbers} \\
\therefore & m = \dfrac{a}{b} - n & \\
\therefore & n \in \mathbb{Q} \implies \exists x, y \in \mathbb{Z} \ni n = \dfrac{x}{y} \wedge y \neq 0 & \text{Definition of rational numbers} \\
\therefore & m = \dfrac{a}{b} - \dfrac{x}{y} & \\
\therefore & m = \dfrac{ay - bx}{by} \implies m \in \mathbb{Q} & \\
\therefore & m \in \mathbb{Q} \wedge m \notin \mathbb{Q} & \text{Contradiction} \\
\therefore & \forall n \in \mathbb{Q}, \forall m \notin \mathbb{Q}, n + m \notin \mathbb{Q} & \text{The theorem is true.}
\end{array}$$

Method of Proof by Contraposition

- Express the given statement in the form of ”$\forall x \in D, P(x) \implies Q(x)$”.
- Rewrite in contrapositive form: ”$\forall x \in D, \neg Q(x) \implies \neg P(x)$”.
- Prove the contrapositive by direct proof.
  - Suppose $\exists x \in D \ni \neg Q(x)$.
  - Prove $\neg P(x)$.

Example Prove the statement by contraposition: ”For all integers m and n, if mn is even then m is even or n is even.”

$$\begin{aligned}
\text{Theorem:}\quad & \forall m, n \in \mathbb{Z}, 2|mn \implies 2|m \lor 2|n \\
\text{Contrapositive:}\quad & \forall m, n \in \mathbb{Z}, \neg(2|m) \land \neg(2|n) \implies \neg(2|mn)
\end{aligned}$$

$$\begin{aligned}
\text{Suppose:}\quad & \exists m, n \in \mathbb{Z} \ni \neg(2|m) \land \neg(2|n) \\
\therefore\quad & \neg(2|m) \land \neg(2|n) \implies \exists k, l \in \mathbb{Z} \ni m = 2k+1 \land n = 2l+1 \\
\therefore\quad & mn = (2k+1)(2l+1) \\
\implies\quad & mn = 4kl + 2k + 2l + 1 \implies mn = 2(2kl + k + l) + 1 \\
\therefore\quad & k, l \in \mathbb{Z} \implies 2kl + k + l \in \mathbb{Z} \\
\therefore\quad & mn = 2(2kl + k + l) + 1 \land 2kl + k + 1 \in \mathbb{Z} \implies \neg(2|mn)
\end{aligned}$$

5. Sequences, Induction, and Recursion

5.1 Sequences

Definiton A sequence is a function whose **domain** is either all the **integers** between two given integers or all the integers greater than or equal to a given integers.

Notation

$$\begin{aligned} a_1 &= f(1) \\ &\dots \\ a_{n-1} &= f(n-1) \\ a_n &= f(n) \\ a_{n+1} &= f(n+1) \end{aligned}$$

Example Write the first three terms of the sequence whose **explicit** or **general formula** is given:

$$\begin{aligned} a_n &= \frac{(-1)^n}{2^n+1} \text{ for } n \geq 1 \\ a_1 &= \frac{(-1)^1}{2^1+1} = -\frac{1}{3} \\ a_2 &= \frac{(-1)^2}{2^2+1} = \frac{1}{5} \\ a_3 &= \frac{(-1)^3}{2^3+1} = -\frac{1}{9} \end{aligned}$$

Summation Notation

Definition If m and n are integers and m ≤ n, then a **series** can be notated as:

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

- **Read as** "the summation from i = m to n of a-sub-i"
- **i** is called the **index** of the Summation
- **m** is called the **lower limit** of the Summation
- **n** is called the **upper limit** of the summation

Example Expand and evaluate the following:

$$\begin{aligned}&\sum_{i=2}^{6}(i-1)^2\\&= 1+4+9+16+25\\&= 55\end{aligned}$$

Re-indexing a Summation Re-indexing a summation involves changing the index variable or the limits of summation, often to simplify the expression or to match another sum's index.

$$\begin{aligned}&\sum_{i=1}^{n+1}\frac{1}{i^2}\\=&\sum_{i=1}^{n}\frac{1}{i^2}+\frac{1}{(n+1)^2}\end{aligned}$$

Example If $j = i + 1$, transform the following summation by rewriting it in terms of j: $\sum_{i=4}^{k-1} i(i-1)$

$$\begin{aligned} &i = 4 \implies j = 4 + 1 = 5 && \text{Rewrite lower limit.} \\ &i = k - 1 \implies j = k - 1 + 1 = k && \text{Rewrite upper limit} \\ &j = i + 1 \implies i = j - 1 && \text{Rewrite i in terms of j} \\ &\sum_{j=5}^{k} (j-1)(j-2) && \text{Rewrite sum} \end{aligned}$$

Product Notation

Definition If m and n are integers andm ≤ n, then a **series** can be notated as:

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

- **Read as** "the product from i = m to n of a-sub-i"
- **i** is called the **index** of the product
- **m** is called the **lower limit** of the product
- **n** is called the **upper limit** of the product

Example Expand and evaluate the following:

$$\begin{aligned} &\prod_{k=2}^{5} \frac{k}{k+1} \\ &= \frac{2}{2+1} \cdot \frac{3}{3+1} \cdot \frac{4}{4+1} \cdot \frac{5}{5+1} \\ &= \frac{1}{3} \end{aligned}$$

Theorem Given sequences $\{a\}$ and $\{b\}$ and $c \in \mathbb{R}$, the following equations hold:

$$\sum_{i=m}^{n} a_i + \sum_{i=m}^{n} b_i = \sum_{i=m}^{n} (a_n + b_n)$$
$$c \cdot \sum_{i=m}^{n} a_i = \sum_{i=m}^{n} c \cdot a_i$$
$$\prod_{i=m}^{n} a_i \cdot \prod_{i=m}^{n} b_i = \prod_{i=m}^{n} (a_i b_i)$$

Factorials

$$n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$$

Binomial Coefficient

Definition Let n and r be integers with $0 \leq r \leq n$, the binomial coeffecient is notated as:

$$nCr = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

It presents the number of combinations of choosing r items from n choices.

Example Evaluate:

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = \frac{5 \cdot 4}{2 \cdot 1} = 10$$

5.2 Mathematical Induction 1: Proving Formulas

Method of Proof by Induction

Definition Induction proof explores the **patterns** we recognize from a list of unknown terms.

Method Consider the statement $\forall n \in \{a \in \mathbb{Z} : n \geq a\}, P(n)$

- Step 1: **(basis step):** Show that P(a) is true.
- Step 2: **(inductive step):** Show that if we suppose P(k) is true, then P(k+1) is true.

Example Use the formula to evaluate $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

$$\begin{aligned}\text{Suppose } n &= 50\\ 1 + 2 + \cdots + 50 &= \frac{50(50+1)}{2}\\ &= \frac{50(51)}{2}\\ &= \frac{2550}{2}\\ &= 1275\end{aligned}$$

Definition If a sum with a variable number of terms is show to equal an expression that does not contain either an ellipsis or a summation sign, we can say that the sum is written in **closed form**.

Example Use the formula to evaluate $1 + 2 + \cdots + n$

Geometric Series

Definition If $r \in \mathbb{R} \wedge r \neq 1$, the sum of the first n terms of a geometric series is given by:

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

Example Use the above formula to evaluate $1 + 3 + \cdots + 3^{m-2}$

$$\begin{aligned} r &= 3, n = m - 2 \\ 1 + 3 + \cdots + 3^{m-2} &= \sum_{i=0}^{m-2} 3^i \\ &= \frac{3^{m-1} - 1}{3 - 1} = \frac{3^{m-1} - 1}{2} \end{aligned}$$

Example $3^2 + 3^3 + \cdots + 3^m$

$$\begin{aligned} & 3^2 + 3^3 + \cdots + 3^m = 1 + 3 + 3^2 + 3^3 + \cdots + 3^m - (1 + 3) \\ \Longrightarrow\ & [3^0 + 3^1 + 3^2 + 3^3 + \cdots + 3^m] - 4 = \sum_{i=0}^{m} 3^i - 4 \quad (r = 3, n = m) \\ \Longrightarrow\ & \sum_{i=0}^{m} 3^i - 4 = \frac{3^{m+1} - 1}{3 - 1} - 4 = \frac{3^{m+1} - 9}{2} \end{aligned}$$

5.3 Mathematical Induction 2

Deduction and Induction

Definitions

- **Deduction** is to infer a conclusion from general principles using laws of logical reasoning.
- **Induction** is to infer a general principle from specific examples.

Example Use mathematical induction to prove
$\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, 3|(2^{2n} - 1)$:

Step 0: Identify the property P(n)

$$P(n) \equiv 3|(2^{2n} - 1)$$

Step 1: Prove P(0)

$$2^{2(0)} - 1 = 2^0 - 1 = 1 - 1 = 0$$

$$3|0$$

$$\therefore \quad 3|(2^{2(0)} - 1)$$

Step 2: Suppose P(k) is true for $k \geq 0,$ then prove P(k+1)

$$\begin{aligned}
&\text{Suppose } 3|(2^{2k} - 1) \\
\implies &\exists m \in \mathbb{Z} \ni 2^{2k} - 1 = 3m \\
\implies &2^{2(k+1)} - 1 = 2^{2k} \cdot 2^2 - 1 \\
\implies &2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1 \\
\implies &2^{2(k+1)} - 1 = 4(2^{2k} - 1) + 3 \\
\implies &2^{2(k+1)} - 1 = 4(3m) + 3 \\
\therefore \quad &3|(2^{2(k+1)} - 1)
\end{aligned}$$

Example Use mathematical induction to prove
$\forall n \in \{x \in \mathbb{Z} : x \geq 5\}, n^2 < 2^n$

Base Step: $n = 5$

$5^2 < 2^5 = 25 < 32$

Inductive Step: Suppose $\forall k \in \{x \in \mathbb{Z} : x \geq 5\}, k^2 < 2^k$ then prove $(k+1)^2 < 2^{k+1}$

LHS $= (k+1)^2$

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

$k^2 < 2^k \implies k^2 + 2k + 1 < 2^k + [2k+1]$

RHS $= 2^{k+1}$

$2^{k+1} = 2^k \cdot 2^1 = 2^k + [2^k]$

Prove $(k+1)^2 < 2^{k+1}$ for $k \geq 5$:

$2 \cdot 5 + 1 = 11 < 32 = 2^5$

$2 \cdot 6 + 1 = 13 < 64 = 2^6$

$2 \cdot 7 + 1 = 15 < 128 = 2^7$

and so on.

$\therefore \quad \forall k \in \{x \in \mathbb{Z} : x \geq 5\}, 2k + 1 < 2^k$

$\therefore \quad \forall k \in \{x \in \mathbb{Z} : x \geq 5\}, (k+1)^2 < 2^{k+1}$

$\therefore \quad \forall k \in \{x \in \mathbb{Z} : x \geq 5\}, k^2 < 2^k$

Recursion

Definition A **recursion** is a function that is defined in terms of itself. A recursive function is a function that calls itself.

Example $a_k = 5a_{k-1}$ for all integers $k \geq 2$.

5.4 Strong Mathematical Induction

Principle of Strong Mathematical Induction

Let P(n) be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$.

- Basis Step: Show that P(a), P(a+1), . . . , P(b) are all true.
- Inductive Step: Show that for every ingeger $k \geq b$, if P(a), P(a+1), . . . , P(k) are all true, then P(k+1) is true.

Example Define a sequence:

$$S_0 = 0$$
$$S_1 = 4$$
$$\forall k \in \{x \in \mathbb{Z} : x \geq 2\}, S_k = 6S_{k-1} - 5S_{k-2}$$

Prove $\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, S_n = 5^n - 1$:

Let $G = \{x \in \mathbb{Z} : x \geq 0\}$

Basic step:
$S_0 = 5^0 - 1 = 1 - 1 = 0$
$S_1 = 5^1 - 1 = 5 - 1 = 4$

Inductive step:
Suppose $\forall k \in G, S_k = 5^k - 1$

$\implies \quad S_{k+1} = 6S_k - 5S_{k-1} = 6(5^k - 1) - 5(5^{k-1} - 1) = 6(5^k) - 6 + 5(5^{k-1}) + 5$
$= 6(5^k) - (5^{k-1+1}) - 1 = (6-1)5^k - 1 = 5 \cdot 5^k - 1 = 5^{k+1} - 1$
$\therefore \quad S_{k+1} = 6S_k - 5S_{k-1}$

$\therefore \quad \forall n \in \{x \in \mathbb{Z} : x \geq 0\}, S_n = 5^n - 1$

Well-Ordering Principle for the Integers

Definition Let S be a **non-empty** set of **integers**. If all elements in S are greater than some fixed integers, then S has a **least element.** For the well-ordering principle to work:

- The set must be integers.
- The set must be non-empty.
- The set must be greater than some fixed integers.

5.5 Skipped

5.6 Solving Recurrence relations by Iteration

Method Starting from the initial conditions, calculate the successive terms of sequences from the recurrence formula until a pattern emerges. Then, use the pattern to find a closed form for the sequence.

Example

$$a_n = \begin{cases} 1, & n = 0 \\ a_{n-1} + 2, & \forall n \in \mathbb{Z}^+ \end{cases}$$

Solve the recurrence relation.

$$\begin{aligned} \forall n \in \mathbb{Z}^+, a_k &= a_{k-1} + 2 \\ a_n &= (a_{n-1} + 2) + 2 \\ a_n &= (a_{n-2} + 2) + 2(2) \\ &\cdots \\ a_n &= a_{n-k} + k(2) \\ \therefore \quad \forall n \in \mathbb{Z}^+, \quad a_n &= a_0 + 2n \\ \therefore \quad \forall n \in \mathbb{Z}^+, \quad a_n &= 1 + 2n \end{aligned}$$

Arithmetic Sequence

Definition A sequence is arithmetic if there is a constant d such that:

$$\forall k \in \mathbb{Z}^+, \quad a_k = a_{k-1} + d$$

General Formula

$$\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, \quad a_n = a_0 + nd$$

Geometric Sequence

Definition A sequence is geometric if there is a constant r such that:

$$\forall k \in \mathbb{Z}^+, \quad a_k = a_{k-1}r$$

General Formula

$$\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, \quad a_n = a_0 r^n$$

Example Use iteration to find the explicit formula of the following sequence:

$$e_k = \begin{cases} 2, & k = 0 \\ 4e_{k-1} + 5, & k \geq 0 \end{cases}$$

$$\begin{aligned}
e_0 &= 2 \\
e_1 &= 4(2) + 5 \\
e_2 &= 4(4(2) + 5) + 5 = 4^2(2) + 4(5) + 5 \\
e_3 &= 4(4^2(2) + 4(5) + 5) + 5 = 4^3(2) + 4^2(5) + 4(5) + 5 \\
&\ \ldots \\
e_k &= 4^k(2) + 4^{k-1}(5) + 4^{k-2}(5) + \cdots + 4(5) + 5 \\
&= 4^k(2) + 5\sum_{i=0}^{k-1} 4^i = 4^k(2) + 5(\frac{4^{k-1+1} - 1}{4 - 1}) \\
e_k &= 4^k(2) + 5(\frac{4^k - 1}{3})
\end{aligned}$$

6. Chapter 6

6.1 Set Theory

Definitions

$$\begin{aligned} A \subseteq B &\iff \forall x \in A \implies x \in B \\ A \nsubseteq B &\iff \exists x \in A \implies x \neq B \end{aligned}$$

A is a **proper subset** of B ($A \subset B$) if and only if:

- $A \subseteq B$ and
- $\exists x$ such that $x \in B$ and $x \notin A$

Example Let

$$\begin{aligned} A &= \{m \in \mathbb{Z} | \exists r \in \mathbb{Z} \ni m = 6r + 12\} \\ B &= \{n \in \mathbb{Z} | \exists s \in \mathbb{Z} \ni n = 3s\} \end{aligned}$$

$A \subseteq B?$:

$$\begin{aligned} & 6r + 12 = 6(r+2) \implies A = \{m \in \mathbb{Z} | \exists t \in \mathbb{Z} \ni m = 6t\} \\ & m = 6n \implies m = 3(2n) \\ \therefore \quad & A \subseteq B \end{aligned}$$

Set Equivalence

Definition Given sets A and B:

$$A = B \iff A \subseteq B \wedge B \subseteq A \tag{2}$$

Example Let

$$\begin{aligned}
R &= \{x \in \mathbb{Z} : 2|x\} \\
T &= \{x \in \mathbb{Z} : 6|x\}
\end{aligned}$$

$$\begin{aligned}
&R \subseteq T \equiv \text{False} \\
&\qquad Letx \in Randx = 2(1) = 2,\ \text{but}\ 2 \neq 6k\forall k \in \mathbb{Z} \\
\implies &\qquad x \notin T \\
\therefore &\qquad R \nsubseteq T \\
\\
&T \subseteq R \equiv \text{True} \\
\therefore &\qquad R \neq T \\
&\qquad Letx \in T \\
\implies &\qquad \exists k \in \mathbb{Z} \ni x = 6k \implies x = 2(3k) \\
\implies &\qquad 3k \in \mathbb{Z} \implies 2|x \implies x \in R \\
\therefore &\qquad T \subseteq R
\end{aligned}$$

Venn Diagrams

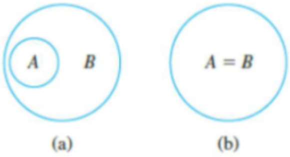
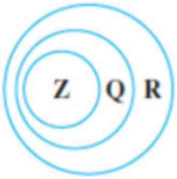


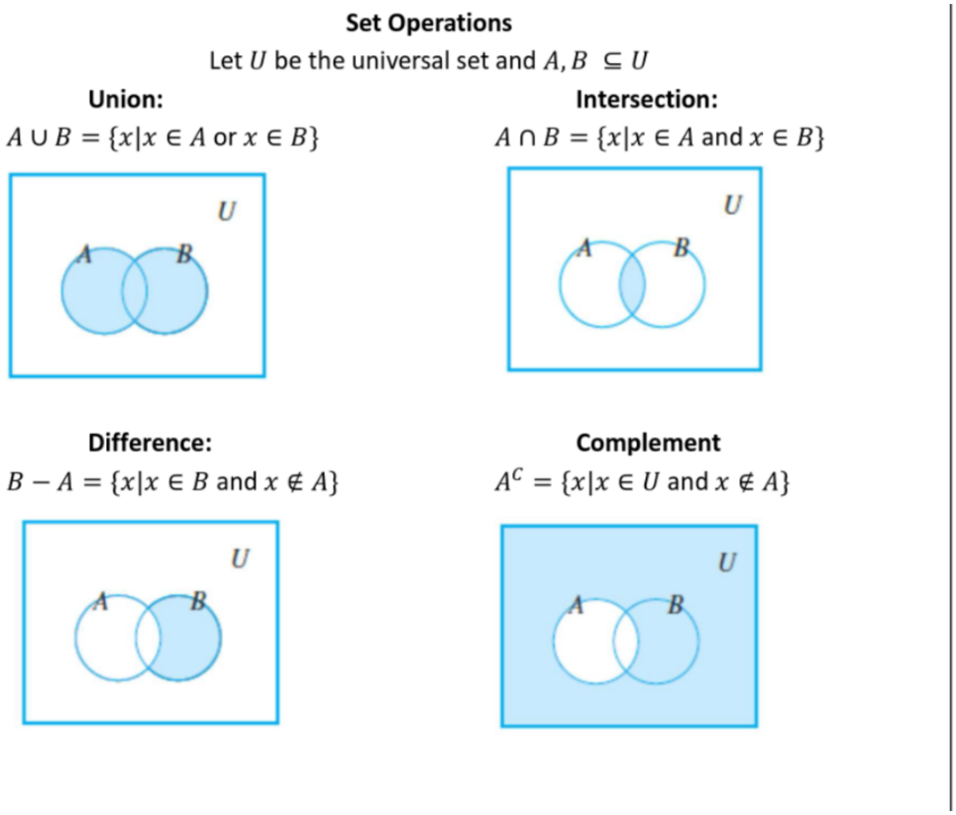
FIGURE 6.1.1 $A \subseteq B$

$\mathbb{R}$: set of real numbers

$\mathbb{Q}$: set of rational numbers

$\mathbb{Z}$: set of integers





Set Operations

Let U be the universal set and $A, B \subseteq U$

Union:

$A \cup B = \{x | x \in A \text{ or } x \in B\}$

Intersection:

$A \cap B = \{x | x \in A \text{ and } x \in B\}$

Difference:

$B - A = \{x | x \in B \text{ and } x \notin A\}$

Complement

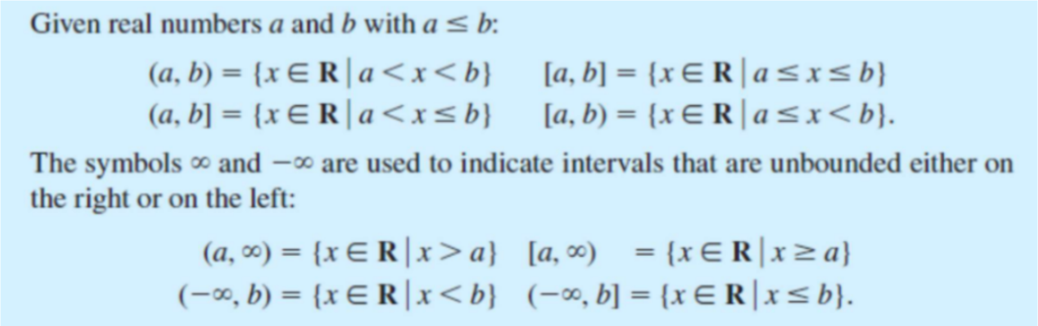
$A^C = \{x | x \in U \text{ and } x \notin A\}$

Example Let

$$
\begin{aligned}
U &= \{1, 2, 3, 4, 5, 6, 7\} \\
A &= \{1, 3, 5, 7\} \\
B &= \{4, 5, 6, 7\}
\end{aligned}
$$

$$
\begin{aligned}
A \cup B &= \{1, 3, 4, 5, 6, 7\} \\
A \cap B &= \{5, 7\} \\
B - A &= \{4, 6\} \\
A^c &= \{2, 4, 6\}
\end{aligned}
$$

Interval Notation



Given real numbers a and b with $a \leq b$:

$$(a, b) = \{x \in \mathbf{R} \mid a < x < b\} \qquad [a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}$$
$$(a, b] = \{x \in \mathbf{R} \mid a < x \leq b\} \qquad [a, b) = \{x \in \mathbf{R} \mid a \leq x < b\}.$$

The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:

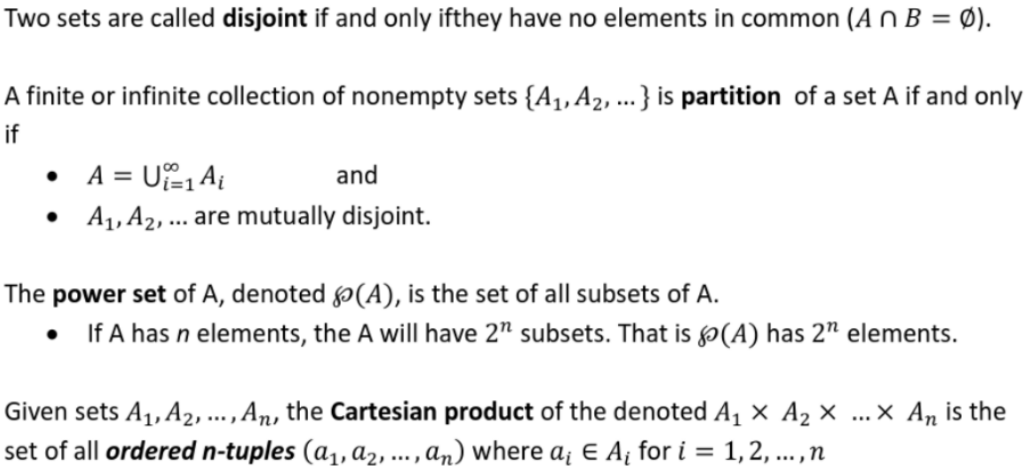
$$(a, \infty) = \{x \in \mathbf{R} \mid x > a\} \quad [a, \infty) \quad = \{x \in \mathbf{R} \mid x \geq a\}$$
$$(-\infty, b) = \{x \in \mathbf{R} \mid x < b\} \quad (-\infty, b] = \{x \in \mathbf{R} \mid x \leq b\}.$$

Example Let $U = \mathbb{R}$,$A = (-1, 0]$ and $B = [0, 1)$

$$\begin{aligned} A \cup B &= \{-1, 1\} \\ A \cap B &= \{0\} \\ B - A &= (0, 1) \\ A^c &= (-\infty, 1] \cup (0, \infty) \end{aligned}$$

Disjoint Sets

Definition



Two sets are called **disjoint** if and only ifthey have no elements in common ($A \cap B = \emptyset$).

A finite or infinite collection of nonempty sets $\{A_1, A_2, \ldots\}$ is **partition** of a set A if and only if

- $A = \bigcup_{i=1}^{\infty} A_i$ and
- $A_1, A_2, \ldots$ are mutually disjoint.

The **power set** of A, denoted $\wp(A)$, is the set of all subsets of A.

- If A has *n* elements, the A will have 2^n subsets. That is $\wp(A)$ has 2^n elements.

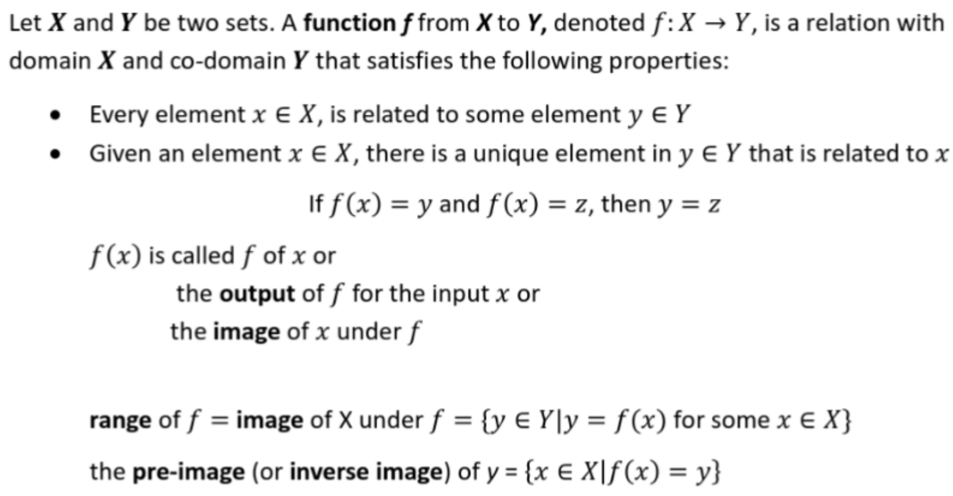
Given sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of the denoted $A_1 \times A_2 \times \ldots \times A_n$ is the set of all ***ordered n-tuples*** $(a_1, a_2, \ldots, a_n)$ where $a_i \in A_i$ for $i = 1, 2, \ldots, n$

Example Find $\mathcal{P}(A)$ if $A = \{1, 2\}$

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

7. Functions

Functions Defined on General Sets



Let ***X*** and ***Y*** be two sets. A **function *f*** from ***X*** to ***Y*,** denoted $f: X \rightarrow Y$, is a relation with domain ***X*** and co-domain ***Y*** that satisfies the following properties:

- Every element $x \in X$, is related to some element $y \in Y$
- Given an element $x \in X$, there is a unique element in $y \in Y$ that is related to x

If $f(x) = y$ and $f(x) = z$, then $y = z$

$f(x)$ is called f of x or
the **output** of f for the input x or
the **image** of x under f

range of f = **image** of X under $f = \{y \in Y | y = f(x)$ for some $x \in X\}$

the **pre-image** (or **inverse image**) of $y = \{x \in X | f(x) = y\}$

Theorem: Function Equality Let X and Y be two sets: If $F : X \rightarrow Y$ and $G : X \rightarrow Y$, are two functions, then $F = G \iff \forall x \in X, F(x) = G(x)$

Identitiy Functions Let X be a set. Define a function $I_X : X \rightarrow X$ by:

$$\forall x \in X, I_X(x) = x$$

Not Well Defined Functions A function is not well defined if

- there is no y that satisfies the given equation.
- There are two different values of y that satisfy the equations.

Example Suppose $f : \mathbb{Q} \rightarrow \mathbb{Z}$ is defined as:

$$\forall m, n \in \mathbb{Z}, \forall \frac{m}{n} \in \mathbb{Q}, f(\frac{m}{n}) = m - n \land n \neq 0$$

Explain why f is not well defined:
$f(\frac{1}{2}) = -1$ and $f(\frac{2}{4}) = 2$, so f is not well defined.

Function Types: Injective, Surjective, Bijective

Injective (One-to-One) Functions A function $f : X \to Y$ is **injective** if for all $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. That is, no two different elements in the domain map to the same element in the codomain.
Injective functions may leave some elements in the codomain unused, but they never "collide" two domain elements to the same output.

Example: $f(x) = 2x$ from $\mathbb{R} \to \mathbb{R}$ is injective.

Example: Define $f : \mathbb{R} \to \mathbb{R}$ as $f(x) = 4x - 1 \forall x \in \mathbb{R}$. Is f injective? Prove or disprove with a counterexample.

Suppose $x_1, x_2 \in \mathbb{R} \ni f(x_1) = f(x_2)$.

$$\implies \quad 4x_1 - 1 = 4x_2 - 1 \quad \implies \quad x_1 = x_2.$$

$$\therefore \quad f \text{ is injective.}$$

Surjective (Onto) Functions A function $f : X \to Y$ is **surjective** if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$. In other words, every element of the codomain is the image of at least one element from the domain.
Surjective functions may map multiple domain elements to the same codomain element, but they never leave any codomain element out.

Example: $f(x) = x^3$ from $\mathbb{R} \to \mathbb{R}$ is surjective.

Example: Define $f : \mathbb{R} \to \mathbb{R}$ as $f(x) = 4x - 1 \forall x \in \mathbb{R}$. Is f surjective? Prove or disprove with a counterexample.

$$\begin{array}{rl} & \text{Suppose } y \in \mathbb{R} \ni f(x) = y. \\ \implies & 4x - 1 = y \quad \implies \quad x = \dfrac{y+1}{4}. \\ \implies & f(x) = 4(\dfrac{y+1}{4}) - 1 = y + 1 - 1 = y. \\ \implies & \exists x \in \mathbb{R} \ni f(x) = y. \\ \therefore & f \text{ is surjective.} \end{array}$$

Example: Define $g : \mathbb{Z} \to \mathbb{Z}$ as $g(x) = 4x - 1 \forall x \in \mathbb{Z}$. Is g surjective? Prove or disprove with a counterexample.

$$\begin{array}{rl} & \text{Suppose } y \in \mathbb{Z} \ni g(x) = y. \\ \implies & 4x - 1 = y \quad \implies \quad x = \dfrac{y+1}{4}. \\ & \text{For } x \in \mathbb{Z}, y + 1 \text{ must be divisible by 4.} \\ & \text{If } y = 2, y + 1 = 3, \text{ which is not divisible by 4.} \\ \therefore & g \text{ is not surjective.} \end{array}$$

Bijective Functions A function is **bijective** (one-to-one correspondence) if it is both injective and surjective. That is, every element of the codomain is hit exactly once by a unique element of the domain.
Bijective functions are both one-to-one and onto: they never "collide" domain elements, and they never leave any codomain element out.

Example: $f(x) = x + 1$ from $\mathbb{R} \to \mathbb{R}$ is bijective.

Example: Define $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ as $f(x, y) = (x + y, x - y)$. Is f bijective? Prove or disprove with a counterexample.

Suppose $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R} \ni f(x_1, y_1) = f(x_2, y_2)$.

$\implies$ $(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2)$.

This gives us two equations:

$x_1 + y_1 = x_2 + y_2 \quad (1)$

$x_1 - y_1 = x_2 - y_2 \quad (2)$

Adding (1) and (2):

$2x_1 = 2x_2 \implies x_1 = x_2$.

Substituting $x_1 = x_2$ into (1):

$x_1 + y_1 = x_1 + y_2 \implies y_1 = y_2$.

$\therefore$ f is injective.

Now, to check surjectivity:

For any $(a, b) \in \mathbb{R} \times \mathbb{R},$ we need to find (x, y) such that $f(x, y) = (a, b)$.

Let $x = \dfrac{a+b}{2}, y = \dfrac{a-b}{2}$.

$\implies$ $f(x, y) = (x + y, x - y) = (a, b)$.

$\therefore$ f is surjective.

$\therefore$ f is bijective.

Inverse Functions

Inverse Functions A function $f : X \to Y$ has an **inverse** if there exists a function $g : Y \to X$ such that $g(f(x)) = x$ for all $x \in X$ and $f(g(y)) = y$ for all $y \in Y$. The inverse is denoted f^{-1}.

A function has an inverse if and only if it is bijective.

Example: $f(x) = 2x + 3$ from $\mathbb{R} \to \mathbb{R}$ is bijective. Its inverse is $f^{-1}(y) = \frac{y-3}{2}$.

How to Find the Inverse

1. Replace $f(x)$ with y.

2. Solve for x in terms of y.

3. Interchange x and y to get $f^{-1}(x)$.

Example: Find the inverse of $f(x) = \frac{x-1}{x+2}$ for $x \neq -2$.

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

Interchange x and y:

$$f^{-1}(x) = \frac{-1-2x}{x-1}$$

Visualizing Function Types

- **Injective:** No two arrows from different domain elements point to the same codomain element.
- **Surjective:** Every codomain element has at least one arrow pointing to it.
- **Bijective:** Each domain element maps to a unique codomain element, and every codomain element is hit.

Properties

- If f is bijective, f has an inverse f^{-1}.
- If f is injective, f may not be surjective.
- If f is surjective, f may not be injective.

Examples

- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x + 1$ is bijective.
- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x$ is injective but not surjective.
- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = \lfloor x/2 \rfloor$ is surjective but not injective.

Composition of Functions

Definition Let $f : X \to Y$ and $g : Y \to Z$ be functions. The **composition** of g and f, denoted $g \circ f$, is the function from X to Z defined by:

$$(g \circ f)(x) = g(f(x)) \quad \forall x \in X$$

Order Matters In general, $g \circ f \neq f \circ g$. The function f is applied first, then g.

Example Let $f(x) = 2x$ and $g(x) = x + 3$ with $f, g : \mathbb{R} \to \mathbb{R}$.

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) = g(2x) = 2x + 3\\(f \circ g)(x) &= f(g(x)) = f(x + 3) = 2(x + 3) = 2x + 6\end{aligned}$$

Domain and Codomain for Composition If $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$ is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in A$. The output of f must be in the domain of g.

Example: Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $C = \{\alpha, \beta, \gamma\}$. Suppose $f : A \to B$ is defined by $f(1) = a, f(2) = b, f(3) = c$ and $g : B \to C$ is defined by $g(a) = \gamma, g(b) = \alpha, g(c) = \beta$.
Then:

$$\begin{aligned}(g \circ f)(1) &= g(f(1)) = g(a) = \gamma\\(g \circ f)(2) &= g(f(2)) = g(b) = \alpha\\(g \circ f)(3) &= g(f(3)) = g(c) = \beta\end{aligned}$$

Composition Not Always Defined If the range of f is not a subset of the domain of g, then $g \circ f$ is not defined for all elements of A.

Identity and Composition For any set A, the identity function $I_A : A \to A$ satisfies $f \circ I_A = f$ and $I_B \circ f = f$ for $f : A \to B$.

Associativity of Composition If $f : A \to B$, $g : B \to C$, $h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

Example with Real Functions Let $f(x) = x^2$, $g(x) = x + 1$ on $\mathbb{R}$.

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1$$
$$(f \circ g)(x) = f(g(x)) = f(x + 1) = (x + 1)^2 = x^2 + 2x + 1$$

Summary

- The composition $g \circ f$ means apply f first, then g.
- The composition is only defined when the codomain of f matches the domain of g.
- Composition is associative but not commutative.
- The identity function acts as a neutral element for composition.

Properties

- If f and g are both injective, $g \circ f$ is injective.
- If f and g are both surjective, $g \circ f$ is surjective.
- If f and g are both bijective, $g \circ f$ is bijective.

Example Let $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x + 1$ and $g : \mathbb{Z} \to \mathbb{Z}$, $g(x) = 2x$.

$$(g \circ f)(x) = g(f(x)) = g(x + 1) = 2(x + 1) = 2x + 2$$
$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 1$$

Cardinality and Infinity

Cardinality of Sets The **cardinality** of a set A, denoted $|A|$, is a measure of the "number of elements" in A.

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

Finite Sets A set A is **finite** if $|A| = n$ for some $n \in \mathbb{N}$, i.e., there is a bijection between A and $\{1, 2, \ldots, n\}$.

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

Countable Sets A set A is **countably infinite** if there is a bijection between A and $\mathbb{N}$. A set is **countable** if it is finite or countably infinite.

Examples of Countable Sets

- $\mathbb{N}$ is countably infinite (identity function).
- $\mathbb{Z}$ is countably infinite (can be listed as $0, 1, -1, 2, -2, \ldots$).
- $\mathbb{Q}$ is countably infinite (can be listed in a sequence, e.g., by diagonals).

Uncountable Sets A set is **uncountable** if it is not countable. $\mathbb{R}$ is uncountable.

Theorem: $\mathbb{Q}$ is Countable There exists a bijection between $\mathbb{N}$ and $\mathbb{Q}$.

Theorem: $\mathbb{R}$ is Uncountable (Cantor's Diagonal Argument) Suppose $[0, 1]$ is countable and list all real numbers in $[0, 1]$ as decimals. Construct a new number by changing the nth digit of the nth number. This new number differs from every number in the list, so $[0, 1]$ is uncountable.

Comparing Cardinalities If there is an injective function from A to B, then $|A| \leq |B|$. If there is a bijection, $|A| = |B|$.

Sizes of Infinity $|\mathbb{N}|$ is the smallest infinite cardinality (”countable infinity”). $|\mathbb{R}|$ is strictly larger (”uncountable infinity”).

Summary

- Cardinality measures the size of sets.
- Countable sets can be listed in a sequence; uncountable sets cannot.
- There are different sizes of infinity.

Summary Table

Set	Countable?	Cardinality
$\mathbb{N}$	Yes	$\aleph_0$
$\mathbb{Z}$	Yes	$\aleph_0$
$\mathbb{Q}$	Yes	$\aleph_0$
$\mathbb{R}$	No	$\mathfrak{c}$

8. Relations

8.1 Relations on Sets

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

$$R \subseteq A \times B$$

If $(a, b) \in R$, we say a is related to b by R (written aRb).

Domain and Codomain

- A is the **domain** of R.
- B is the **codomain** of R.

Examples Let $A = \{1, 2, 3\}$, $B = \{x, y\}$. Define $R = \{(1, x), (2, y)\}$. R is a relation from A to B.

Types of Relations on a Set A

- **Reflexive**: $\forall a \in A,\ (a, a) \in R$
- **Symmetric**: $\forall a, b \in A,\ (a, b) \in R \implies (b, a) \in R$
- **Antisymmetric**: $\forall a, b \in A,\ (a, b) \in R \wedge (b, a) \in R \implies a = b$
- **Transitive**: $\forall a, b, c \in A,\ (a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$

Special Relations

- **Equivalence Relation**: Reflexive, symmetric, and transitive.
- **Partial Order**: Reflexive, antisymmetric, and transitive.

Notation

- $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- $R(a, b)$ or aRb means $(a, b) \in R$

Matrix Representation A relation on a finite set $A = \{a_1, ..., a_n\}$ can be represented by an $n \times n$ matrix M where $M_{ij} = 1$ if $(a_i, a_j) \in R$, else 0.

Graph Representation A relation on A can be visualized as a directed graph (digraph) with vertices for elements of A and edges for pairs in R.

Closures

- **Reflexive closure**: Add (a, a) for all $a \in A$ if missing.
- **Symmetric closure**: Add (b, a) whenever $(a, b) \in R$.
- **Transitive closure**: Add (a, c) whenever $(a, b) \in R$ and $(b, c) \in R$.

Example: Let $A = \{1, 2, 3\}$, $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$. R is reflexive and symmetric, but not transitive (since $(1, 2)$ and $(2, 1)$ are in R, but $(1, 1)$ is already present).

8.2 Equivalence Relations

Definition An **equivalence relation** on a set A is a relation R that is reflexive, symmetric, and transitive.

Equivalence Classes For an equivalence relation R on a set A, the **equivalence class** of an element $a \in A$ is the set of all elements in A that are related to a by R:

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

Properties of Equivalence Classes

- Every element belongs to exactly one equivalence class.
- The equivalence classes form a partition of the set A.
- $aRb \iff [a]_R = [b]_R$

Examples of Equivalence Relations

- **Equality** on any set: $a = b$ defines an equivalence relation.
- **Congruence modulo** n: For integers a and b, $a \equiv b \pmod{n}$ if n divides $(a - b)$.
- **Same size**: For sets A and B, $A \sim B$ if there exists a bijection between A and B.

Example: Modular Arithmetic In $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with relation $a \equiv b \pmod{5}$, the equivalence classes are:

- $[0] = \{..., -10, -5, 0, 5, 10, ...\}$
- $[1] = \{..., -9, -4, 1, 6, 11, ...\}$
- $[2] = \{..., -8, -3, 2, 7, 12, ...\}$
- $[3] = \{..., -7, -2, 3, 8, 13, ...\}$
- $[4] = \{..., -6, -1, 4, 9, 14, ...\}$

Partition of a Set A **partition** of a set A is a collection of nonempty subsets $\{A_i\}$ such that:

- Each element of A belongs to exactly one subset A_i.
- The union of all subsets equals A.
- The intersection of any two distinct subsets is empty.

8.3 Partial Orders

Definition A **partial order** on a set A is a relation R that is reflexive, antisymmetric, and transitive. A set with a partial order is called a **partially ordered set** or **poset**.

Common Notation For a partial order, we often use the symbol $\leq$ or $\preceq$ instead of R.

Properties

- Two elements a, b in a poset are **comparable** if $a \leq b$ or $b \leq a$.
- If neither $a \leq b$ nor $b \leq a$, then a and b are **incomparable**.
- A partial order where any two elements are comparable is called a **total order**.

Special Elements in a Poset $(A, \leq)$ For a subset $B \subseteq A$:

- An element $m \in A$ is a **minimal element** of B if there is no element $b \in B$ with $b < m$.
- An element $M \in A$ is a **maximal element** of B if there is no element $b \in B$ with $M < b$.
- An element $g \in A$ is a **greatest lower bound (glb)** or **infimum** of B if:
  - $g \leq b$ for all $b \in B$ (lower bound)
  - If $h \leq b$ for all $b \in B$, then $h \leq g$ (greatest lower bound)
- An element $l \in A$ is a **least upper bound (lub)** or **supremum** of B if:
  - $b \leq l$ for all $b \in B$ (upper bound)
  - If $b \leq k$ for all $b \in B$, then $l \leq k$ (least upper bound)

Examples of Partial Orders

- The relation $\leq$ on $\mathbb{R}$ is a total order.
- The subset relation $\subseteq$ on the power set $\mathcal{P}(S)$ is a partial order.
- The divisibility relation $|$ on $\mathbb{Z}^+$ is a partial order.

Hasse Diagrams A **Hasse diagram** is a visual representation of a finite poset where:

- Elements are represented as vertices.
- If $a < b$ and there is no c such that $a < c < b$, then an edge connects a to b.
- If $a < b$, then a is drawn below b.

Example: Divisibility For the set $A = \{1, 2, 3, 4, 6, 12\}$ with the divisibility relation $|$:

- 1 divides every number, so it's at the bottom of the Hasse diagram.
- 12 is divided by every number, so it's at the top.
- 2 and 3 are incomparable (neither divides the other).

Summary

- A relation is a subset of $A \times B$.
- Equivalence relations (reflexive, symmetric, transitive) partition a set into equivalence classes.
- Partial orders (reflexive, antisymmetric, transitive) create hierarchical structures.
- Both have important applications in mathematics and computer science.

9. Counting and Probability

9.1 Introduction to Probability

Definition

- A **sample space** is the set of all possible outcomes of a random process or experiment.
- An **event** is a subset of a sample space.

Probability Formula

If S is a finite sample space in which all outcomes are equally likely and E is an event in S, the probability of E, denoted $P(E)$ is:

$$P(E) = \frac{|E|}{|S|}$$

where $|E|$ is the number of outcomes in event E and $|S|$ is the number of outcomes in the sample space S.

Theorem

If m and n are integers such that $m \leq n$, then there are $n - m + 1$ integers in the set $\{m, m+1, \ldots, n\}$.

9.2 Possibility Trees and Multiplication-Rule

Definition A **possibility tree** is a graphical representation of all possible outcomes of a random process, where each branch represents a choice or event leading to further choices or outcomes.

The Multiplication Rule

The **multiplication rule** states that if a process can be broken down into k stages, where the first stage has n_1 possible outcomes, the second stage has n_2 possible outcomes, and so on up to the k-th stage with n_k possible outcomes, then the total number of possible outcomes for the entire process is given by:

$$N = n_1 \times n_2 \times \ldots \times n_k$$

Permutation

A **permutation** of a set is an arrangement of its elements in a specific order. The number of permutations of n distinct objects is given by:

$$P(n) = n!$$

where $n!$ (n factorial) is the product of all positive integers up to n.

Example You can arrange the letters int the word "COMPUTER" in 8! different ways, since there are 8 distinct letters.

r-Permutation

An **r-permutation** of a set of n distinct objects is an arrangement of r objects selected from the set. The number of r-permutations is given by:

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

where n is the total number of objects and r is the number of objects to arrange.

Example The number of ways to arrange 3 letters from the word ”COMPUTER” is given by:

$$P(8,3) = \frac{8!}{(8-3)!} = \frac{8!}{5!} = 8 \times 7 \times 6 = 336$$

9.3 Counting Elements of Disjoint Sets

Addition Rule

The **addition rule** states that if A and B are two disjoint sets (i.e., they have no elements in common), then the number of elements in the union of these sets is given by:

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

Difference Rule

The **difference rule** states that if A and B are two sets, then the number of elements in the difference of these sets is given by:

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

If S is a finite sample space and A is an event in S, then:

$$P(A^c) = 1 - P(A)$$

Example Consider tossing a coin 5 times.

- There are 6 possible outcomes where there is exactly one head.
- There are $2^5 = 1 = 31$ possible outcomes where there is at least one head.

The includion/exclusion rule for Two or Three Sets

If A, B, and C are finite sets, then:

$$N(A \cup B) = |A| + |B| - |A \cap B|$$
$$N(A \cup B \cup C) = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$